Digital Identity Toolkit

A GUIDE FOR STAKEHOLDERS IN AFRICA

June 2014

WORLD BANK GROUP

Digital Identity Toolkit

A GUIDE FOR STAKEHOLDERS IN AFRICA

June 2014

WORLD BANK GROUP

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Table of Contents

ACKNOWLEDGMENTS v

EXECUTIVE SUMMARY vii

SECTION I: OVERVIEW – IDENTITY MATTERS

I.1 Identification is Necessary for Modern Development 1

I.2 Digital Identity as a Platform for National Identification 3

I.3 Digital Identity is Growing in Developing Countries 4

SECTION II: HOW IDENTITY MANAGEMENT WORKS

II.1 Identity as a Set of Attributes 7

II.2 Identity Lifecycle: Registration, Issuance, and Use 8

II.3 Registration: Enrollment and Certification that Identity is Authentic 9

II.4 Issuance: Providing a Credential 12

II.5 Use: Authentication and Updating of an Identity 15

SECTION III: DEVELOPING A DIGITAL IDENTITY PROGRAM

III.1 Policy and Regulation 19

III.2 Institutional Framework and Governance 21

III.3 Technology 26

III.4 Trust, Privacy, and Security 36

III.5 Operational Processes and Controls 40

SECTION IV: POLICY CONSIDERATIONS 43

Acknowledgments

This report was prepared by Joseph J. Atick, PhD (Chairman, Identity Counsel International) and Zaid Safdar (Task Team Leader, World Bank), with inputs from Alan Gelb (Center for Global Development), Elena Gasol Ramos (World Bank), and Seda Pahlavooni (World Bank). The work was conducted under the management of Randeep Sudan (Sector Manager, ICT), Mavis Ampah (Program Coordinator, ICT Africa), and Samia Melhem (Chair, DigDev CoP) of the World Bank. The team is grateful to the Government of France for its financial contribution, which has made this project possible. The report additionally benefited from a background note and extensive work done by PricewaterhouseCoopers (PwC) of South Africa. We wish to thank Véronique Massenet of the Government of France; Alain Ducass of Adetef; Frank Leyman of IDM Expert Group; and Robert Palacios, James Neumann, Harish Natarajan, Balakrishnan Mahadevan, Tenzin Norbhu, Mariana Dahan, and Kaoru Kimura of the World Bank for their helpful feedback and comments. We wish to thank the Translation & Interpretation Unit (GSDTI) of the World Bank for the Editing of the Toolkit and Manuella Lea Palmioli (GSDTI) for the cover design. The team also wishes to thank Tasneem Rais and Michele Ralisoa Noro of the World Bank for managing the publication of the report.

Executive Summary

Digital identity, or electronic identity (eID), offers developing nations a unique opportunity to accelerate the pace of their national progress. It changes the way services are delivered, helps grow a country's digital economy, and supports effective safety nets for disadvantaged and impoverished populations. Digital identity is a platform that transcends economic and social sectors and contributes to enhancing a country's political environment. For some, digital identity is a "game changer" or a "poverty killer."[1] India's *Aadhaar* and Estonia's identity programs are examples in which eID has effectively been used to promote economic and social development.

Though of particular relevance to developing nations, eID has been important to developed nations as well. Most rich countries have robust identification systems, which provide their people with an "official identity," grounded on official documentation, such as birth certificates. The official identity is used to provide public safety, policing, national security, and border protection. Today, firms in developed countries use innovative techniques in authenticating a user's official identity, whether in mobile applications, digital commerce, social media, or everyday use. For developing nations, the absence of an official identity would pose a fundamental challenge.

The advent of new technologies—in the form of mobile devices, social media, and the Internet—offers additional opportunities for developing countries. When combined with mobile phones and the Internet, identification allows services to be delivered electronically, giving a boost to government efficiency and leading to the creation of new online products and services. With 6.5 billion mobile phone users in the world today,[2] moile phones and the Internet are the widest channels for service delivery. By 2013, 67.4 percent of Sub-Saharan Africans had a mobile phone subscription, totaling 614 million mobile phone subscriptions.[3] Today, 8.5 percent of Africans are using smart mobile devices, such as smartphones or tablets, totaling 77 million users.[4]

Though digital identity is an opportunity, it raises important considerations with respect to privacy, cost, capacity, and long-term viability.

This report provides a strategic view of the role of identification in a country's national development, as well as a tactical view of the building blocks and policy choices needed for setting up eID in a developing country.

Why identification?

Identification plays an important role in facilitating the interactions of individuals with their government and with private institutions to operate in a structured society. Without a robust means of proving one's identity, exercising one's basic rights, claiming entitlements, accessing a range of governmental services, and conducting many daily activities could be hampered. In addition, a lack of effective identification could render government organizations less efficient and less

[1] See press release: "India's Massive I.D. Program Exemplifies 'Science of Delivery,'" at http://www.worldbank.org/en/news/feature/2013/05/02/India-8217-s-Massive-I-D-Program-Exemplifies-8216-Science-of-Delivery-8217 (last accessed May 10, 2014).
[2] Wireless Intelligence (2014).
[3] Wireless Intelligence (2014); World Bank (2014).
[4] Ibid.

accountable. As such, robust identification is recognized as an important tool for socioeconomic and political development.

What is electronic identity (eID)?

Today, the importance of identification is increasing, as more human activities and transactions are conducted online and are becoming mobile. This trend creates new opportunities and new vulnerabilities, and prompts the need for digital identity. eID provides technology-based solutions for identification in order to uniquely establish a person's identity and to credential it, so that the identity can be securely and unambiguously asserted and verified through electronic means for delivery of services across sectors, including healthcare, safety nets, financial services, and transport. National governments play an important role in facilitating the development of such systems, and in building the trust required to establish and maintain them, through informed policy and regulations, which must be in effect before the full benefits of such systems can be realized.

Privacy is pivotal

The data-centric nature of eID and the collection and retention of information—often deemed personal—of individuals can be perceived as an invasion of privacy. A successful eID program can become pervasive over time, creating digital data trails of a person's routine actions, linked to a unique and traceable identity. Thus, the effects on privacy can be further compounded. To protect the privacy of people, an eID program has to institute strong measures, including, but not limited to, appropriate legislation, data protection, public notices, an individual's right to consent, design principles for privacy, a documented privacy policy, an independent body for privacy oversight, and the effective enforcement of laws and regulations.

Technology as an enabler

Technology provides a means by which to automate the various steps involved in a national identification system. Chief among the technology choices is the possible use of biometrics—i.e. technologies that use patterns, such as fingerprints, iris texture, or facial geometry—to determine a person's identity. Biometrics can be used to uniquely identify individuals in lieu of robust civil registration systems, which capture the birth or death of people, or in the absence of official birth certificates in developing countries. Governments face the choice of strengthening their civil registration systems or using biometrics, or both. Though biometric technologies offer an attractive option in the context of developing countries, they pose additional considerations regarding privacy, cost, capacity, and long-term viability. Biometrics can also be used for authentication, though this approach requires strong provisions with respect to fraud prevention and liability management.

Two aspects of a national technology strategy are also noteworthy: a country's underlying technology infrastructure and the importance of international standards for eID systems. A modern eID system can require a well-developed infrastructure offering high-speed Internet, which is not always a given in many developing countries. A vibrant domestic information technology (IT) industry can be important, offering human capacity, possible partnership with the private sector, and a local marketplace of new products and services using eID. Additionally, the use of international standards is essential to ensure interoperability across, at times, disparate eID systems, and to protect against lock-in due to a single vendor or a specific technology.

The cost dimension

Such eID systems can be costly, in terms of expenditures related both to upfront setup and ongoing operations. Expenses are to be minimized, keeping in view the total cost of ownership of eID systems. Governments can consider potential revenue flows by offering identity services to offset the investment necessary to develop an eID and to induce sustainability in its operation. Public-private partnerships (PPP) can provide an avenue through which to relieve the fiduciary burden. A financial and economic model, with detailed expected costs and potential revenue streams, needs to be developed in advance. This report offers insights into the cost dimension of eID systems, though

indicates that a separate, detailed study on cost-benefit analysis could help bolster the findings of this report.

Coordinating across sectors and building human capacity

Launching an eID system can be a significant undertaking for a government in a developing country. Two challenges are noteworthy. First, the cross-sectoral nature of eID 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 the form of multiple identity cards supported by multiple identity registers. Coordinating the development of an official identity across these disparate eID programs can be difficult. Second, the technology-centric nature of eID 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 eID platform.

In this report, we present a conceptual overview of digital identity management practices, providing a set of guidelines at a national level that policymakers can find helpful as they begin to think about modernizing the identity infrastructure of their country into eID. The report provides an operating knowledge of the terminology and concepts used in identity management and an exposition of the functional blocks that must be in place. Given its abridged nature, the report is intended to be insightful and detailed, though not exhaustive. Several important topics related to eID are noted though deserve further discussion, including: economic and financial analysis, the development and setup of a national civil register, and cross-border aspects of eID. The building blocks, as discussed, can help ensure that a secure, robust and reliable digital identity platform can serve the development needs of a country for the foreseeable future.

I. OVERVIEW: Identity Matters

I.1 Identification is Necessary for Modern Development

Central to a government's ability to deliver services to its people, whether those services be healthcare, safety nets, or drivers' licenses, is knowledge of who those people are. The same is true for private enterprises. For example, a bank's ability to offer services to its clients—such as opening a bank account or securing a loan—requires a certain knowledge of the intended recipient. This is where identification programs come in.

With the growing use of mobile phones, social media, and the Internet, the need for identification becomes even more important. When combined with mobile phones and the Internet, identification allows services to be delivered electronically, giving a boost to government efficiency and leading to the creation of new products and services online. With 6.5 billion mobile phone users in the world today,[5] mobile phones and the Internet are currently the largest channels for service delivery. By 2013, 67.4 percent of Sub-Saharan Africans had a mobile phone subscription, totaling 614 million mobile phone subscriptions.[6] As for smart mobile devices, 8.5 percent of Africans are using a smart phone or a tablet, totaling 77 million users.[7] Employing these new channels for service delivery requires investing in robust and reliable identification systems capable of establishing unique, official identities for individuals to enable e-government and e-commerce.

Identification is thus a prerequisite for modern development. A robust identity system involves capturing the unique identity of each individual in a national identity registry. Once a registry is established, a government may issue official identification to each person in the form of a national identity card with a unique identification number, and it may also operate identity services that verify personal identity online. A national registry can then be used across sectors—from education and healthcare to transportation and urban development—for the delivery of services, both public and private (see **Figure 1**). For example, a government offering safety net transfers to the country's poor can use the national identity registry to help identify the target population and issue cash transfers electronically. A financial institution can use the national registry to easily validate identity, thereby addressing a key aspect of Know Your Customer (KYC), and can offer a host of financial services, such as opening an account, securing credit, taking deposits, or paying for services, whether at a bank branch, on a

> TODAY'S MODERN SOCIETY CREATES NEW DEMANDS ON IDENTITY: IDENTITY HAS TO BE MOBILE, TRANSACTIONAL, INTEROPERABLE, PORTABLE, AND SOCIAL—IN ADDITION TO BEING SECURE.

[5] Ibid.
[6] Ibid.
[7] Ibid.

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 person. Without a reliable way of proving one's identity, exercising basic rights, claiming entitlements, accessing a range of governmental services, and conducting 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.[8]

For developing countries, identification poses a daunting challenge. Many of these countries lack robust identification systems inclusive of their entire population. Some operate in a fragmented identification space, where several agencies, both public and private, compete to offer identification in the form of a health insurance card, a bank identity card, a voter identity card, or a ration card. An official identification is often missing among these varied identities, leading to inefficiencies in the way the government and firms interact with the population. Offering an official identity in a developing country is even more difficult in the absence of birth certificates, a foundation for official identification. In 2000, some 36 percent of children worldwide and 40 percent of children in the developing world were not registered at birth.[9] South Asia had the highest percentage of unregistered births (63 percent), followed by Sub-Saharan Africa (55 percent) and Central and Eastern Europe (23 percent). Among the least-developed countries, under-registration was at 71 percent.[10] Even for those who are registered, birth certificates are often difficult to access due to poor record keeping, lack of mobility, or corruption.[11]

Depending on the context, identification can go beyond delivering services efficiently. Identification can also be a foundation for a secure society. Herein lies the difference between rich and poor countries in the way governments sponsor identification. In rich countries, official identity has long been used to provide public safety, policing, national security, and border protection.

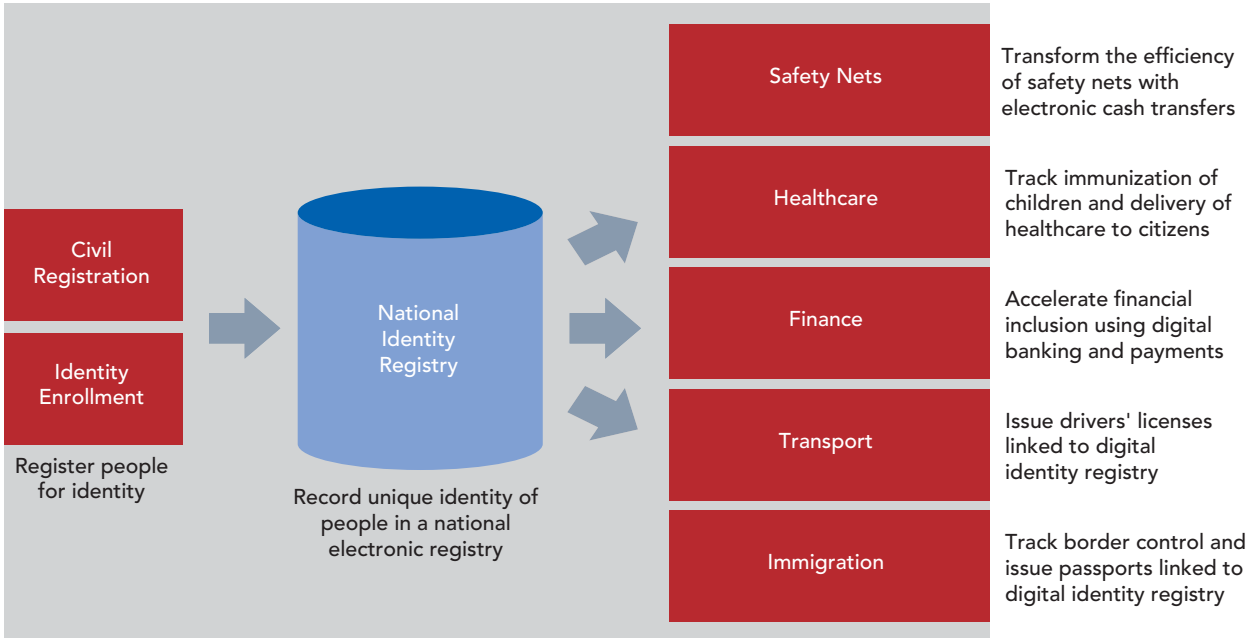
[8] See Organization for Economic Co-operation and Development Report "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy" (2011).

[9] The United Nations Children's Fund (UNICEF), "The 'Rights' Start to Life: A Statistical Analysis of Birth Registration," (New York: UNICEF, 2005).

[10] UNICEF Innocenti Research Centre, "Birth Registration: Right from the Start," Innocenti Digest No. 9, (Florence: UNICEF, 2002).

[11] See Gelb and Clark, "Identification for Development: The Biometrics Revolution," Working Paper 315 (Center for Global Development, 2013).

FIGURE 1: A National Vision for Economic and Social Development



Source: World Bank analysis.

Identification in Social Protection

When mechanisms for identification are weak, individuals may experience difficulty proving their eligibility for social protection assistance. Without a common identity, coordination among different development programs on the identification of potential beneficiaries becomes more difficult and costly. Invariably, multiple databases result, with beneficiaries' identities not necessarily linked across them. These programs become vulnerable to misuse and sizeable leakages.

Examining how fraud could manifest itself within this illustrative context underscores the scope of vulnerability of identification-based service programs in general:

- An individual may assume multiple identities, using false or assumed names when registering for benefits, and thereby receive more than his or her fair share of assistance (monetary, food, etc.).
- A head of a household may inflate the size of his or her family by "borrowing" children from other households during household registration. Often those same children are lent back to other households and registered again, resulting in exaggerated family units.
- When aid is in the form of guaranteed employment, an individual who secures work may "outsource" that labor by selling it to another individual who performs the work in his or her place.
- In long-term programs, the death of a beneficiary may not be communicated in a timely fashion. The ration or benefit card of the deceased could continue to be used by a family member or another individual.
- The registration of fictitious individuals (or ghost workers) through collusion with local government may aid workers who see the lack of identity accountability as an opportunity to defraud the program.

In poor countries, official identity is seen as instrument for economic, social, and political development, such as by reducing leakage in government-sponsored programs, enhancing government efficiency, improving labor mobility, and enhancing social inclusion, empowerment, and accountability. The gap between rich and poor countries is, however, narrowing, as more transactions are conducted online. Even in rich countries, identification systems are beginning to play an important role in facilitating e-government and e-commerce.[12]

I.2 Digital Identity as a Platform for National Identification

Digital identity provides a cross-sector platform on which to establish a robust identification system in a country, on a rapid timetable, and enables services across sectors to be delivered electronically. Such a development can be transformational for a country, offering gains in government efficiency, private sector development, and national development. However, these gains come with risks, which are to be mitigated.

A digital identity platform automates the steps of a national identification system with a number of technology-based solutions, which include:

- *Biometrics:* In the absence of a strong civil registry system (such as for birth, death, or marriages) in developing countries, biometrics offers a possible technology to uniquely identify individuals. Biometrics consists of electronically capturing a person's face photo, fingerprints, or iris. Biometrics may also be useful for authentication.

- *Electronic databases:* Instead of storing identity information in paper registers, creating significant stress on cost and efficiency, electronic databases can be used to store and reference identity data. Electronic capture and storage of data is also a first step towards offering electronic services. Electronic

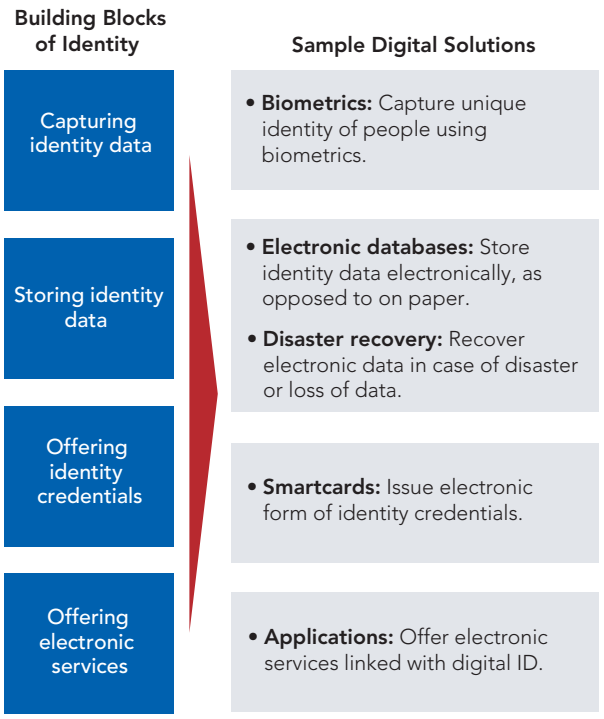
[12] See for example The U.S. White House Report, "National Strategy for Trusted Identities in Cyberspace," (April 2011).

storage of identity data allows data to be recovered in the face of natural or man-made disasters.

- *Electronic credentials:* Once identity information is captured, governments may offer identity credentials to individuals in the form of paper-based national ID cards, or electronic smartcards. The use of smartcards can offer advantages for electronic health records, immunization records, electronic payment transfers, and other applications.

- *Mobile, online, and offline applications:* With digital identity, services can be delivered on a computer or a mobile phone for a range of sectors, including healthcare, education, banking, social services, and others. The availability of point-of-sale (POS) devices can enable an efficient means of authentication, allow signup for bank accounts or other transactional accounts, and further increase the use of electronic transactions.

FIGURE 2: Digital Identity Platform for National Identification



Source: World Bank analysis.

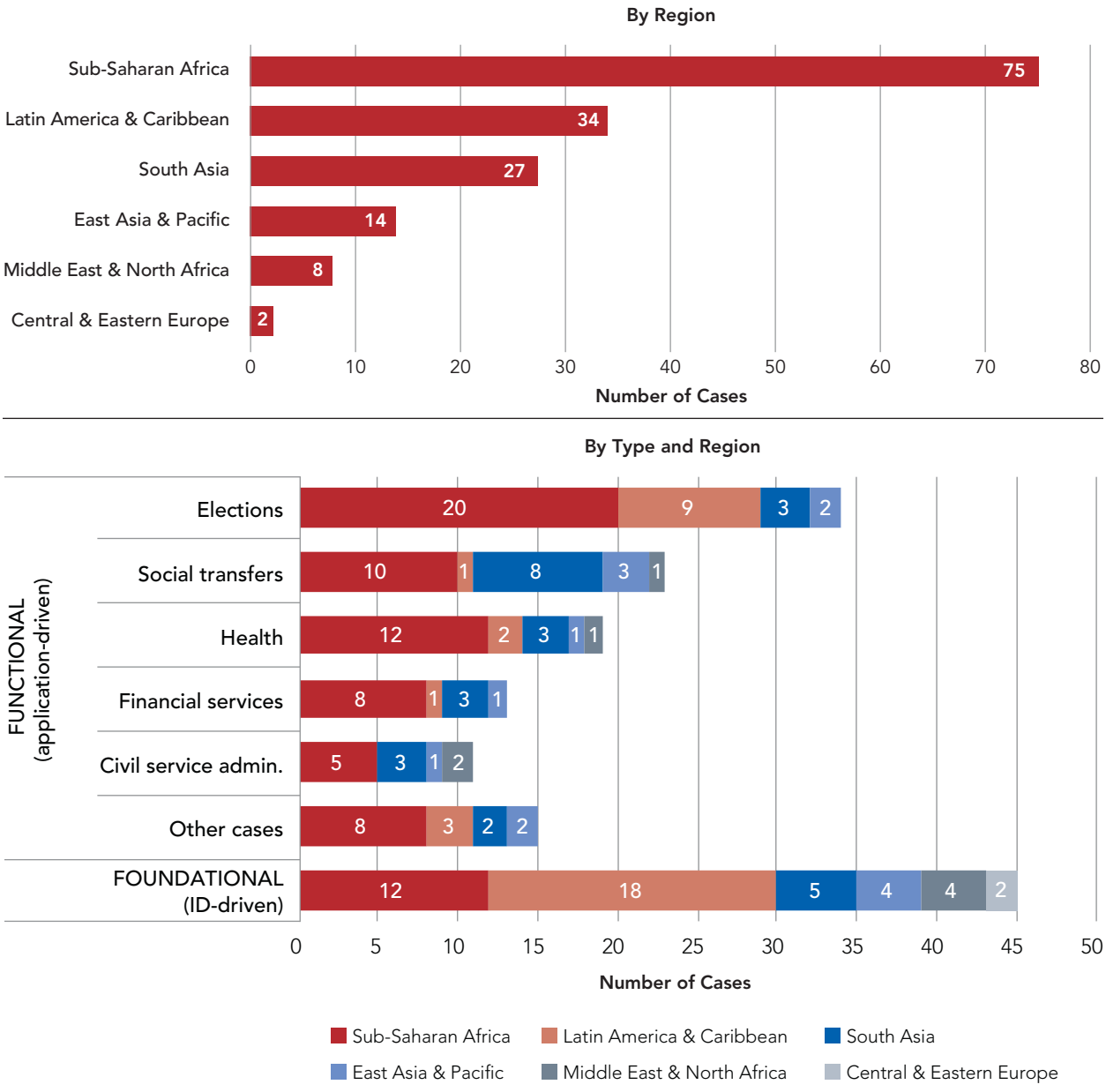
Along with its benefits, a digital identity platform poses several risks, which require mitigation. First, the electronic capture and storage of personal data requires strong provisions of governance and management to ensure its security and privacy, protecting it from misuse, exploitation, or theft. Second, building a digital platform can be costly, requiring careful attention to optimizing the cost structure, and exploring potential revenue streams for making the effort sustainable. Third, a digital platform puts greater demands on the technical capacity of the responsible organization and requires balancing with the use of public-private partnerships, where feasible. Finally, a digital platform requires an eye towards long-term operations and maintenance, necessitating provisions of cost, capacity, and upfront design, to ensure that identification works well in the long run and is not subject to operational decay over time.

I.3 Digital Identity is Growing in Developing Countries

A number of developing countries are building digital identity platforms as a means of enabling economic and social development. In 2013, Gelb and Clark surveyed and identified over 230 digital identity systems across more than 80 developing countries. These systems use biometric technology to identify a segment of population for the sake of economic or social development. These systems consist of two types: (a) *foundational* – which are built in a top-down manner with the objective of bolstering national development by creating a general-purpose identification for use across sectors; and (b) *functional* – which evolve out of a single use-case, such as voter ID, health records, or bank cards, and have potential for use across sectors. According to Gelb and Clark, at least 37 countries offer multiple functional platforms for digital identity. For example, in India, there are 15 or more instances in which a range of actors (central, state, and municipal governments; donors; and NGOs) use biometric identification. Kenya, Malawi, Mexico, Nigeria, and South Africa offer a similar scenario. People in these countries carry multiple forms of identity for different government agencies or private firms, posing potential challenges.[13]

[13] Gelb and Clark (2013).

FIGURE 3: A Sample of Digital Identity Platforms Using Biometrics



Source: Gelb and Clark 2013.

Digital identity platforms differ across countries, including in the way technology is used (for registering people or for issuing credentials) or in the way the institutional structure is setup. Estonia and India present two examples at two different extremes. In Estonia, the government uses a strong civil registry system to record digital identity, issues a chip-based identity card bearing a photograph, and allows users to use digital identity with a personal identification number (PIN). No biometrics information is collected.[14] Such a model works well in a developed country, where the population is highly educated, online services are widely used, and the civil registry is well developed. In contrast, in India, the government has launched a biometric system, capturing 10 fingerprints and two irises of each registering individual, in order to issue a 12-digit unique identification

[14] Non-citizens provide 10 fingerprints, and Estonia now has a biometric passport.

number. No identity card is issued. The unique ID number is then used for a variety of public and private services, often in conjunction with the person's address, biometric information, or password. Similarly, Ghana and Pakistan present two different models of institutional structures. In Ghana, the National Identity Authority (NIA) is an agency within the Office of the President responsible for rolling out the country's unique identity program. In contrast, in Pakistan, a National Database & Registration Authority (NADRA) serves as an autonomous body within the government to offer digital identity services, and sustains operations in part through fees collected via identification services.

TABLE 1: Common Models of Digital Identity Systems

Technology	**Estonia** **Institution**: Citizenship and Migration Board, within Ministry of Internal Affairs. **Registration**: Civil registration. **Credential**: Identity card with a photograph and a chip. **Target population**: 1.3 million people. **Use of ID based on**: Personal ID number (PIN).	**India** **Institution**: Unique Identification Authority of India, within Planning Commission of India. **Registration**: Biometrics (10 fingerprints and iris). **Credential**: No physical credential (a 12-digit unique ID number or "Aadhaar" is given). **Target population**: 1.2 billion people. **Use of ID based on**: Aadhaar number, along with demographic, biometric, or password.
Institutional Structure	**Ghana** **Institution**: National Identity Authority, within the Office of the President. **Registration**: Biometrics (fingerprints). **Credential**: National identity card ("Ghana Card"), and smartcard. **Target population**: 25 million people. **Use of ID based on**: National identity card and biometrics.	**Pakistan** **Institution**: National Database and Registration Authority (autonomous body). **Registration**: Biometrics (fingerprints). **Credential**: National identity card with a photograph, smartcard, and mobile ID. **Target population**: 180 million people. **Use of ID based on**: Smartcards, mobile phones, and biometrics.

II. How Identity Management Works

II.1 Identity as a Set of Attributes

For our purposes, identity is defined through a set of human attributes or characteristics (referred to as identifiers) that, once specified, narrow down all possible entities to one and no other.[15] Thus "identity = A, B, C, …" attributes. The choice of attributes is what is called the *identity regime*.

Traditionally, this regime has operated with attestable *biographic identifiers*, such as name, birth date, citizenship, address, profession, family, tribe, etc. Today, such a regime is considered less reliable, since its attributes could be hijacked or faked. This is rectified in the *biometric identity regime*, which relies either exclusively or primarily on immutable and indisputable attributes called biometrics (see box on page 8).

An identification program should be able to answer the question *who is this person* by searching the unknown person's template within the database of templates associated with known people (identification, or 1:N search or matching) or to validate that *they are who they claim to be* by comparing their template to the one associated with the claimed identity (verification, or 1:1 matching) retrieved from a central data repository or residing on another storage medium (e.g., a smartcard the person may be carrying).

There are some misconceptions and differences in terminology as to what identity management is about. For the sake of clarity, it is worthwhile to distinguish, from the outset, two related processes:

- **Identification Management:** establishes a unique identity for each real person (identification), fixes it, credentials it, and binds it to individual actions as they occur in the future (authentication). Optionally, it can also link identity to an appellation or a legal name (legal or social identity) through a process called vetting, or identity resolution.

> THE GOAL OF A NATIONAL IDENTITY PROGRAM SHOULD BE TO ATTRIBUTE ONE IDENTITY PER PERSON PER LIFETIME FOR ALL NEEDS.

- **Identity Intelligence & Identity Risk Assessment:** discovers and tracks the reputation of an identity. Performs background checks against watch-lists and other sources of identity knowledge.[16] Uses statistical inference (e.g., big data) to predict intention based on a history of prior actions; assesses the risk attributed to a given identity; and determines a trust score (just like a credit score).

Often, and especially in rich countries, the two processes are inextricably lumped together. In this paper,

[15] Underlying this definition is Quine's well known philosophical view that "To be is to be the value of a variable," and the assertion that "No entity is without identity." W. V. Quine, "*Ontological Relativity and Other Essays*," (Columbia University Press, New York, 1969). The implication is that specifying a rich group of attributes can always achieve the specificity of identification.

[16] This may include checks of Internet protocol (IP) addresses, postal addresses, or other forms of information relevant to a person.

Biometrics

Biometrics are characteristics of the human body that can be used as attributes to establish personal identity. Biometric systems begin with patterns, such as fingerprints, iris texture, and face geometry, imaged via specialized sensors. The images are then converted, using proprietary algorithms, into a set of templates, which are mathematical codes intrinsic to the individual, insensitive to extrinsic image variability (skin condition, eye color, expression, hair style, viewing conditions, etc.). Given a large enough set (e.g., using enough numbers of fingers), this code can be demonstrated to be unique for each individual within a population size, with reasonable accuracy. Thus, identity can be conveniently fixed through a set of biometric identifiers that have sufficient resolving power to distinguish unambiguously any given person from the entire group. In addition to fingerprints, face prints, and iris scans, additional forms of biometrics have emerged in recent years, including voice prints, retinal scans, vein patterns, and DNA. Other ways to fix identity that do not use biometrics include the use of robust civil registration procedures.

we focus on identification management as defined in article 1 above, since that is most relevant for developmental applications and the practice of that discipline is mature enough that it can be considered a standard element of a country's information and communication technology (ICT) activities. We will refer to that interchangeably as identity or identification management.

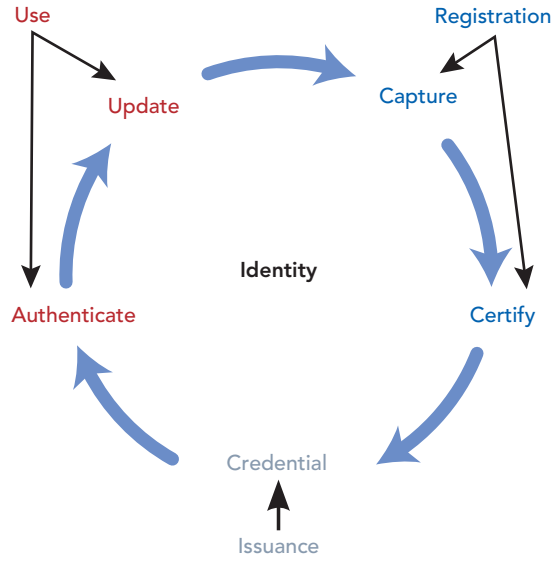
II.2 Identity Lifecycle: Registration, Issuance, and Use

An eID management program consists of a set of coordinated processes supported by business functions, technical systems, policies, and procedures that, in their totality, deliver solutions for the different phases of the identity life cycle.

It is widely accepted that the identity lifecycle can be divided into three basic phases: *Registration, Issuance,* and *Use*; but these have sub-phases. For example, sometimes Registration is subdivided further, as *Data capture/Enrollment* and *Certification*, while Issuance is referred to as *Credentialing* and Use is subdivided into *Authentication/Verification* and *Update* (or revocation), as shown in **Figure 4**.

In **Table 2** we also present some of the processes that need to be established in order to manage identity during each phase, as well as some of the *Use Cases*, that emerge in the public as well as private sectors once an identity has been registered and issued a proof of identification. The list of Use Cases is extensive but by no means exhaustive.

FIGURE 4: Identity Lifecycle Showing the Sub-phases under Registration, Issuance, and Use



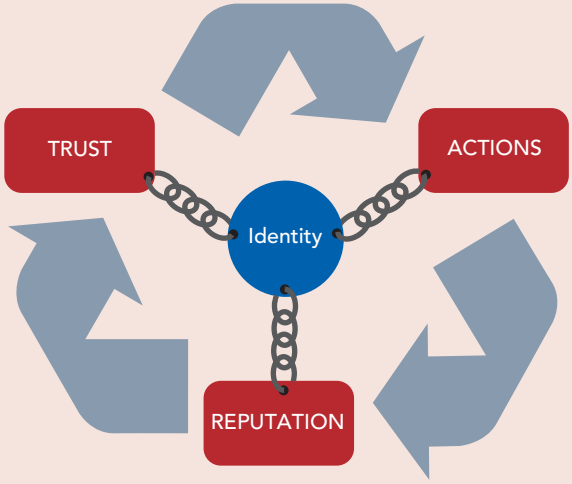
Source: World Bank analysis.

Identity and Trust

It can be argued that the role of identity has not changed since the beginning of civilization. Humans use identification to determine in which type of interactions to engage with other people. More specifically, we use identity to facilitate the actions of those we know and trust, and to protect us from those we do not trust or from those we do not know.

Identity is what binds a person to his or her reputation, and reputation is what earns that person trust within the community, which in turn facilitates or inhibits that individual's actions depending on his or her level of trust. The cycle of identification does not end. As we conduct more actions, the volume of our reputational data increases and our trust level is continually adjusted through the judgment of the prevailing social, moral, and legal codes.

Identity is at the core of human-human interactions and, by analogy, eID will be at the core of human-machine or human-information systems interactions as eID achieves more penetration.



II.3 Registration: Enrollment and Certification that Identity is Authentic

Identity Registration is the first and most important step in capturing a person's identity.[17] It consists of a set of procedures for collecting data (enrollment) and using it to verify that the identity is authentic by validating the following conditions:

- **Existence:** claimed identity exists (and is alive, not a ghost) at the time of enrollment and can be localized (reached through address, email, phone number, etc.).
- **Uniqueness:** claimed identity is unique or claimed only by one individual.
- **Linkage:** presenter can be linked to claimed social identity.

The process begins by capturing identifying data from each person, which can include biographic or biometric information at an enrollment center or in a field office using an enrollment station. The captured data consists of the three elements in **Table 3**. It is important to note that the use of biometrics is helpful in establishing uniqueness, as we discuss below, but it is by no means the only method for doing so. In cases where the civil register is highly developed and reliable, the use of biometrics becomes less important or may not be needed.

Biographic or biometric data associated with the *Core Identifying Data* (CID) are first collected. In the case of biometrics, key attributes are imaged on specialized off-the-shelf scanners or sensors, or standard face cameras, producing high-definition images of the fingerprint pattern, the iris texture of the eye (in the infrared spectrum), or a standard photograph of the face.[18] The *Validation Data* and the *Metadata* can consist of scanned copies of breeder documents, such as birth certificates, voter cards, drivers' permits, community affidavits (including those from religious institutions), certificates from educational institutions, and other proofs of identification or

[17] Identity management is additionally about comparing the person who is physically present with the data retained in a database.

[18] The market for biometric scanners is mature and is subject to a body of standards and certifications that ensure consistency of performance and quality of captured images.

TABLE 2: Identity Management Processes throughout the Identity Lifecycle

Process / Owner	Registration		Issuance	Use	
	Capture/Enroll	Certify	Credent	Authenticate	Update
Enrollment Agencies	• Data Capture • Field Validation • Transmission				
National Identity Repository		• Vetting • Linkage • De-duplication • Unique ID Number • Digital Certificates and Credentials	• ID-in-Cloud • Certificate Authority (CA)	• Identity Services • Identity Authentication	• Identity Profile Updates • Maintenance • Identity Revocation
Public Sector			• Credential Issuance • ID Cards • eID and Mobile ID • Smartcards • SIM Cards	• Passport Acquisition • Immigration Control • Universal Health Care • Access to Social Services • PDS Programs • Public Safety • Law Enforcement • Education • Children's Rights • E-Government Services • Taxation • Business Registration • Pension Claims • Electoral Registration • Drivers' Licenses • Property Registration	
Private Sector				• Financial Services • Healthcare • Transportation • Mobile Transactions • SIM Card Registration • Creditworthiness • Employment • Travel	

use of name and social reputation, and/or may include self-declarations of applicant collected by a trained agent during enrollment.

The collected data is automatically compressed, encrypted by the enrollment software, and submitted to a central repository. This repository is sometimes referred to as the National Population Register or the *National Identity Register* (NIR). There, it undergoes several steps of processing and validation. First, templates are generated from the biographical data or biometric images, which are then exhaustively searched against all previously enrolled templates associated with known identities. For biometrics, the search engine is called Automated Fingerprint Identification System (AFIS) or Automated Biometric Identification System (ABIS), depending on whether it uses fingerprints only or multiple biometrics for the search and match function. A schematic of this process is shown in **Figure 5**. If no match is found, the identity is considered new and is passed on to the next phase for further validation. If, on the other hand, a match is found, it means that this identity was previously enrolled (duplicate). A human intervention or control step by a trained operator is used to validate that the match is a fraudulent attempt and to

TABLE 3: Type of Identity Data Typically Captured during Enrollment

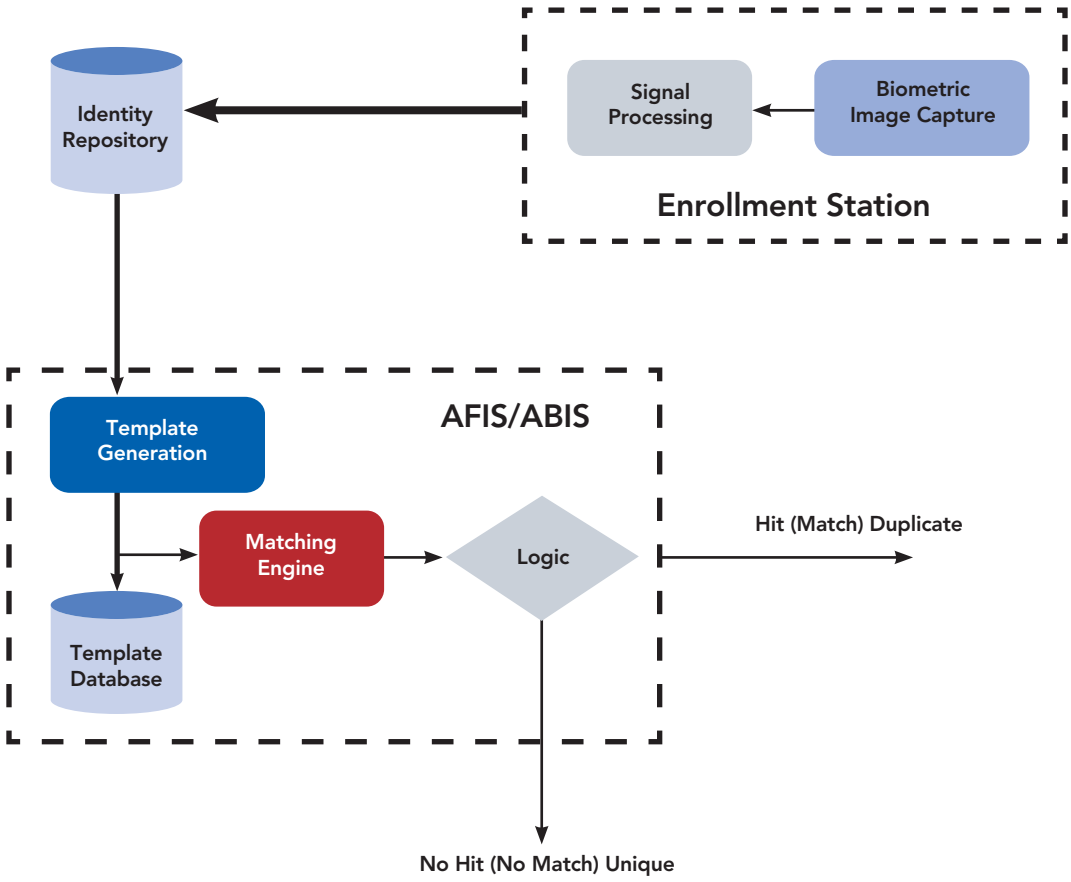
Data Type	Description
Core Identifying Data (CID)	Minimum set of attributes required to define a unique identity and to fix it thereafter.
Validation Data	Proof that claimed identity exists and can be linked to a legacy social identity associated with a natural or legal person.[a]
Metadata	Other attributes or personally identifying information (PII) needed for Know Your Customer (KYC).

a European Commission, Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transaction in the Internal Market. See http://ec.europa.eu.

take appropriate action to prevent it from registering. Through this *de-duplication process*, the uniqueness of each record in the NIR is assured.

A de-duplicated identity is then subjected to several procedures for vetting, proofing, and linking to the claimed social or legal identity. These use the validation and identity metadata collected at the time of enrollment. Here, an identity examiner analyzes the social footprint of the claimed identity by examining evidence from breeder documents as well as by cross-referencing

FIGURE 5: Schematic of the Identity Registration Process Using Biometrics



Source: World Bank analysis.

Note: The enrollment station at the frontend captures biometric data and the AFIS/ABIS at the backend de-duplicates that data to ensure uniqueness of each record in the identity repository.

with other external databases, including property registers, voter registers, civil registers, and police records. When the examiner is satisfied that the identity is real and is linked to a socially existing identity, it may be issued a Unique Identification Number (UIN)[19] and is added to the NIR. From there on, this identity is fixed and is bound to the NIR for life.

The process of data capture (enrollment), vetting, and validation (certification) completes the registration process of identity. An identity registered in this way is an official identity.

II.4 Issuance: Providing a Credential

i. Non-Electronic Credentials

Before a registered identity can be used (asserted), it first has to go through a credentialing process. In traditional identity systems (non-eID), this involves the issuance of a proof of identification in the form of a printed ID document that is linked to the bearer through a secure mechanism of *personalization* (e.g., a photo of the owner, or a description securely printed on the document) and carries a hallmark of trust in the form of some physical security features (an official seal, a hologram, etc.). Depending on the degree of trust implemented by the issuing agency, this ID becomes more than just a badge; it becomes a secure identity or a *credential*.

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 was impractical. Hence, it provided a general-purpose mechanism for meeting society's identification needs (supported many Use Cases).

However, as the need for identity management has shifted online, this credential has proved to be inadequate, and the process of credentialing eID has consequently become more involved than simply printing and issuing an ID card.

ii. The Credential Medium

For our purposes, a credential is a mechanism, process, device, or document that unequivocally vouches for the identity of its bearer through some method of trust and authentication.[20] This encompasses the specific form of eID credential (as discussed in item iii. below), but it also allows for other means. This is necessary because other traditional forms of credentials are likely to remain in operation for a long time to come, and hence the eID credentials may not be the dominant framework of identity trust during this transition. **Table 4** compares a range of options.

The choice of the credential medium has important implications for overall identity system architecture, operations, Use Cases, and cost. These are all factors that have to be considered in deciding what form of credential is ultimately to be carried by a country's population.

- **Non-Electronic ID Cards:** These continue to be the least expensive but also the least reliable form of identification. The information printed on them could be vulnerable to sophisticated alterations, counterfeiting, cannibalization, duplication, and substitution attacks, unless costly physical security features are implemented. But more importantly, they are largely unfit for electronic commerce, as they have no provisions for carrying a digital credential or interfacing with a digital certificate and hence cannot be used to secure transactions online. Simply said, these are badges and not secure electronic IDs that can be integrated into secure point-of-sale terminals or online electronic commerce engines.

- **Smartcards:** These emerged in the last twenty years as an alternative to printed ID cards because, as fraud grew more sophisticated, the integrity of identity documents could no longer be guaranteed through advanced printing technology alone. Smartcards, through the use of encryption and digital signature, are able to ensure that data on the ID credential was recorded by the authorized issuing agency and not altered subsequently and they are capable of carrying the digital identity credential of the bearer, as

[19] The quest to attribute a unique number to each identity is not new. It goes back to the end of the 19th century when Dr. Luis Almandos, in Argentina, lobbied to issue each citizen a unique number based on the Dactyloscopic analysis of their fingerprints (manual fingerprint classification). What is new is the fact that the technology to achieve uniqueness exists today in the form of multi-biometric ABIS systems. India's Aadhaar was the first example that showed the scalability of multi-biometrics for the purpose of producing unique ID numbers for hundreds of millions of people without any practical impediments.

[20] In a world where traditional identity and eID co-exist, we take a broader definition of a credential.

TABLE 4: Types of Credential Mediums Used Traditionally and in eID Programs

Credential Type		Description
Non Electronic	Printed ID Cards	Produced through a variety of printing technologies, including dye sublimation, laser engraving, and digital offset printing, and made resistant to fraud by adding a myriad of physical security features. These include special inks, lamination, optically variable devices, overlapping data, redundant data, forensic features, etc. Personalization is what binds it to bearer. When the printed ID card is equipped with a data pointer stored, for example, on a magnetic strip or quick response (QR) code and supported by back end identity services, this becomes an electronic ID (see ID in the Cloud below).
eID	Smartcards	A form of eID carried on a standard-size ID card. Offers advanced security features, since it can hold digital credentials and biometrics data on a chip that can be used for strong authentication to ensure that the holder of the card is the same as the authorized identity. This is a more secure and privacy-assured method, especially when the credential-certificate pair is generated onboard the card and the credential never leaves the chip. The certificate is exported to a CA directory. They come with different interfaces: contact, contactless, and near-field communication (NFC).
	SIM Cards	Mobile-based eID carried on a mobile communication device, such as a smart phone with a digital credential. Similar comments as to Smartcards credential-certificate pair apply (albeit different in detail, since security mechanisms are different between the two).
	ID in the Cloud	Certificate as well as biometrics stay on the Identity Server at the NIR. Authentication happens through biometrics first, then the certificate is used to secure authorized transactions. This does not necessarily require a physical credential. An ID number is sufficient, although that number can be stored on the magnetic strip of a printed card or a QR code.

discussed above. In the past, their cost and their requirement for a complex IT environment were the principal criticisms against them. Use of smartcards requires the development of a new service delivery and distribution platform. Today, several countries have adopted smartcards to support eID and there is a tremendous body of available worldwide experience. However, smart mobile phones have emerged as an alternative to smartcards, as mobile phones seem to provide a widely-available medium for carrying credentials and for asserting identity.

- **Mobile Devices:** Smart mobile devices have a great number of advantages that go beyond their high penetration into society. They have powerful computing, communication, and secure storage capabilities, both on subscriber identity module (SIM) and off SIM. They can hold digital credentials, which can be conveniently asserted in the course of mobile transactions, assuming there is an appropriate mechanism of authentication in operation. Nevertheless, while they are very promising, the standards have not yet been established for how these devices could deliver *fully trusted interoperable identity*. There are several groups working on such standards and, in view of the significance of this platform in the mass market, further developments are expected with a potential for participating in identity management for mobile commerce.[21]

In addition to the need for standards for interoperability of identity, mobile devices lack strong authentication mechanisms. Currently, a PIN or a password may be used to authenticate an identity carried on a

[21] See for example the FIDO Alliance http://fidoalliance.org, and the Identity Ecosystem Steering Group http://www.idecosystem.org.

mobile device. This may be adequate for many purposes but may not be strong enough for high-value transactions or for those in which the requirement of non-repudiation is present. For these, two-factor authentication or biometric readers incorporated into mobile devices present alternatives. This is starting to happen. The world's top two makers of smart mobile devices have incorporated fingerprint readers into their offerings.[22] In such a case, readers would likely be able to interoperate and offer strong biometric-based authentication. A useful feature of mobile devices is that they do not require a new token, in contrast to smartcards, and hence mobile devices offer good convenience to consumers and potentially significant cost benefits in identity issuance.

- **Non-token Credentials:** Future eID is likely to include a mobile component. But several interoperability and security aspects require attention for mobile identity to represent a dominant form of eID. In the meantime, there are other non-card-based options that do not require a new token in the hands of the consumer. For example, the NIR could develop an identification-on-demand or identity authentication service. Identity can be asserted and verified via the cloud (i.e., Internet) from any computer, terminal, or device with a biometric reader securely connected online. India has demonstrated that identity over the cloud is a viable option.[23] In fact, instead of investing billions of dollars to equip each individual in the country with a physical card (which could cost US$3 to US$5 per person), the government decided to invest in the ICT infrastructure at points of service throughout the country to ensure their connectivity to the backend identity services of the Aadhaar system. Of course, identity on demand has challenges of its own. It can primarily succeed if strong measures to protect privacy and data security are adopted and enforced, and a robust communications infrastructure is available for online identity.

iii. eID Credentials

Under eID, credentialing involves the use of a public key infrastructure (PKI) framework, or other alternative frameworks, for encryption and digital signature, in order to establish a trusted mechanism for securing electronic interactions between two entities. In this case, once an identity has been registered, it is also issued two additional digital assets, namely a public and a private key,[24] which are securely bound to the identity.[25] The central authority managing the NIR serves the function of a Certificate Authority (CA), which the authority either operates on its own or outsources to one or more third parties, including to the private sector. The public key is packaged with some identifying information (name, UIN, use restrictions, etc.), which is digitally signed, and is issued as an *eID Certificate,* and is henceforth kept in the public key directory (PKD). The private key is secured though an appropriate access control mechanism so that it can only be used by its rightful owner. For example, (strong) authentication could be implemented, which would require a PIN, two factors, or a biometric match, before the private key could be released for use by the owner. Thus a private key secured through an authentication mechanism becomes an *eID Credential.*

To guard against impersonation, it is imperative that the owner maintains total control over his or her digital credential. Given the importance of this, the questions concerning where the eID credential is generated, during what step of the process, where it is kept after generation, and how it is secured are crucial in order to maintain trust in the overall framework. The security details are beyond the scope of this report, so here we shall simply

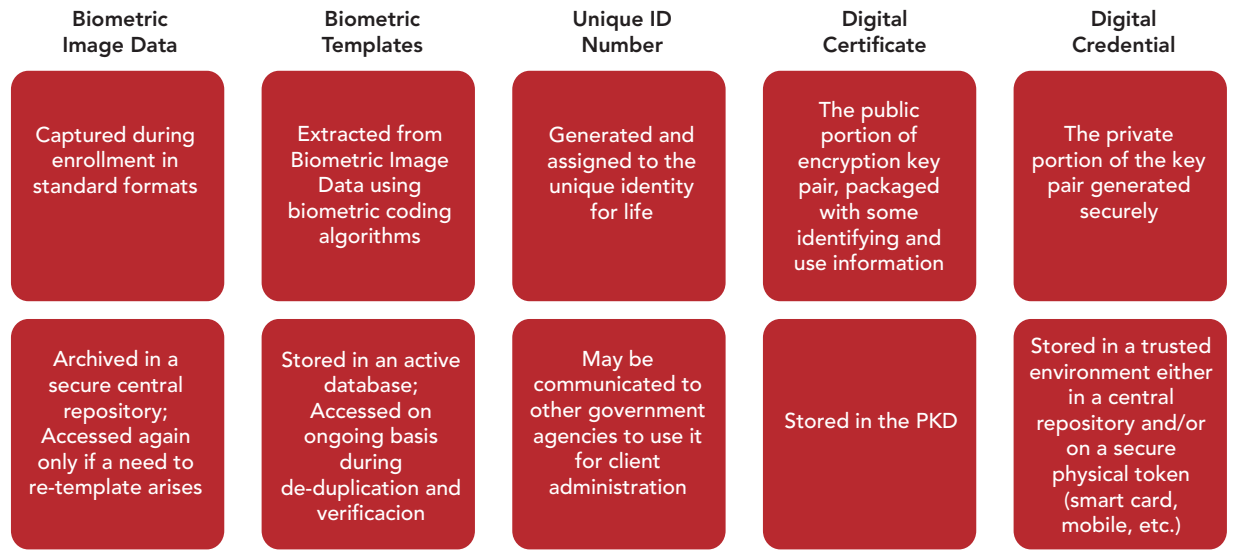
[22] Both Apple Inc. iPhone 5S and Samsung Galaxy S5 feature a fingerprint reader in order to control access to the device. These are not fully interoperable and hence do not provide the type of fingerprint authentication needed to turn the mobile device into a national eID but it is a first step towards this eventuality.

[23] See Unique ID Authority of India http://uidai.gov.in for more information on the success of authentication services for the Aadhaar program.

[24] To understand the nature of these two assets, it is crucial to know how public key infrastructure (PKI) works to secure interactions. At a very high level, PKI is based on the use of a pair of encryption keys: one is public and kept in a public key directory (PKD) managed by a trusted Certificate Authority (CA), while the other is private and is controlled by its owner. An individual's public key can be used by a sending party to encrypt a message so that it can only be read by that person using their corresponding private key for decryption. Similarly, the owner of a private key can use it to digitally sign a message such that, when decrypted using the corresponding public key, the receiving party is assured that the message originated from that and only that person.

[25] Mechanisms for generating certificates and credentials securely are complex, since they depend on whether these are issued in the central facility or on the medium (such as smart or SIM card) directly. We will simplify the discussion by glossing over the subtleties.

FIGURE 6: Digital Assets Associated with an Identity in an eID System



Source: World Bank analysis.

assume that a master copy of the identity credential is kept securely in a trusted environment at the NIR and that a trusted copy of it (digitally signed by the issuing authority) is kept on some medium or token, which constitutes an assertable credential. We discuss different forms of credentials next. **Figure 6** gives a summary of all the digital assets associated with an eID.

In summary, we now operate in a technology regime where identity can be unique, certified, and digitally credentialed, yet the options for what physical credential to use are multiple. We believe 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.

II.5 Use: Authentication and Updating of an Identity

Once an identity has been registered and issued a proof of identification, several Use Cases can be envisioned, in both the public and private sectors, as highlighted in **Figure 7**.

These Use Cases illustrate how eID can help improve the lives of the poor in developing countries, as demonstrated by the following examples.[26]

- **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 employment, crop failure, or to raise capital to start a small business. Mobile phones, automated teller machines (ATMs), 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.

- **Preventing fraud:** Digital identities can help plug the leakage of funds and prevent fraud in government programs. For example, in India, an audit of muster rolls of the National Rural Employment Guarantee Scheme found 8.6 percent ghost beneficiaries, 23.1 percent ghost person days, and only 61 percent of wage payments reaching eligible workers.[27] Paying

[26] Randeep Sudan, "Using Digital Identities to Fight Poverty," (2013) at http://blogs.worldbank.org/ic4d/node/593 (last accessed May 10, 2014).

[27] National Institute of Public Finance and Policy, "A Cost-Benefit Analysis of Aadhaar," (2012) at http://planningcommission.nic.in/reports/genrep/rep_uid_cba_paper.pdf (last accessed May 10, 2014).

Data is Pervasive in eID

eID systems are heavily data-centric: they consume data and they generate it. During registration, enrollment data is collected, transmitted, stored, and archived (upon death for example); but that is not all. Every time an eID is asserted by its bearer, it generates usage and transaction records that can accumulate in audit trail databases, controlled commercially or by government institutions. As such, the management of identity has gone from the issuance of ID cards in the past to the management of databases of large amounts of personally identifying information, and this data will only continue to grow as more eServices rely on eID and eID becomes more pervasive.

Add to this the massive amounts of unstructured data that is accumulating online and on social media. In this way, one can see that we are heading towards a regime in which massive amounts of data are digitally available concerning people, their actions, and their reputations; all of this is linked through a reliable, unique, and traceable eID. These databases are likely to become key for organizations seeking to perform identity or entity resolution, identity harvesting, and reputation discovery, as well as other identity intelligence and analytics for the purpose of developing interest or risk profiles (targeted marketing or security risk assessment).

The implication of this growth in data is that, increasingly, identity will be defined based on data external to the enrollment process, such as vetted social résumés (community vetted self-declarations), open-source reputational data, as well as from audit trails of use of eID. This situation could raise major concerns, the severity of which may vary according to each country, its policy and laws, and regional differences. Significant discussions are taking place around the world related to how to address this potential mega-data problem. These include use of Privacy Enhancing Technologies (PET), distributed databases, match-on-card, improved notice and consent provisions, as well as frameworks of trust that manage identity alongside anonymity. See Section III below for further discussion.

beneficiaries and workers electronically introduces enormous efficiencies and prevents loss of funds. In Nigeria, biometric audits resulted in a reduction of 40 percent in the number of federal pensioners.[28]

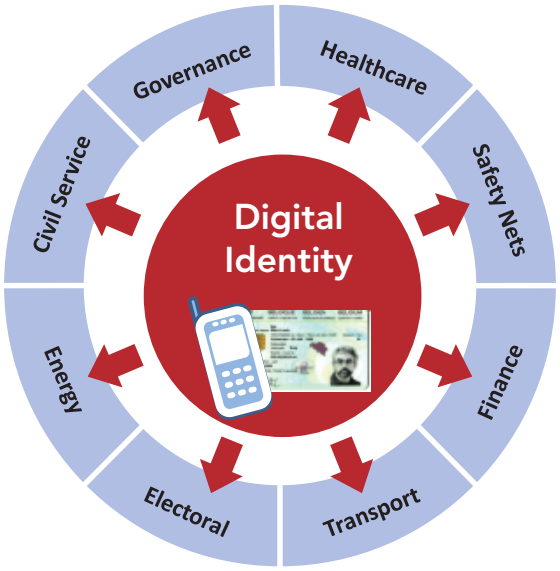
- **Enhancing women's incomes:** A digital identity can ensure that benefits meant for women, such as conditional cash transfers, actually reach women. According to the International Labor Organization (ILO), women contribute 70 percent of working hours globally, but receive only 10 percent of income flows.[29] Thirty out of the bottom 40 percent 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 women is spent on nutrition, education, and clothing for the family, directly impacting poverty.

Creating a nationwide authentication infrastructure is a gargantuan task. Such an infrastructure consists of: portals for online authentication; mobile applications for mobile-based authentication; POS terminals for smart card- or mobile phone-based authentication; and biometric terminals for biometric-based authentication, to name a few. Both a country's government agencies (such as driver's license issuing centers, healthcare service providers, and passport issuing centers) and its private firms (such as banks and airlines) rely on authentication as e-government and e-commerce applications continue to grow around the world.

[28] Gelb and Clark (2013).

[29] The Guardian, "Is Empowering Women the Answer to Ending Poverty in the Developing World?" (2013) at http://www.theguardian.com/global-development-professionals-network/2013/mar/26/empower-women-end-poverty-developing-world (last accessed May 10, 2014).

FIGURE 7: Sample Use Cases of Digital Identity



Public Sector
- Driver's license
- Passport
- Healthcare
- Safety nets
- Taxation

Private Sector
- Financial Services
- Business Registration
- Property Registration
- Transport Services
- Mobile Transactions

Source: World Bank analysis.

Authentication requires iron-clad provisions for fraud protection and high reliability and necessitates additional considerations in the 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 in terms of authentication. Digital authentication, when achieved through PINs, passwords, or SIM cards, relies on the inherent ability of these mediums to change. For example, in the event 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.[30] Related to such risks is also a determination of liability. In traditional authentication, the organization issuing the service, such as a financial service provider, assumes sole responsibility and liability for wrongful authentication or for misuse of digital information, such as a PIN or password. In cases where 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.

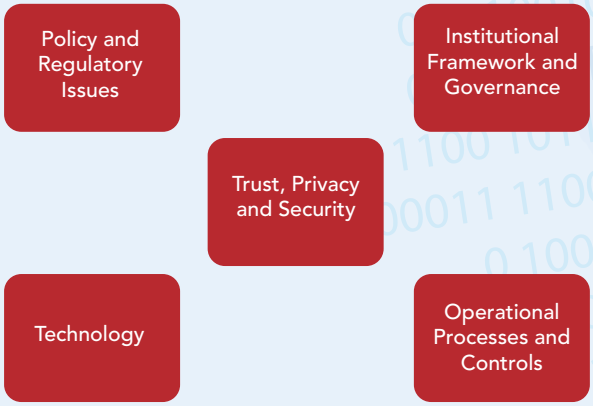
[30] Mitigation measures may involve using advanced technology to ensure that biometric templates are dynamically generated from a live person, instead of from a stored file, which may have been injected by a fraudulent event.

III. Developing A Digital Identity Program

As discussed in Section I, digital identity is an important infrastructure for any modern society. As such, it is the government's responsibility to assure the development of robust, secure, and comprehensive programs that are capable of meeting the country's identity needs, now and for the foreseeable future. Setting up the correct identity program is a complex process with risks and challenges. Luckily, the worldwide experience in this domain is now rich and can supply lessons learned on how to develop an economically viable and a risk-managed eID program. Based on this body of experience, we will highlight in what follows the types of decisions that policymakers should expect to make; furthermore, we will identify the more critical components that have to be established in order to launch an identity program on a national scale.

Before a government commits to an eID program, it should conduct an assessment of identity management within the country, in the context of its cultural, political, economic, and development landscapes, to determine a go or no-go decision on eID. The analysis may include an examination of the Use Cases (such as healthcare, safety nets, or financial services) to be considered for eID; user eligibility (determining, for example, what groups are eligible for eID: citizens, residents, foreigners, etc.); and the feasibility of safeguards for human values in the country's then state of development. Once a go decision is supported by such an examination, the government can implement the steps needed to realize eID in the country.

FIGURE 8: The Functional Building Blocks in an eID System



Source: World Bank analysis.

In discussing the overall framework of eID, the issues that arise can be grouped under five functional building blocks (see Figure 8).

III.1 Policy and Regulation

The first step is the adoption of a vision, at a Cabinet level, for the pathway towards a national eID. At this stage two distinct options emerge:[31] a top-down or a bottom-up approach, as discussed in Section I and summarized in **Table 5**. There are pros and cons related to both approaches and a decision can only be made after careful analysis of the fact patterns specific to the country's

[31] In this Section, we use the terminology of Gelb and Clark.

TABLE 5: Pathways to National Identity Depending on What is Developed First

Development Priority	Description	Advantages/Disadvantages
Foundational to Functional	**Top-down identity regime**: A country first develops a general-purpose identity platform, which is designed to support all the identity Use Cases expected down the line. It focuses on the enrollment under the framework of "enroll once and be identified for life." The expectation is that, once identity becomes a supplied commodity, an entire ecosystem of applications, not even imagined initially, will emerge; as such, this approach views eID as a true general-purpose infrastructure. **Examples**: India, Nigeria, Malaysia, Pakistan, South Africa, Kenya.	**Advantages:** • A true infrastructure for the country. • Aligned with national vision of the country. • Avoids multiple registration and redundancy. • Supports many Use Cases and innovation. • Provides economies of scale. **Disadvantages:** • Requires multi-stakeholder coordination. • Slower to launch and take up, since immediate applications may not drive it. • Requires sustained political will. • Could be vulnerable to changing governments. • Could potentially be more costly initially. • Development returns are realized on adoption and use.
Functional to Foundational	**Bottom-up identity regime**: A country begins with a system that addresses the needs of a very specific application of identity (e.g., identification of vulnerable populations or healthcare recipients). Over time, such a system can evolve and merge with other functional programs, then migrate towards a universal identity regime in phased steps. **Examples**: Ghana, Ethiopia, Afghanistan, Colombia, Venezuela, Vietnam.	**Advantages:** • Easier to launch without multi-stakeholder coordination. • Lower initial cost, since focused on one specific application. • Faster adoption, since driven by a champion and an immediate application. **Disadvantages:** • Difficult to evolve to multisector foundational identity in the long run. • Prone to creating fragmented identity space, with multiple overlapping and incompatible identity systems in a country. • More costly to add additional applications. • A higher level of inconvenience to people, since they may be required to enroll multiple times in multiple programs.

needs, timelines, budgets, political will, institutional readiness, cultural and demographic composition, the state of the legacy civil registration system (birth registration), and the government's overall vision relative to the role of identity. In Section I, we mostly discussed the foundational approach; here we compare the two.

Generally speaking, the biggest risk of a functional approach is fragmented and overlapping, or, even worse, incompatible identity systems, which can be costly to harmonize down the line. International standards could be used early on to mitigate such risks and to improve the odds that the multitude of functional systems will interoperate down the line. In practice, we have yet to see this approach succeed on a large scale. Functional programs are typically focused on serving the immediate needs of the ministry that is driving them, and their success is not necessarily measured in their theoretical ability to work with other external or national systems many years down the line. Nevertheless, functional approaches have some advantages: often, a single government agency presents a clear and immediate need for identification and acts as a driver and a champion for the system from day one, which improves the chances of success. This advantage of the functional approach is in contrast to the foundational one. A foundational approach requires sustained political will during the initial enrollment phase to encourage take-up and participation by the population in the absence of clear Use Cases at that early stage. Assuming that this can be achieved, the foundational approach offers more

TABLE 6: Legal and Policy Matters that Need to be Investigated in Planning an eID Program

Area of Inquiry	Goal	Issues to Investigate
Legal Authority	*Determining if there are any legal show stoppers to proposed identity system*	• Does the government have the appropriate authority to implement each of the tasks under the proposed eID program, including requiring its people to provide personally identifying information such as biometrics? • What are the boundaries of authority when it comes to collecting, storing, archiving, accessing, using, disposing of, and modifying identity data? • Does paper identity equal electronic identity? • Which authorities can collect identity-related information? • What legal protections are afforded for validation or authentication, including with use of biometrics?
Protections of Rights of People	*Establishing what is required to earn the confidence of the population*	• Identity bill of rights. • Privacy rights. • Data rights and ownership. • Anti-discrimination. • Anti-surveillance. • Recourse for abuse.
Pro eID Policies	*Leveraging enabling policies to promote eID*	• Recognition of eID as a new legal category. • Use of digital signature. • Policies that promote eID as a trusted platform for interactions between people and their government, as well as for general trusted commerce. • Long-term ICT development policies.

attractive benefits. For example, it provides a universal infrastructure that can encourage innovation in uses and can be leveraged over time to address an ever-increasing number of applications, hence achieving an economy of scale, even if the development returns may be slower.

Once a vision for a national eID is established, a comprehensive legal assessment is needed to clarify the current situation and to identify gaps in the three basic areas of inquiry, listed in **Table 6**. In most countries, existing legislation that would impact identity and eID is scattered throughout many different legal acts and regulations—including those pertaining to electronic communication and commerce, electronic signature, data protection, and privacy—market regulation laws, and even the constitution. Many of these legislations may have to be amended and new laws may have to be enacted to fill in identified gaps.

Ultimately, for eID to realize its adoption potential, it should be based on a sound legal environment, but it should also ensure that it is a safe and secure means for transacting with adequate provisions for ensuring the privacy of consumers. Building trust with the public will go a long way in allowing this new form of identification to be adopted and used. We discuss this topic in further detail under the section of Trust, Privacy, and Security below.

During the legal review, attention should be given to the broader ICT policies and regulatory environment. eID is an integral element of ICT and could benefit from policies that aim, in the long term, to promote modern and effective ICT infrastructure in a country. For example, policies that aim to provide more connectivity and online access to everyone, improved digital education and training, and incentives for the private sector to participate in the development of ICT infrastructure in the country could also positively affect eID development.

III.2 Institutional Framework and Governance

i. Institutional Arrangements

Though identity management benefits several governmental agencies, especially when it comes to functional

TABLE 7: Possible Institutional Arrangements for the National Identity Authority

Organizational Type	Examples
Autonomous with Direct Cabinet- or Executive-Level Reporting	• **India**: the Unique Identity Authority of India was set up as an organization attached to the Planning Commission of India, reporting into a Chairman who has the stature of a cabinet minister. • **Ghana**: the National Identification Authority of Ghana was set up as an organization within the Office of the President.
Autonomous Governed by a Board Representing Stakeholders	• **Nigeria**: the National Identity Management Commission (NIMC) was established as a Commission through an Act with the mandate to establish, own, operate, maintain, and manage the National Identity Database, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to those registered individuals, and to harmonize and integrate existing identification databases in Nigeria. It is governed by a board of 18 individuals representing different government agencies and stakeholders. • **Pakistan**: the National Database Registration Authority (NADRA) is an independent, constitutionally established institution that manages the country's identity registration database.
An Agency or Directorate of an Existing Ministry	• **Indonesia**: Population Administration Directorate in the Ministry of Home Affairs. • **Argentina**: Registro Nacional de las Personas (RENAPER), is a directorate under the Ministry of Interior and Transportation.

programs, developing countries pursue different institutional models for developing foundational identity in a country. Which government agency takes responsibility for implementing digital identity and how the distribution of responsibility is shared across government agencies is determined by policy, legislation, and institutional capacity, among other factors.

To start with, appointing a national organization to coordinate the development of a country's digital identity is beneficial. Such an organization should be empowered through law and political will, and should demonstrate the capacity to serve as a national champion and an effective implementer. We will generally refer to such an organization as the *National Identity Agency* (NIA). At a high level, the NIA is a central government body mandated with implementing the vision and mission of the National Identity Register (NIR), as discussed in Section II. The agency manages, shares, secures, and facilitates the use of information related to eID of citizens and of eligible residents. Several options exist for the institutional arrangements of the NIA, as presented in **Table 7**. These include an autonomous body reporting to a cabinet-level minister or to the executive, an autonomous organization governed by an independent board representing the stakeholders, or a directorate within an existing ministry. Additional institutional models, including with PPP, can be envisioned.

ii. Institutional Roles: Scope of the NIA

The scope of the NIA's mission requires a careful review. Identity systems involve the collection and management of sensitive data pertaining to a country's population. Hence, the responsibility of the NIA should be clearly defined, and should be balanced and managed with the aid of other government agencies, the private sector, and the identity stakeholders. Strong provisions for the effective governance of the NIA should be put in place. At the highest level, five institutional roles need to be assigned for the development of a country's eID. These roles could be grouped, from a data-centric viewpoint, into three functions: collect, store, and use identity data, as shown in **Table 8**.[32]

Among those five institutional roles, the second is often attributed to the NIA and is considered to be its core mission, irrespective of the organization's other responsibilities. In this role, the NIA focuses on establishing population enrollment data standards, operating the backend systems for de-duplicating identity and ensuring its uniqueness, and for storing and protecting the consolidated identity information. In this case,

[32] As discussed in Section II, the collect function includes both capturing and certifying an identity. In addition, the use function includes authenticating and updating (or revoking) an identity.

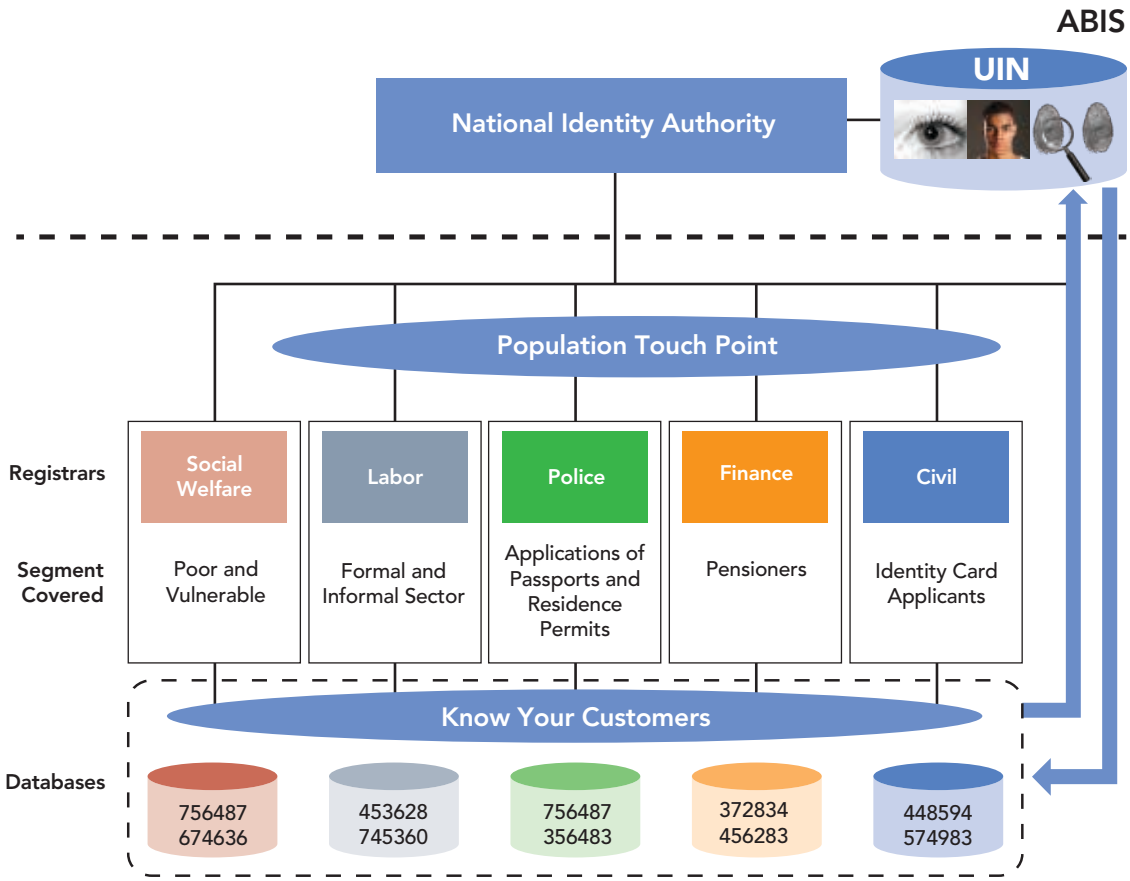
TABLE 8: The Institutional Roles Required to Affect a National eID Program

	Institutional Role	Possible Tasks
Collect	Enrollment Agency	• Establish enrollment centers around the country (fixed, as well as temporary or mobile field enrollment units) which people can visit to enroll their identity. • Mobilize the population, inviting them to come register their identity; or mobilize registrars to visit populations in their towns and villages to register them and collect information. • Capture the population's identity data into eID profiles.
Store	Central Repository	**Central Data Store:** • Establish, own, and operate the country's national repository for identity data. • Guarantee the uniqueness of individual identity through the deployment and operation of backend IT systems for the de-duplication of identity records, as well as through procedures for the adjudication required to resolve matches. • Attribute a unique number to each identity (UIN), where applicable, fixing an identity for life. • Secure and protect the population identity data against unauthorized access, corruption, fraud, and misuse. • Update/change/terminate eID profiles based on need. **Standards and Interfaces:** • Define the standards for enrollment data types and formats, quality, and processes related to the registration of eID profiles. • Define the pathway for total enrollment coverage (inclusive) of the entire population, either as a standalone organization or as part of a collegial cooperation strategy involving other stakeholders in the country's identity ecosystem ("the registrars"). • Establish the standards for identity vetting through links to the civil registry (birth and death registers) or through procedures for identity proofing. • Certify the registrars. • Set the standards and specifications for the ICT infrastructure required for secure access to the NIR for the purpose of identity verification.
Use	National Identity Card-Issuing Body (Optional)	• Personalize and issue physical National Identity Cards to every registered person. • Manage the National Identity Cards throughout their life cycle.
	Identity Service Provider	• Establish and operate a platform for identity verification and identification services that allows individuals to assert their identity and be authenticated online. • Assure the long-term value of the NIR by working with all government agencies concerned, as well as private sector enterprises (banking, healthcare, transportation, etc.) in order to meet their identity needs and to promote continued adoption of the platform.
	Credential and Certificate Authority	In the event that eID is built on PKI, this needs to be established or outsourced to private entities. • Issue eID digital certificates and credentials to each registered identity. • Establish and operate a Certificate Authority (or equivalent). • Establish and operate the identity directory.

the NIA is essentially a back-office organization; it can remain fairly small in its head count and is limited to a central head office.

Enrolling the population (as shown in the first institutional role above) can be done by *registrars*, following a national standard established in coordination with the NIA. The registrars can collect information from their customers, either in the normal course of their operations or as part of special mass-enrollment campaigns. There are broadly two models for registrars: they may be members of select government agencies, or members of the NIA. In the first model, government agencies may be selected to serve as registrars that have technical capacity and a distribution network throughout the population, such as the Civil Registry, the Ministry of Health, the Ministry of Social Welfare, etc. Based on an

FIGURE 9: Possible Institutional Framework Showing a Collegial Cooperation Strategy between the NIA and the Registrars

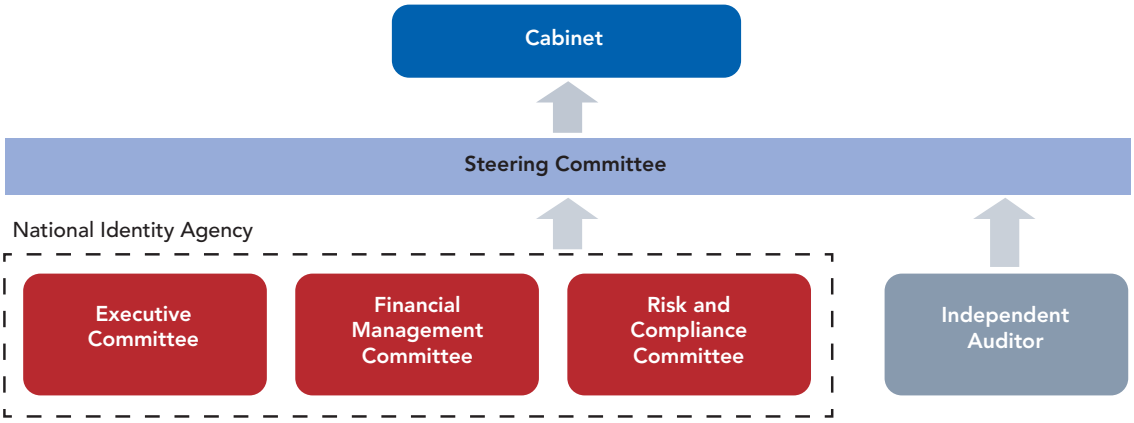


Source: World Bank analysis.

Note: For example, a Social Welfare organization could collect biometric enrollment data as part of its door-to-door poverty survey using the NIA standard. The survey data needed for establishing the poverty score of a household would be retained in the information systems of that ministry, while the biometrics, if collected, would be sent directly to the NIA for de-duplication, issuance of a UIN, as applicable, and registration of the identity in the NIR for use by any other approved application, including the ones run by Social Welfare.

established government policy, the registrar may collect information broader than the minimum set established by the NIA for its core mission. It could include data for Know Your Customer (KYC) purposes specific to the needs of individual government agencies. The registrar would submit only the core identifying data to the NIA, retaining the rest for specific KYC databases (see for example **Figure 9**). The coordination among registrars would be done according to the collegial cooperation plan for total enrollment coverage developed by the NIA. With such plan, several relevant government institutions can contribute to the data collection effort by leveraging their existing customer-facing infrastructures, including human resources, field offices, and ICT platforms. In the second model, the role of the enrollment agency is added to the NIA. Here, the NIA would have to build the geographical footprint required to achieve total coverage. In such a case, it would have to establish and operate enrollment centers or regional offices in addition to its central head office. This is obviously a different type of institution, and its establishment and management would require a more complex operating plan and a significantly higher budget. Of course, a hybrid model is also possible, where the NIA captures minimal data needed for its operations, while other government agencies capture their own data, on a different timescale or lifecycle, and maintain their own databases. These databases could be interlinked by a UIN. Additional scenarios may be considered; people

FIGURE 10: A Potential Governance Structure for eID at a High Level



Source: World Bank analysis.

may be expected to appear for registration at a registration office, or registrars may visit different towns and villages to register people and to collect data.

Equally important is the decision on how the roles pertaining to the use of identity are distributed. An organization may need to issue and manage national identity cards. In addition, the same or another organization may need to provide identity services that allow registered individuals to assert their identity and be verified or identified online. Lastly, for the eID to realize its full potential, digital credentials need to be managed. This means establishing identity services, as discussed earlier, and may include the establishment of a full-fledged CA, or equivalent authority, in support of the adopted institutional framework.

iii. Institutional Governance for eID

In a data-centric world, where eID uses and generates data, the role of any organization that deals with identity grows in importance over time, as more data accumulates and the dependency on eID increases. In order to maintain checks and balances over such organizations, a robust multi-layer institutional governance structure is needed.

One such structure is shown in **Figure 10** at a high level and consists of multiple specialized committees as follows:

- **Steering Committee:** This is a high-level oversight organization with representation from multiple identity stakeholders. It provides the strategic orientation for the NIA and is responsible for the development of eID policy. During the implementation phase, the organization ensures the supervision of the project roll-out. During the operational phase, it serves as the committee that sets the ongoing eID objectives, priorities, and performance targets, as well as determines the funding requirements and the business model. It evaluates the performance and supervises the utilization of funds. The body reports to the cabinet, a sponsoring minister, or the executive, on all matters related to eID and the country's identification requirements. The Chairman of the committee is typically appointed by the head of state (the president or the prime minister).

- **Executive Committee:** This is the body that sets the overall NIA strategy and objectives in line with the requirements of the Steering Committee and ensures that the organization delivers according to the strategy. It also sets accountability measures and controls within the organization. It consists of the most senior body of individuals within the NIA that are responsible for managing operations.

- **Financial Management Committee:** Oversees and manages planned capital and operational funding usage. Monitors the financial performance metrics for the NIA.

- **Risk and Compliance Committee:** Ensures that risks are identified, assessed, and mitigated in a reasonable and coherent manner for the whole program.

- **Independent Auditor:** This is a critical component of the NIA's institutional governance. It is typically put in place to ensure that the eID program delivers on its mission within the framework of the legal act that led to its creation, while respecting the applicable human and citizen rights. It is the body that enhances the trust in the organization and its independence has to be a high priority for the government.

The government may require a regulatory body to have direct oversight of the eID program's operational phase.

iv. Public Private Partnerships (PPPs) for eID

While the ultimate responsibility for the development of a foundational eID program lies with government, participation of the private sector can be helpful in securing implementation success and sustainability. The private sector is a user of identity programs, such as for banking or healthcare services, and is thus an identity stakeholder. Developing and implementing a well-functioning national program for eID requires significant technical expertise, which may be lacking within the government. The long-term viability of eID requires institutional efficiency, which can oscillate within a government agency over time. Private sector institutions can thus play an important role in balancing the government mandate of a national eID program while boosting operational efficiency. In addition, the private sector can act as a service provider, to which implementing government agencies could outsource some or all of their operations, on a competitive basis, including for data capture and office or project management. The private sector companies can also serve as suppliers of consumables (card stock, ink, smart chips, etc.), equipment (computers, biometric scanners, cameras) and can be system integrators or total solution providers. They can play a role in the longer-term operations and maintenance of the eID program for the government.

Given the nature of an identity issuance operation over the long term, a national eID program could be structured as a PPP. Within this model, the private sector players could seek to participate in the investments required to put in place the necessary infrastructure and solutions for eID, in order to register and issue credentials to the population. The public and private entities could decide on a model for the return of investments made by the private sector, including through a per-card charge,[33] as identity cards are issued over a long contract period, or through charges for identity services.

In order for PPP schemes to attract private sector participation, good policy and credible incentives are needed to offer an enabling environment with a level playing field, a competitive marketplace, and a deterministic model for the return of investment.

III.3 Technology

An eID system is built by putting in place several technology solutions. Technology strategy thus plays a crucial role in the development of eID in a country; dimensions that come into play include cost, capacity, interoperability, usage, security, privacy, and long-term viability.

As discussed in Section I, an eID includes several technology-based solutions:

- **Biometrics:** Biometrics offers the technology to uniquely identify or authenticate an individual by electronically capturing a face photo, fingerprints, or an individual's iris.

- **Electronic databases:** Electronic databases offer a way to electronically store identity data and make it available for online or mobile usage. Electronic storage of identity data also allows data to be recovered when faced with natural or man-made disasters.

- **Electronic credentials:** Electronic credentials, such as smartcards or mobile phones, offer a way to electronically authenticate the identity of a person for in-person, online, mobile, or offline services.

[33] For example, in the United States, Departments of Motor Vehicles in different states establish long-term contracts with private sector companies (typically five to 10 years in length). These companies put in place systems to issue drivers' licenses at their own cost and they, over the period of the contract, return their investment from the per-card charge they are allowed to keep as part of the overall fee they collect from the applicant. The rest of the fee is given to the state. These PPPs have become very successful revenue centers for the states.

- **Mobile, online, and offline applications:** Digital applications, when linked with eID, offer new products and services to consumers, available in-person, online, offline, or via mobile.

An important part of the technology strategy is an assessment of a country's underlying, enabling technology infrastructure. High-speed Internet is often a necessary requirement for an online identity solution. Many developing countries, particularly in Africa, are still working to develop and deploy high-speed Internet. The degree of penetration of smart devices in a country—in the form of smartphones and tablets—determines the potential for mobile identity and mobile applications. A strong domestic IT industry is needed to provide the human capacity and the products and services that can benefit from digital identity. Electronic banking and financial services require the availability of a financial infrastructure—such as a national payment system, POS devices, ATMs, agent networks, and payment networks—to benefit from eID.

A determination also has to be made as to whether an online or offline mode of authentication is to be adopted. An online approach offers a higher degree of robustness and reliability, but also requires a more robust communications infrastructure. An offline approach offers greater flexibility, especially in remote and rural areas, though it poses potential gaps in reliable authentication and suggests some costs for proliferating relevant credentials for offline use.

Many of the technical components revolve around identity data, including technology for capturing, encrypting, transmitting, storing and using this data to identify and verify the identity of individuals. In this section, we present an overview of some of the more critical technology elements in this field as we highlight the choices that lie ahead and consider the importance of creating the right environment, in which technical and vendor dependencies can be effectively managed.

i. Creating the Identity Ecosystem: Mitigating Network Effects

A first step in the technology strategy for eID is to design an open architecture platform that protects against lock-in due to a specific vendor or technology.

> In selecting a solution, the overall identity system should work with any mix of equivalent components from different suppliers. The implementing agency should be able to easily replace backend matching engines, biometric capture devices, or any other elements seamlessly, without jeopardizing the operations of the overall system. Systems should be based on open standards at all levels—biometric or IT.

An identity system has to be based on a design that is flexible enough to meet the country's needs into the foreseeable future, independent of the vendor that initially delivered the solution and the specific technology upon which it was built.

Vendor and technology lock-in is an important consideration, since identity systems tend to develop a *network effect*, i.e. they increase in size and value as more people enroll and more governmental and non-governmental programs depend on them. This dependency—whose effect is often seen at the time of contract renewal, in the form of the incumbent or legacy system advantage—makes it harder (or more costly) to migrate from one vendor or technology to another.

In order to protect against such risks, the implementing authority needs to ensure that its identity system is "vendor neutral" and "technology neutral," by putting in place a set of design elements for the architecture, a sample of which is provided in **Table 9**. These are intended to be applied as requirements during the procurement process.

The ultimate goal is to promote the emergence of an *identity ecosystem* in the country, which allows many vendors, products, solutions, and technologies to continually compete on features, performance, and price. Identity is an important national asset and it needs to be served by a healthy and robust market that offers choice, rather than by one that is dominated by a single or a handful of vendors. Devising a prudent technology strategy should be a priority for any country that sees identity as an infrastructure to be protected through informed regulations.

TABLE 9: Ensuring the eID System is Open and Does Not Suffer from Vendor Lock-in or Technology Lock-in

Requirement	Description
Modularity and Open Architecture	The total solution should be built as a collection of modules, or subsystems, each performing a well-defined identity task and having an open interface. In the language of Service-Oriented Architecture, the modules represent specialized services that are easy to orchestrate into total solutions using standard IT integration and open architecture methodology. **Applicable Standards:** • All communications between modules should be subject to accepted international open interface and security standards, as specified in ISO/IEC 7498 family and the standards referenced therein.
COTS, Scalability, Reliability, and Availability	• The hardware and IT platform should be based on Common Off-the-Shelf (COTS) modules, including computer servers, storage devices, and all ICT components. • Scalability: the system should be designed to easily scale up for national coverage through the straightforward addition of more hardware and software. • Reliability: the system should be reliable, with high-quality performance and minimum or no down-time. • Availability: the system should be easily available for coverage in urban and rural centers. • The implementing agency should be able to second-source every element (i.e., procure each element from multiple vendors).
Certified Biometric Capture Devices	Biometric capture devices, if used, should be certified for image quality and should have standard interfaces to allow for their plug-and-play interchangeability. **Applicable Certification:** • US FBI Appendix F for livescan 10-print fingerprint scanners or its equivalent US NIST Mobile Profile 60. • US NIST Mobile Profile 45 for two-print fingerprint scanners. • US NIST PIV for single-finger scanners. **Applicable Interfaces:** • BioAPI standard family (ISO/IEC 19784, 19785, 24709, 24708, 29141).
Standard Identity and Biometric Data Formats	• Identity data should be in a format based on the internationally accepted standards for electronic data exchange. • No portion of the data should be proprietary or vendor-encrypted, and all data should be accessible (reading, writing, querying, etc.) through standard IT protocols without vendor intervention. • The biometric data, if used, should be stored as raw images (compressed for transmission, as allowed by the standard) from which the proprietary templates of any algorithm can be generated. Having the biometric image data ensures that migration to a new vendor template is possible. • On smartcards, if used, proprietary 1:1 verification templates should be avoided; instead the interoperable template format (so called MINEX template) should be used. **Applicable Standards:** • Biometric data formats: ISO/IEC 19794 (parts 1 to 10) or the equivalent US ANSI/NIST-ITL-1-2007 and 2008. • NIST INCITS 378 for verification template interoperability (so-called MINEX certified).

ii. Linkage with Civil Registry or Use of Biometrics

One of the important requirements of an eID system is to establish the uniqueness of an identity before it is issued a credential, if any. There are a couple of ways in which this can be achieved:

- Verification of uniqueness of entries in civil registries; or
- De-duplication using biometrics.

The first method uses a set of controls and procedures for civil registration to ensure that every birth is well-documented as early as possible. A robust civil registration process can link each individual to a unique entry in the register. Given the state of civil registration in many developing countries,[34] establishing uniqueness by

[34] UNICEF reports that up to 40 percent of children are not registered at birth in developing countries (compared to 36 percent worldwide). "*The 'Rights' Start to Life: A Statistical Analysis of Birth Registration.*" New York: The United Nations Children's Fund, UNICEF 2005.

TABLE 10: Factors to Be Considered in Selecting a Biometrics Set

Criteria	Description
Accuracy	Provides adequate 1:N accuracy such that each individual can be identified unambiguously from the population. This is the resolving power of the biometric set. The more biometric data is available, the higher the resolving power.
Inclusion	Ensures that everyone is able to provide some biometric sample, including those that represent challenges for certain modalities (e.g., children, manual laborers, or amputees that typically challenge fingerprints) but seem to be fine for face or iris scans.
Flexibility	Necessary to support the diverse Use Cases during the lifetime of the program. For some applications, fingerprints are ideal (mobile), while for others it may be face or iris (electronic gates).

relying exclusively on civil registration may not be feasible. Governments may have to heavily invest in digitizing historic civil records, capturing future civil information electronically, and establishing the institutions, systems, and processes for a civil registration system to efficiently function. The second method, as given by biometrics,[35] offers an alternative to the civil registry and can be instrumental for establishing uniqueness and for the de-duplication process, as was described in Section II.

Governments may consider establishing a strong civil registration program, or using biometrics for identification. Both options present pros and cons. In the case of developing countries, especially in Africa, biometrics offers an attractive way to expeditiously enroll, register, and authenticate people, and allows a country to develop a reliable and robust identification system, albeit one that comes with important considerations of cost, capacity, security, and privacy. Governments aiming to pursue a civil registration route should consider a detailed strategy and implementation plan.

In case the government decides to use biometrics for identification, the type of biometrics most suitable for the program needs to be determined. Note that biometric technologies are used not only for the de-duplication process (1:N matching), but also for authentication (1:1 matching), where a claimed identity is verified at the time it is asserted or used. Today, the three most mature and effective types of biometrics that can be used, both for 1:N and 1:1 matching, are: fingerprints, the iris, and the face.[36] In practice, a multi-biometric strategy (as opposed to uni-modal) can be helpful for the core identifying information, where a combination of these three modalities is used. Ultimately, the specific choice of the multi-biometric set should be measured against the three criteria, shown in **Table 10**. Generally speaking, this set needs to have sufficient accuracy to resolve each individual from the entire population, it should be inclusive in that everyone can provide some biometric sample, and it should be flexible enough to support any Use Case envisioned.

The amount and type of data to be captured should be governed by policy. A mass initial enrollment is a sizeable exercise, and is likely a single opportunity to capture the population's data. The policy of collecting more data has to be weighed against the cost (including the cost of equipment, time, and labor) and the inconvenience caused to people due to a heavy process. As a consequence, the NIA working with all the stakeholders needs to arrive at a minimum set of biographic or biometrics to be included in the Core Identifying Data (CID) that could satisfy the above three criteria. For example, this set could consist of six fingerprints as well as a face photograph for a program that might cover up to 50 million people. In other environments, such as, for example, India, it is necessary to capture 10 fingerprints in addition to two irises, in light of the large size of population (1.2 billion people in India).

[35] DNA is the ultimate ground truth of human uniqueness (modulo identical twins). However DNA for the foreseeable future is unlikely to offer an ethically acceptable and technically viable solution for large-scale civil identity programs.

[36] Other technically mature modalities are voice and 3D face, but those do not truly support large-scale 1:N de-duplication and hence they have not had utilities in civil identity registration, even though they are useful for 1:1 verification applications, such as access over the phone or through a physical portal.

Capturing Biometrics of Children

Capturing biometrics of children is a challenge. The papillary ridge structure of fingers does not develop before the age of six, which means no reliable identifiers can be extracted from children's fingerprints before that age. Above the age of six, fingerprints continue to change with growth until adulthood. But that variation is predictable and is compensated for by some of the leading AFIS software.

Some countries, including the European Council (Presidency meeting document 9403/1/06), use 12 years as the minimum legal age for capturing fingerprints from children. An alternative could be to capture iris, which is a biometric that is fully formed in the first year after birth, and seems to be practically feasible to capture down to five years without any challenge and down to one year with significant assistance of mother noted.

In any case it is always a good policy to capture a face starting from birth, even though it is not as accurate as a finger or iris and the photo would have to be updated over time.

In deciding the final set of biometrics, special attention needs to be given to their capture from segments of the population that may represent exceptions. These could be: individuals that cannot physically provide an acceptable biometric and hence represent a technical challenge to the capture process; or individuals, who, because of religious or cultural constraints, represent a social consideration to enrolling biometrics. In the first category, the most important groups are manual laborers—whose fingerprints tend to wear off from excessive use of their hands—and children, whose fingerprints are not fully developed or undergo changes with development; as well as the disabled or amputees. These challenging cases require adopting exception-handling protocols (which may be relevant for 1 to 2 percent of the population) in order to ensure total inclusion. Exception handling for biometric capture may include the use of:

- newer fingerprint scanners based on thin film imaging devices (e.g., Light-Emitting Sensors) instead of optical sensors;
- fingerprint conditioning materials (gels, alcohol, etc.) to improve the finger image contrast on the scanner;
- membrane coating of scanner platen;
- multi-biometrics: when finger is not feasible, the iris and/or face can supply an adequate alternative, or other forms of biometrics could be used.

It is recommended that a biometric-capture feasibility study be performed early on to assess the scope of the challenge within the country's diverse population. The study can recommend the right mix of choices among the ensemble of exception-handling measures that is most suitable for the requirements of the country and its budget constraints.

The cost of exception handling for biometric-capture among children has, in the past, led countries to decide to only enroll the adult population. For example, Indonesia enrolls individuals over the age of 17 in its e-KTP program,[37] which captures 10-print fingers, the two irises, and the face. Children are required to be registered under a parent or guardian (typically mother) until the age of 17, when the children attain their own record and are de-duplicated as a unique identity and issued their e-KTP card. The approach offers benefits but may not be ideal for every application. For example, in areas such as healthcare, there is a need to identify children individually, so as to assure the follow-through required in certain vaccination and treatment programs.

A comparison of the different types of biometrics is presented in **Table 11**.

In summary, a policy must be developed specifying what biometrics are required, if any, by age group and spelling out the exception-handling procedures as part

[37] See the official website of the e-KTP program http://www.e-ktp.com/.

TABLE 11: Comparison of the Most Mature Biometric Modalities Commonly Used in Civil Identity Programs

	Finger	Face	Iris
Available Number	1-10 flat fingers	1	2
Capture Scanner Cost	*Low to Medium* [a]	*Low* [b]	*Medium to High* [c]
Ease of Capture	*High*	*High*	*Low to Medium*
Computing Resources Needed for De-duplication	*Medium to High* • Most intensive among all biometrics • Requires high-end computer cluster with large memory	*Medium*	*Low* Iris-matching algorithms are the most efficient, consuming least computing resources
Adjudication	Requires a trained fingerprint examiner	Any human can compare two faces	Determining if two irises match is not possible via the naked eye
Accuracy	*Very High* when 10 prints are used	*Low to Medium*	*Very High* when 2 iris are used
Failure to Acquire	<1–3%	0%	~1–2%
Children	• < 6 yrs. finger ridges may not be useable identifiers • > 6 yrs. to adulthood useable wt. special software that compensates changes	All ages	• Down to 5 yrs. of age, possible without parental assistance • Below 5 down to 1 yr., challenging and requires parental assistance • Below 1 yr. of age, iris may not be suitable
Manual Laborers	Challenge	No problem	No problem

a Costs are assessed as follows: 10-print scanner (approximated at US$500–US$750), 2-print scanner (approximated at US$200–US$250), and 1-print scanner (approximated at US$5–US$40).
b Using inexpensive webcams.
c Cost of iris camera is assessed at US$500–US$1000.

of the NIA mission. This policy is informed by technical, cultural and human usability factor studies relevant to the country.

In addition to the choice of the type of biometrics, several technical decisions have to be made regarding the capture devices and the ABIS/AFIS backend systems needed to perform the de-duplication. The global market for these technology components is robust and has many players worldwide. Using open standards requirements, as discussed above, should help in developing an effective technology solution.

iii. Choice of Identity Credentials

The NIA may issue a physical identity credential though it is not required to do so. The organization's responsibility could be limited to the generation of a

TABLE 12: Cost and Security Tradeoffs for the Different Credential Media

Card Type	Description	Security
No Physical Credential (zero cost)	Identity is asserted through the UIN (printed on some low-cost medium).	**Offline**: no mechanism is provided. **Online**: authentication via online identity services.
Low-End Cards (low cost)	Such as cards printed on PVC, Teslon and other low-cost substrates. Can contain the UIN in a magnetic strip, which serves as a data pointer to the central identity record in the NIR.	**Offline**: can support a reasonable set of physical security features that give moderate protection against forgery. **Online**: pointer in magnetic strip could connect identity to online identity services for authentication.
High-End Cards (high cost)	Includes single-as well as multi-application smartcards on a high-end durable medium such as polycarbonate.	**Offline**: can support a high degree of security using laser engraving personalization, which is harder to forge. **Offline Electronic**: using a smartcard reader, which reads the data on the card and verifies against the live person (verifies biometrics, or requires PIN) without needing to reach a central database online. **Online**: In the absence of a card reader, the card can serve as a pointer to an identity record and identity can be verified via the online services.
Mobile Credential (low cost)	The credential is carried on a special SIM on the mobile or smart phone.[a]	**Offline:** no natural mechanism, unless an application can be used to securely read the credential on the phone along with a mechanism for strong authentication. **Online:** credential can be authenticated through online services using strong authentication with or without biometrics.

a Note that a dedicated SIM is not needed.

UIN, as applicable, and the associated digital certificates and credentials. These digital assets can be subsequently used by other government agencies, which can optionally incorporate them into the physical evidence of identity with which they equip the sector of the population they serve.

Whether the identification is multi-purpose (foundational) or functional, the choice of credential is significant, since it could be costly. The cost consists of three elements:

- Cost of the medium (the cards)
- Cost of the Personalization and Issuance Systems
- Cost of the Card Management Systems

The first is proportional to the size of the population served, and hence could be prohibitive for large populations. The second represents the cost of establishing and operating secure card issuance systems that include printing and engraving. The third is the ongoing cost required to manage and keep up-to-date the population of cards in circulation.

The emergence of online identity (identity in a cloud) as well as mobile identity can provide some cost-effective alternatives. In the long term, physical ID documents may persist, but the availability of the purely digital alternatives places a cap on how much one should spend per ID card. **Table 12** shows a comparison of four different mediums for credentials, focusing on cost and security trade-offs for offline and online transaction purposes.

At one end, a government may opt for no physical credential at all;[38] here, identity is verified only online via the identity services run at the NIA. These services would work as follows: a data pointer is used to retrieve

[38] Note that credentials would still be needed for specific functions, such as travel (e.g., passport) or driving (e.g., driver's license).

the identity record from the central repository, which is then verified through some mechanism of authentication, including a PIN or 1:1 matching of biometrics of claimed identity, against what is stored in the central database. Alternatively, a government could use a low-cost, non-smartcard with physical security features, which could be used as an offline credential, suitable for most low-risk purposes. This would be supplemented by online identity services for when there is a need for a higher degree of trust or for electronic transactions.

At the other end, the government may use smartcards, where personal information and digital credentials are stored securely on an embedded chip. High-end smartcards may not just be a credential to vouch for identity but a secure platform to deploy applications needed by different government sectors. In this case, smartcards are an enabler of new services and those Use Cases could justify the added cost. One unique capability that is attractive about smartcards is their ability to provide an offline identity authentication mechanism through the use of card readers. Smartcards entail higher costs and require a card reader infrastructure (such as POS) for use.

Mobile devices are emerging as a potential contender for carrying digital identity. They have tremendous cost and convenience advantages, since they are already in the hands of many consumers and do not require yet another physical item, such as a smartcard. This type of identity credential has the potential to gain a strong footprint in the future worldwide.

In the end, how a population is credentialed is informed by an examination of the identity needs in all sectors and is impacted by the current state of development of the country's ICT infrastructure. Countries with strong connectivity and communication coverage can take advantage of online services to provide the authentication and trust, while for those where connectivity is not consistent throughout the country, smartcards become indispensable for offline identity verification.

iv. The Structure of the Unique Identifying Number (UIN)

From a data-centric viewpoint, an individual identity may appear in many databases distributed across several government organizations. Those entries are generated in the course of the individual's interactions with different state functions over time. Absent a foundational identity framework, each database may refer to the same individual differently (different number), making it harder to link entries pertaining to the same individual across multiple databases. With the UIN associated with a fixed identity, the situation can become dramatically different. The UIN may be supplied to all government agencies for incorporation into their databases, ensuring a holistic view of the individual by linking fragmented identity information across different databases. This unified view can help agencies improve their service delivery and cut down on fraud. It has significant value in streamlining the administrative functions of government. Hence, the issuance and utilization of the UIN is recommended, though has to be considered in light of potential privacy risks caused by such a construct.

> Under all circumstance one should keep in mind that, in a data-centric world, what is fundamental is not the ID card, but the identity data, which can be leveraged by storing it on various media depending on needs and budgets.

To decide on the structure of the UIN, a technical analysis is often needed. This includes deciding if the number codes certain immutable information about its bearer or not; and if it does not, whether it will be a serial number or a completely random number. As can be seen from **Table 13,** some countries have opted to code information such as gender, date of birth (DoB), district of birth, etc. There are obvious advantages to such coding, but also potentially some dangers. For example, the UIN can reveal information that could be used for discrimination, profiling, and social exclusion. This is of particular concern in an eID context. Service providers could decide to price their services or restrict their availability, depending on certain digits in the UIN. In addition, a structured number makes it easier

TABLE 13: Examples of UIN as Implemented by Several Countries, Showing the Number of Digits and the Information Coded

Country	UIN Name	Digits	Information Coded
Gambia	National Identification Number (NIN)	11	Place of birth; Place of issuance; Nationality
Nigeria	National Identification Number (NIN)	11	No apparent code
South Africa	Identity Document Number	13	Date of birth; Gender; Citizenship
India	Unique ID Number or Aadhaar	11	None, Totally random
Indonesia	Nomor Induk Kependudukan (NIK)	16	Date of birth; Place of issuance
Pakistan	National Identity Card (NIC) Number	13	Gender; Locality
Estonia	Personal Identification Code	11	Gender; Century of birth
Latvia	Personal Code	11	Date of birth

for fraud perpetrators to guess the number (or at least narrow down the range of possibilities) starting with a few known facts about its bearer (i.e., through social engineering). In the United States, the social security number (SSN) was structured, until it became clear that in the age of social media, where a lot of personal information is publicly available online, a structured SSN is vulnerable to being guessed. Since June 25, 2011, the newly issued SSNs are randomized. Of course, this is relevant only if the UIN is to be considered private, like the SSN is in the US.

In the case where the UIN is to code no information, a serial number is mildly easier to issue, from a technical standpoint. It can also give a sense of when enrollment took place, since lower numbers would have been issued earlier. But those are only minor advantages in favor of a serial number.

Another basic decision is the number of digits to be used. The number of digits selected should provide for more than enough UINs to comfortably accommodate all new births expected for the foreseeable future in the country (on a scale of 50 to 100 years). Typically, this puts the number anywhere between 11 and 16 digits (including a control digit), which should be sufficient for most countries in the world, including all African countries.

On a final note, we should point out that the UIN could provide a mechanism for identity authentication through a PIN. This can be implemented by adding some hidden digits, say four, to the UIN (see **Figure 11**). The PIN can be set by the individual and can become a part of the UIN assigned to the individual's identity and stored in the NIR. The PIN can be used to verify the identity of the bearer in circumstances where biometrics are not practical or are not available. Clearly, this would provide weaker confidence in the identity of the bearer (especially for non-repudiation purposes) and hence would be used for lower-risk transactions, in accordance with the country's risk management model. For example, a citizen interacting with a government agency via a mobile device may be required to supply his or her UIN and, in addition, authenticate himself or herself by providing the PIN, which could be sufficient for requesting routine documents. This is convenient, since it allows this individual to use a mobile device that is not equipped with a fingerprint reader, for example. Some countries

FIGURE 11: Structure for an Uncoded UIN Showing the Identifying Digits, the Hash Control, and the Optional Security Pin

Source: World Bank analysis.

Note: The hash digit (or checksum), is designed to identify common errors when typing or exchanging the UIN (e.g., Luhn checksum algorithm in the public domain and specified in ISO/IEC 7812 standard pertaining to ID card).

TABLE 14: Measures and Technologies Used in Identity Vetting

Measures	Description	Technology
Linking to Breeder Documents	Presenting documentation such as birth certificate, nationality certificate, passport, driver's license, voter ID, property title, tax ID, ration cards, ID from recognized educational institution, trade or labor association, etc.	• Document scanners. • Document readers with automated fraud detection systems (documetrics). • Forensic analysis.
Checking External Databases	Online validation of the name by checking its presence in external and legacy databases, such as the register of births and deaths, social security records, tax records, property records, pension records, poverty registers, etc.	• Digitized civil records. • Secure access portal controlled by organizations owning the data. • Access privilege to external data by NIA. • Ability to query the databases. • Software for entity or identity resolution to disambiguate a person based on text data.
Examining Identity and Social Footprints	In a structured society, the actions of real persons leave behind a trail, the so-called life's audit trail or footprint.	• Identity intelligence software that uses open source to create a body of knowledge around an identity. • Can use the identity knowledge to establish a test of proof of identity–the so-called challenge response. The real person is the only one likely to answer correctly questions related to his life's audit trail as extracted from this data.
Community Affidavits	Testimonials from trusted community members who can act as witnesses to the existence of this person and perhaps his/her reputation. This is evolving into the new domain of social media and online communities.	• Traditional filled-in affidavit forms (offline or online). • Oral interviews. • Increasingly, access to social media with vetting from friends.

in Africa have reported difficulty in the use of PIN due to low literacy rates among the population or among its older members.

v. Identity Vetting

One costly element in an eID program is the vetting of identity. This is the process of connecting a claimed identity to a natural person. It involves establishing documentation for use of the name, the DoB, and the address where this identity can be localized.

Ideally, all persons should be documented in the civil register at birth or upon entry into the country and would have been given a secure birth certificate, the possession of which would go a long way in proving that the person is entitled to the claimed name with that DoB. Unfortunately, in many developing countries, documentation of proof of identification is lacking, primarily because of inadequate civil registration,[39] and because of the ease with which civil documents can be forged or counterfeited.

Robust vetting requires an elaborate process involving several investigative measures and technologies. This is costly because it involves the collection and scanning of evidence, as well as its subsequent examination and validation through mechanisms that could include cross-referencing against external databases (birth or death registers, health records, etc.), forensic examination of breeder documents to ensure they are not forged, and interviews with individuals and members of the community (see **Table 14**).

Thus it is important to adopt a detailed policy on what constitutes acceptable vetting within a framework of risk tolerance. This should represent the shared vision of the government stakeholders as to how to prove identity. In one extreme, the example of India, biometric data is captured along with minimal biographic information. The identity is fixed and from then on is enriched not in the NIR but in the databases of other ministries that

[39] See UNICEF report Opt. Cit.

take upon themselves the responsibility of vetting the data they need for the conduct of their specific mission. For example, a passport agency would need to establish nationality before a passport is issued. A department of motor vehicle agency needs to validate that an individual is fit to conduct a vehicle and uses identity to bind to that individual certain driving privileges.

A decision on what vetting data to collect during the mass enrollment requires consultation with the country's identity stakeholders. A government may be keen to capture as much information as possible and to document everything digitally. Certain government agencies may argue that, unless specific information is provided, identity does not achieve its full potential value in their domain. While they see value in its uniqueness and in the UIN as administrative tools, they believe the missing information might inhibit their ability to perform KYC from the outset.

The ultimate choice will always be a balancing act, where requirements are weighed against cost and the inconvenience factor to the people. The optimal equilibrium point is a national policy that turns the shared vision into an ID data model with acceptable standards for identity vetting and affordable technologies in support of those standards. It can also outline how the additional or missing data, desired by other government sectors, could be collected later in the course of normal business interactions between those agencies and their clients. The government thus has alternatives to: (a) capture a core set of data early on in its mass enrollment, some of which is retained by the NIA, while other data is stored by and of use to other government agencies; or (a) capture a minimum set of data early on to be retained by the NIA only; other government agencies would thus capture their own data, during a different timeline and lifecycle, which would be retained in their own electronic databases, potentially interlinked by an UIN.

Finally, we should point out that eID systems are often second-generation identity systems introduced to replace legacy ones. An eID program can take advantage of these legacy databases both for more robust identity proofing (better than scanning paper documents) as well as for mobilization planning (along with population surveys). In Indonesia, these databases were helpful in targeting individuals who were sent invitations to come to specific centers during the enrollment phase of the e-KTP national identity program.

III.4 Trust, Privacy, and Security

The establishment and operation of an eID system requires putting in place an elaborate set of safeguards that fall under the heading of trust, privacy, and security. Collectively, these are intended to ensure that the system operates within the boundaries of the law, does not violate people's rights, and is protected from abuse, risks, and vulnerabilities, so that it can earn the confidence of those who rely on it.

For simplicity, we have chosen to discuss these safeguards under three separate headings, knowing that these three topics are intertwined. For example, measures that achieve security also enhance privacy and build trust. In addition, this topic should be considered alongside the sub-section on operational processes and controls that have to be put in place in order to ensure operational success of eID, which we discuss in Section III.5 below.

i. Trust

Building trust in the system is an important objective of any IT program. It is even more so for an infrastructure as critical as a national eID with many different parties relying on it. These parties include: the identified persons who are providing their data during enrollment and use; the partner government agencies that require system access for their KYC and to provide services to their people; and the private entities relying on eID to conduct commerce or to provide services. For an eID program to work well, all parties must be convinced of the integrity of the overall system. Unfortunately, building trust is challenging, as it takes a significant effort to earn, yet it can be lost easily without safeguards. In addition, trust is not always fact-based; perception at times is as much of a factor as reality.

Practically, what does trust mean in a national eID program and how is trust built? **Table 15** provides a summary of some of the more important issues that a program needs to address in order to earn and retain trust. These come from lessons learned from similar eID programs around the world. The list is by no means exhaustive, nor is it prescriptive; it is intended to create a starting point for an internal planning dialogue in a country that could culminate into an identity assurance

TABLE 15: Requirements for Building Trust in an eID System

Trust Element	Key Considerations
Registration Integrity	This is a crucial element in the chain of trust. The registration process should ensure that only legitimate identities are able to enroll. **Required Measures:** • Assurance of captured data integrity at the enrollment centers and during transmission to prevent alternations, substitutions, or other manipulations. • When using biometrics, controlling captured image quality as measured metrics such as NIST NFIQ for fingerprints or ICAO face image quality 19794–5. If image quality is not kept high, fraud perpetrators could attempt evasion by intentionally providing bad-quality samples, since match accuracy is directly related to quality. • Matching accuracy of ABIS, if used, in the backend system should be high enough that (together with deterrence) it can lead to practically zero duplicate enrollments.
Trusted Credential	The digital credential as well as the physical proxy should be virtually impossible to fabricate outside the NIA process. **Required Measures:** • Mature and consistent information security, digital signature, certificate management, and encryption practices that leave no loopholes. • Minimum security requirements for any medium that will carry the credential, such as smartcards or mobile phones.
Identity Assurance	Relying parties need to be assured that the person conducting a transaction is who he claims to be and not someone who stole a legitimate identity. **Required Measures:** Strong authentication: multifactor or biometric 1:1 match.
Combating Malfeasance (Human Factors)	Preventing the issuance of *true-false identity*, where a human operator could issue a genuine document for a false identity due to bribe or coercion. **Required Measures:** • Supervised procedures and technology to limit the ability of enrollment agents to fabricate fake enrollment data (often by presenting wrong sequence of fingers, or by mixing and matching fingers from multiple people including their own as they reconstitute the 10-print). • Internal controls at the NIA to ensure that no single operator is capable of surreptitiously modifying or enrolling identity records without supervisor approval. • A higher standard for screening of new hires and ongoing monitoring of agents.
Data Protection and Security	The public should be assured that their data at the NIR is protected against unauthorized access, including external (hacking), internal (rogue employee), as well as organized mission creep. **Required Measures:** • Information security measures that emphasize strong data rights management. • Physical security measures to protect data centers. • Identity data segregation. • Enforced internal policy and procedures for access. • Public policy on data use.
Trust Model	Underlying the eID program, there is technology for trusted communication. This includes enabling authentication for access to online services, digital signature for commitment and non-repudiation, and encryption to secure transmission of transactions. Not only technical measures have to be in place, but also clearly defined responsibilities and liabilities of the authority providing this trust (e.g., CA) should be set in a Legal Act.

strategy for the country. For example, in order to promote trust, some countries have granted individuals a "right to view" all data that is being retained by the government about them. Of course, the topic of trust cannot be separated from the operational controls that have to be put in place, as discussed in Section III.5.

Finally, we should remind the reader that the considerations listed in **Table 15** are designed to address trust in

the system itself and do not address trust in a particular identity. An identity registered and credentialed through such a system may still pose a threat to a relying party, even though it may have been registered legitimately. The question of trust in a particular identity requires other practices, such as identity intelligence and identity risk assessment, which are outside the scope of this report and are typically carried out by organizations other than the NIA for specific needs (employment checks, credit checks, criminal checks, etc.).

ii. Privacy

Privacy is the ability of individuals or a group to free themselves or the information about themselves from being observed, thereby controlling what information they reveal to others (also referred to as the "right to be left alone"). The boundaries and content of what is considered private differ among cultures, individuals, and nations and are changing with the evolution of the Internet and social media. Nevertheless, privacy concerns are evoked universally by data-centric programs such as eID, and, if not addressed correctly from the outset, could jeopardize their success.

eID generates sensitive data during enrollment and when it is used to enable the actions of its holder (audit trail of transactions). More precisely, eID evokes privacy concerns primarily for the following reasons:

- **Enrollment Data:** the eID registration process requires the collection of significant amounts of personally identifying information (PII) for validation and vetting, as previously explained. The collection of such information by its very nature is invasive to privacy. PII includes information that people generally consider private.

- **The Central Database:** not only does an eID system capture PII during enrollment, it consolidates that data into central repositories to guard against duplicative registration and to deliver identity services. Having a roster of all individuals in a country in a central repository creates significant concerns of security, exploitation, and misuse.

- **The UIN:** the use of the Unique Identity Number as an administrative tool to manage identity evokes privacy concerns, since it enables the linking of disparate information about an individual across databases, which a priori are not linked. Linkage deepens the insight into an individual, since the sum of data is more invasive than its individual parts.

- **Digital Audit Trail:** Over time, if eID is successful, it would become pervasive; it would enable a dominant number of the population's daily actions. Such massive reliance on a unique and traceable ID produces a significant amount of data exhaust in the form of an audit trail of actions, which can easily accumulate in digital trail databases without the user's intervention or knowledge. These can be mega-sized databases and may contain biometric data, personal directory data, locational data, device identifiers, transaction details and other PII, which are not the direct outcome of controlled enrollment but a byproduct of identity-facilitated use.

In addition to the potential for privacy invasion, there is the perception of loss of control. The consolidation of massive amounts of data could be perceived as giving to one entity (government, in our case) an instrument that could be used to control the individual and the population. For example, if a log of eID activities is retained, it could evolve into a surveillance program, with significant risks to eID adoption and to people's privacy.

In order to avoid the potential privacy pitfalls of eID, suitable protective measures need to be put in place. Some of the options are listed in **Table 16**.

To start with, privacy-specific legislation forms the foundation of a pro-privacy environment. The legislative acts can pertain to specific applications or verticals (such as healthcare, financial sector, etc.), or they can be omnibus and recognize privacy as a right covered in any context. Often, the act that leads to the creation of the eID references and supplements such privacy laws. On this legal foundation, a government can build a series of measures, similar to those first articulated by the US Federal Trade Commission (FTC) as far back as in 1998, and are collectively referred to as Fair Information Practice Principles (FIPPs). These were the result of the FTC's inquiry into the way online entities collect and use information and represent general safeguards to assure adequate information privacy. Though slightly dated,

TABLE 16: Building a Pro-Privacy Environment for eID

Measure	What is Involved
Legislation	Bodies of privacy laws that impact eID: • Industry-specific laws (for example HIPAA covers privacy of medical information, while GLBA covers financial records in the USA).[a] • Omnibus privacy laws covering all ID data (identity bill of rights). For example European Commission Data Protection and Privacy Directives 95/46 and 2009/136; Article 8 Charter of Fundamental Rights of EU; Convention 108/81 of the Council of Europe (COE). These types of laws cover privacy of PII no matter what type of data or application is involved. • eID specific Legal Acts: sometimes the acts that authorize the establishment of eID in a country also reiterate or introduce new bodies of legislation that explicitly provide privacy protection to people.
Access and Data Protection	The protection of identity data and limiting its use, using technical measures: • Data rights access management. • Anti-data retention measures (e.g., retention of audit trail data only for the period required by law for non-repudiation). • Use limitations.
Notice	• Individuals' right to have notice regarding the data gathered about themselves and the right to know how and for what purpose it will be used. This may be required by law or it may be a good practice for all eID processes (enrollment, use). • Clear, meaningful, and prominent notice when collecting identifying data (iconic plus information link).
Consent/Choice	The individual's right to consent to the collection and use of their personal data.
Privacy by Design	These include privacy-enhancing technologies and measures such as: • Data minimization and proportionality: capture data in proportion to risk. • Identity data segmentation and segregation: e.g., store identifiers separately from PII. • Do-not-track (DNT). • Right to be forgotten. • Right to view. • Pseudonymous, or anonymous transaction management (Trusted Agents).
Privacy Policy	Program-specific (eID program-wide), as well as specific applications.
Privacy Commissioner	An independent body that reports directly to the legislative body (parliament) and acts as an advocate for privacy rights, with powers that include: • Investigate complaints, conduct audits, and publicly report on the privacy practices of public and private sector organizations. • Educate the public regarding privacy. • Pursue legal actions for violations, where supported by law.
Enforcement	Meaningful legal instruments and mechanisms that provide sanctions for noncompliance. Enforcement is not necessarily limited to the scope of action of the Privacy Commissioner's Office.

a HIPAA stands for Health Insurance Portability and Accountability Act of 1996 in the USA, while the GLBA stands for Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999.

these principles embody the four protection principles for privacy in the electronic marketplace, which are *Access, Notice, Choice, and Security*.

The first three of the principles are discussed in entries 2, 3, and 4 of **Table 16**. Security is discussed in the next section. In addition to these principles, best practices now encourage the use of what has become known as Privacy-by-Design. This is an approach of system engineering that takes into account, at all steps of the design and implementation process, the protection of privacy. It is not a single measure, but a collection of technologies and methodologies that fit under the rubric of

Privacy- Enhancing Technologies (PET).[40] PET continue to grow as more attention is being paid to this important issue. The examples of practices that we present in **Table 16** are by no means exhaustive.

Another ingredient that has become important in the privacy dialogue is the privacy policy (PP). This is not a legal agreement, but an easy-to-understand document that any person can read and that explains in plain language what an organization that collects PII is committed to doing to safeguard the information. It is usually the document that Privacy Commissioners start with in examining the privacy practices of a public or private institution.

Finally, as a best practice, it is recommended that the eID program incorporate a PIA (privacy impact assessment) that can be part of the initial planning as well as the change management procedures on an ongoing basis.

iii. Security

At a basic level, an eID program is an information system that is supposed to secure online human interactions. As such, in addition to the measures needed to build trust and respect privacy, as discussed above, the information system requires sound information security safeguards that mitigate against the risk of breach and other operational vulnerabilities, spanning areas of legislation, governance, technology, and operational control. This is the fourth element in the FIPPs, as mentioned earlier.

From a technology standpoint, there is a body of well-developed best practices that can be followed. A pertinent standard is the ISO/IEC 7498-2, which identifies the need to build the following security functions in any information system, including eID:

- **Authentication:** Applies to both entity authentication and data origin authentication. The first provides checking of a claimed identity at the time of usage, while the second provides verification of the source of data (this does not in itself protect against duplication or modification in data units).
- **Access Control:** Provides protection against unauthorized use of resources at all levels of the system. It includes: use of a communication resource, reading, writing, or deletion of an information resource, and the execution of a processing resource or application.
- **Data Integrity:** Ensures that information has not been altered by unauthorized or unknown means at any point in its journey.
- **Data Confidentiality:** Protects against unauthorized disclosure, ensuring that information is kept secret from all but those authorized to see it.
- **Non-repudiation:** Prevents the denial of previous commitments or actions, including repudiation of origin (sender of data denies having sent it) and delivery (receiver of data denies having received it.).

It is recommended that a full-scale IT risk and vulnerability assessment be conducted prior to implementation of the eID solution, as well as on an ongoing basis, in order to monitor how the system withstands real-world operational attacks that could undermine its functionality.

III.5 Operational Processes and Controls

Ultimately, an eID system needs to be run as a going concern. This means that there must be processes and controls in place to avoid the failure of the NIA and to ensure the achievement of the following corporate objectives:

- **Regulatory compliance:** the NIA has to function in compliance with all applicable laws and regulations, including the act that led to its formation. It has to respect the rights of the people that it serves (privacy, as well as the right of access to service without exclusion or discrimination). This is in order to avoid potential regulatory penalties and sanctions, and potential loss of goodwill in the eyes of the public.
- **Protection against man-made operational risk:** both internal (corruption, bribery, and collusion) and

[40] See Ronald Hes and John Borking, "Privacy Enhancing Technologies: The Path to Anonymity," joint report of the Information and Privacy Commissioner of Ontario, Canada, and the Dutch Data Protection Authority, Revised edition 2000, can be downloaded from http://www.cbpweb.nl/downloads_av/av11.pdf.

external (data breaches, cybercrimes, terrorism, and general hacking and disruption of service). These could adversely impact the trust in the system, as discussed above, and could cause it reputational damage.

- **Continuity of operations:** an eID is a mission-critical system. Procedures and measures have to be established to ensure that it can recover and continue to operate in the event of business disruption (such as a disaster).

- **Continued relevance:** as a going concern, the eID needs to continue to be relevant and to grow its role within society. This requires capturing, on an ongoing basis, the public mind share.

- **Efficiency of operations:** invariably, the NIA will be judged by its ability to operate as a successful entity. That means it will have to deliver on financial and operational performance metrics (e.g., efficiency and customer satisfaction).

The processes and controls necessary for achieving the above objectives can be grouped into two categories (i) Corporate and support function controls, and (ii) Controls related to identity management. A summary of these are given in **Table 17** and **Table 18,** respectively.

It is important to emphasize that the audits referenced in **Table 17** are intended to be over and above any audits that the Independent Auditor may perform on the entire system pursuant to the requirements established by the cabinet or the parliament, as discussed in Section III.2 on Institutional Governance.

The controls for the processes of identity management, shown in **Table 18**, include procedures applicable to each phase of the identity lifecycle: registration, issuance, and use, including maintenance or updates. They are designed to render the system efficient and accountable, and to protect the system from any form of fraud or abuse in accordance with the requirements of trust in the system, as set out in **Table 15** above.

TABLE 17: Corporate and Support Function Controls for eID System

Category	Control Description
Operational Governance	These involve internal policies and procedures for the operation of the NIA as an autonomous corporate entity: • Information security policies • Privacy policy and notices • Human resources policies • IT governance policy • Business continuity management and disaster recovery • Data retention policies • Communication to and acknowledgement by employees of policies There are a number of sources that provide guidance on this matter, including the ISO/IEC 38500:2008 on standards for corporate governance in IT organizations. In addition, regulatory requirements may have significant operational governance implications and should be consulted.
Human Resources	Screening of all employees, contractors, and consultants prior to their involvement in the eID program. This may include background checks, criminal history checks, and previous employment and credit checks. In some cases, a formal security clearance may be required for certain sensitive roles.
Supplier Vetting	Due diligence for suppliers as well as periodic review of performance. This is to ensure that they can actually deliver on contractual commitments and that they have the qualifications and skills necessary for quality of implementation.
Change Management	Procedures to facilitate the adoption of change within the eID system. Change control procedures should be designed to ensure that changes are appropriately considered, approved by management, and are not disruptive to the operations. Best practice standards are available, such as ISO/IEC 200000 Information Technology Service Management.

TABLE 17: Corporate and Support Function Controls for eID System (Cont'd.)

Category	Control Description
Audit and Compliance	Rigorous audits for the entire system, which would be conducted on a regular basis both internally and by trusted independent entities. The goal is to demonstrate the compliance of the eID system with applicable laws and regulations, as well as internal policies, and that it operates effectively as designed and presented to the public.
Awareness	• Marketing and public education programs to improve public awareness and understanding of the eID and to promote its continued use. • Internal training and awareness for employees to ensure they understand their roles and responsibilities in terms of security and privacy, and all other internal policies.
Security and Privacy	• Physical access control and security procedures to the eID issuance site to protect against unauthorized use. • Role-based system and logical access controls to prevent system abuse. • Segregation of operational authority to combat malfeasance. • Secure audit logs to enhance investigative power in case of an incident and to provide deterrence. • Privacy controls.
Business Resilience	Business availability, business continuity, and disaster recovery.

TABLE 18: Controls Related to Identity Management in an eID System

Category	Control Description
Registration	• Request for eID application • Collection and scanning of identifying documents • Capturing of data into the eID system • Enrollment of biometric data into profiles • De-duplication of identity • Adjudication of potential matches • Vetting of identity • Confirmation of eID profile creation • eID profile approval • eID profile submission for creation
Issuance	• Creation of eID • Issuance of a physical credential, where applicable • Activation of the eID • Issuing the eID to the righftul individual
Use: Authentication	• Use of the eID for various authentication functions through identity services • Identity verification and authorization
Use: Maintenance	• Call center for customer care • Updates or changes for eID profile • Renewal of an eID • Revocation of an eID

IV. Policy Considerations

Developing countries face a myriad of pressing challenges, from battling poverty and curbing corruption to improving governance and ensuring the efficient delivery of services. eID can serve as a powerful instrument to help tackle these challenges. eID provides a cross-sector platform to accelerate economic and social development in a developing country, eID is increasingly referred to as a "game changer" or a "poverty killer,"[41] as illustrated by the Use Cases in Section II.5.

Though offering transformational benefits, eID also presents a sizeable undertaking for a developing country's government, and requires careful planning. Building an identity program spans several years, is costly, requires multi-sector coordination, relies on scarce technical skills, and mandates strong provisions for data protection and privacy. Political will and top-level commitment are thus prerequisites for a successful eID program. Like many electronic government programs, eID promises huge rewards in return for calculated and managed risks.

In developing an eID program, a government has a number of policy choices to make. These choices require a review of the country's specific economic, social and political context, and a discourse with the actors in the local identity ecosystem to build a viable eID program. Section III gives a detailed account of these discussions and the decisions to be explored.

As governments contemplate a digital identity program, the following policy considerations serve as a useful reference and draw on the detailed account from this report:

- **Conduct a diagnostic on the scope of eID in the country:** Before embarking on a full-fledged program of eID, a government may consider conducting a rapid diagnostic on eID to examine the potential and readiness of eID in the country. The diagnostic can communicate a go or no-go decision to the government. It may involve reviewing several elements, including but not limited to: (a) cultural and political environment; (b) economic and political environment; (c) legal and regulatory environment; (d) state of civil registry, such as for birth, death, and marriages; (e) current identity landscape in the country, for foundational and functional identities; (f) potential Use Cases of eID for rapid adoption; (g) eligibility criteria for participants to enroll in eID, such as for citizens, residents, foreigners, etc.; (h) capacity of government agencies with potential role in identity management; (i) capacity of domestic IT industry as potential partners; and (j) governance mechanisms for identity.

- **Enlist champions and engage stakeholders of identity:** A successful eID program requires several

[41] See press release "India's Massive I.D. Program Exemplifies 'Science of Delivery,'" at http://www.worldbank.org/en/news/feature/2013/05/02/India-8217-s-Massive-I-D-Program-Exemplifies-8216-Science-of-Delivery-8217? (last accessed May 10, 2014).

key ingredients: high-level, sustained political commitment, champions, and active stakeholders. The overarching vision convening stakeholders, partners, and champions should underscore that: "identity concerns all." The identity ecosystem spans several line ministries, government agencies, regulatory bodies, industry associations, the private sector, and civil society. To build collaboration across these organizations, the government should establish a consultation strategy that identifies and involves stakeholders, and defines appropriate roles and responsibilities for them. Such a strategy would affect identity registration and ensure that eID, when run across multiple programs and government actors, is properly integrated.

- **Establish a supportive legal, regulatory, and authorizing environment:** The government needs to decide early on whether a foundational or functional identity program suits the country's development needs. (See Section III.1 for a discussion and comparison of the two programs.) Based on the approach, the government should review and update the existing legislative environment as affected by digital identity, identifying gaps and enacting appropriate remedial policies and legislations. For a foundational identity, legislation is needed to authorize a government agency (such as the NIA), whether existing or new, to serve as the coordinator for eID in the country. The government needs to set the charter for NIA, and balance the charter with the role of other government agencies, for functions of enrollment, national ID card issuance, and identity services.

- **Determine enrollment approach for identity—through civil registry or biometrics for development:** The government has broadly two avenues through which to register people: (a) through a civil registry; or (b) using biometric technology. Many developing countries lack a strong civil registry for births and deaths. Revamping and building the capacity of a civil registry is a sizeable task, and requires digitizing paper records of *historic* births and deaths, creating applications and processes to electronically capture data of *future* births and deaths (at healthcare centers and related institutions), and instituting compliance, monitoring, enforcement, and audit systems to ensure the authenticity of the data captured. In the absence of a strong civil registry, biometrics offers an attractive technology. Over 1 billion people in developing countries reportedly have had their biometrics taken for one or more purposes.[42] Before opting for biometrics, the government should perform feasibility studies to assess the type of biometrics to be used, and whether any obstacles—technical, cultural, or operational—hinder the adoption of this approach.

- **Decide on a credential, if any:** Whether a government plans to issue a new national identity card to its people or update an existing one, the choice of credential, if any, is important. The credential comes at different price points, from inexpensive simple ID cards or using mobile phones to more expensive but sophisticated smartcards. The government also has to decide whether to underwrite the cost of credentials or offer identity free of charge to its people. The country may choose not to offer credentials at all, depending on the type of the eID program, as demonstrated by India's Aadhaar program.

- **Anchor the eID program in a strong institution, with provisions for good governance, change management, sustainable business model, managerial and technical capacity, data protection, strong operational controls, monitoring and evaluation (M&E), and long-term operations and maintenance (O&M):** eID requires a strong operating arm of the government that demonstrates operational efficiency over time and is resilient to changes in the political environment. To build a robust institution, the government may consider putting in place specialized commissions that provide recommendations to the government on various technical and operational details. These recommendations may span: the structure of the UIN, the use of biometrics, the digital signature and trust model, the identity data model, the choice of

[42] See Gelb and Clark (2013).

credentials, the data security and privacy underpinnings, the technology strategy, and the approach for mapping the population for mass enrollment. The business model for the institution should focus on affordability of registration and credentialing to the population, while examining potential revenue streams for sustainability. The technology-centric nature of eID requires extra attention to building technical and operational capacities throughout the eID organization: for enrollment, back end, de-duplication, credential issuance, certification management, and identity services. The government would need to plan and budget for M&E, O&M, and staff training. Financial planning for the eID program should be realistic, taking into account the total cost of ownership, including up-front fixed costs and yearly operating costs.

- **Pursue PPP, where feasible:** eID can pose challenges of technical know-how and investment for a government. The long-term operations of an eID program are also susceptible to changes in the political environment. The private sector can help balance the government mandate of a national eID program with the private sector's efficiency, expertise, and resource mobility. The government could explore a PPP arrangement with the private sector, including but not limited to, using outsourcing, concession, service-level agreement, build-operate-transfer, or private participation.

- **Adopt a technology strategy, aiming for cost efficiency, interoperability, scalability, reliability, and availability:** From the outset, the government should consider a technology solution that is low-cost and is scalable to reach national coverage. The technology architecture should adapt to the specific socioeconomic conditions of the country, leveraging existing resources, where possible, and prioritizing important Use Cases for rapid adoption. International standards and an open architecture platform for interoperability are necessary conditions. The government should give special attention to preventing any lock-in due to vendor or technology in its technology solution. The procurement of technology should be based on a competitive and transparent procurement process, open to international, regional, and local vendors. The technology strategy should support a healthy marketplace of identity within the country.

- **Communicate effectively and provide channels for complaint resolution and redress:** A digital identity touches people directly—in the way it prompts people to register, gives them a badge of identity, and allows them to use identity in their daily lives. To be effective, an eID program should employ a strong communication plan, raising public awareness about eID and educating people about what is expected of them, what changes are brought about by eID, and how the government has put in place benefits and protections for people to use eID. The program should address misconceptions and concerns about eID among the population and provide a channel—whether in-person, online, or by phone—through which individuals can file complaints and seek redress when in need.

This report has provided a conceptual framework for identity management and a strategic overview of the functional blocks that need to be put in place in order to build a modern electronic identity system. In the coming years, the convergence of several factors (such as mobility, electronic commerce, hyper-connectivity, and social media), which are already under way, is likely to deepen a dependency on digital identification and to alter societal and legal notions of identity. This will likely make the subject of eID more important. Today, national governments recognize their responsibility to facilitate the development of eID to exploit the opportunities offered, enhance the security of transactions, and improve the delivery of services to people.

WORLD BANK GROUP

1818 H Street, NW
Washington, DC 20433, USA
Telephone: +1 (202) 473-1000
Internet: www.worldbank.org