# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>3</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td><strong>BENCHMARKING REPORT</strong></td>
<td>9</td>
</tr>
<tr>
<td>Benchmarking Report Overview</td>
<td>10</td>
</tr>
<tr>
<td>Benchmarking Framework</td>
<td>12</td>
</tr>
<tr>
<td>Benchmarked Features</td>
<td>14</td>
</tr>
<tr>
<td>Benchmark Summary</td>
<td>22</td>
</tr>
<tr>
<td><strong>SCOPING REPORT</strong></td>
<td>24</td>
</tr>
<tr>
<td>Scoping Report Overview</td>
<td>25</td>
</tr>
<tr>
<td>Policy, Legal &amp; Regulatory Considerations</td>
<td>25</td>
</tr>
<tr>
<td>Institutional Structures</td>
<td>30</td>
</tr>
<tr>
<td>Business Models</td>
<td>32</td>
</tr>
<tr>
<td>ID4D Integration Technology</td>
<td>36</td>
</tr>
<tr>
<td>Additional Integration Approaches</td>
<td>42</td>
</tr>
<tr>
<td><strong>STRATEGY AND ROADMAP FOR IMPLEMENTATION</strong></td>
<td>45</td>
</tr>
<tr>
<td>Strategy Overview</td>
<td>46</td>
</tr>
<tr>
<td>High-level Strategy</td>
<td>46</td>
</tr>
<tr>
<td>Roadmap</td>
<td>49</td>
</tr>
<tr>
<td>Monitoring and Evaluation</td>
<td>53</td>
</tr>
<tr>
<td>Conclusion</td>
<td>56</td>
</tr>
<tr>
<td><strong>ANNEXES</strong></td>
<td>57</td>
</tr>
<tr>
<td>Concepts</td>
<td>58</td>
</tr>
<tr>
<td>Introduction</td>
<td>60</td>
</tr>
<tr>
<td>Highly Integrated Identification Reference Model</td>
<td>60</td>
</tr>
</tbody>
</table>
COMPENDIUM OF CASE STUDIES: ................................................................. 65

Disclaimer ............................................................................................................. 69
Introduction ............................................................................................................ 70

STUDIED COUNTRY PROFILES ........................................................................ 72
Guinea .................................................................................................................. 73
Rwanda ............................................................................................................... 79
Botswana ............................................................................................................ 85

BENCHMARKED COUNTRY PROFILES .............................................................. 91
Estonia ............................................................................................................... 92
Portugal ............................................................................................................ 100
Belgium ........................................................................................................... 104
Pakistan .......................................................................................................... 112
Kenya ............................................................................................................. 120
Mexico ............................................................................................................ 131
Nigeria ............................................................................................................ 139
Sierra Leone ........................................................................................................ 146
Liberia ............................................................................................................ 152
Djibouti .......................................................................................................... 159
Laos .................................................................................................................. 164
India ................................................................................................................ 170
References ....................................................................................................... 176

LIST OF TABLES

Table 1: Research Methodology Stages ............................................................... 7
Table 2: Country Categories ............................................................................... 11
Table 3: Features of a Highly Integrated National ID System ................................. 12
Table 4: Country Category Summary .................................................................. 22
Table 5: Principles of Data Privacy ...................................................................... 26
Table 6: Principles of Electronic Transactions ..................................................... 27
Table 7: Principles of Policy, Legal and Regulatory Frameworks ......................... 29
Table 8: ID4D Integration Layer Adapter Technologies ....................................... 41
Table 9: ID4D Service-Enablement Governance Process Steps ............................. 50
Table 10: Key Components of the Highly Integrated ID4D Identification Model ... 62
LIST OF FIGURES

Figure 1: ID4D Integration Model ................................................................. 17
Figure 2: ID4D Integration Layer Adapter Functional Diagram ...................... 38
Figure 3: Figure 3: ID4D Integration Layer Adapter Detailed Diagram .......... 39
Figure 4: STORK Platform Model ............................................................... 43
Figure 5: X-Road EU Model ................................................................. 44
Figure 6: ID4D Integration Strategy ....................................................... 47
Figure 7: Greenfield Country Integration Roadmap ......................................... 49
Figure 8: Intermediate Country Integration Roadmap ...................................... 51
Figure 9: Advanced Country Integration Roadmap ......................................... 52
Figure 10: ID4D Balanced Scorecard ....................................................... 53
Figure 11: Emergent Identity Concept ...................................................... 58
Figure 12: Strong Authentication .............................................................. 59
Figure 13: ID4D Integration Model Diagram ............................................. 61
Figure 14: Integration Areas of Focus for Guinea ........................................... 78
Figure 15: Integration Areas of Focus for Rwanda .......................................... 84
Figure 16: Botswana’s Ministry of Labour and Home Affairs Jurisdictions .......... 87
Figure 17: Integration Areas of Focus for Botswana ....................................... 90
Figure 18: X-Road Middleware Architecture ............................................. 93
Figure 19: India’s UID Architecture ....................................................... 170
Official identification (ID) is more than a convenience; it is a fundamental human right. It is indispensable for connecting residents to electoral participation, educational opportunities, financial services, health and social welfare benefits, and economic development. It gives people a chance to better communicate with and be recognized by their government while giving governments the opportunity to listen and improve the lives of their citizens. Yet in the developing world, over 2 billion people lack an official ID. The problem disproportionately affects children and women, from poor rural areas in Africa and Asia.

The role of robust identification systems and their importance to development outcomes places them within the new Sustainable Development Goals (SDG) agenda — specifically as one of the proposed SDG targets (#16.9), but also as a key enabler of the efficacy of many other SDG targets. Although there is no one model for providing legal identity, this SDG would urge states to ensure that all have free or low-cost access to widely accepted, robust identity credentials. Regardless of the modalities to achieve it, unique identification — together with its associated rights — is becoming a priority for governments around the world. The international community should join forces to support this goal.

Disparate initiatives and siloed investments in registration and identification systems are likely to be wasteful and duplicative, detracting from the far-reaching public and private sector implications of universal digital identities. A standards-based approach to ensure interoperability of systems – both at national and regional level - could help in driving the technology costs down and in enhancing service delivery across boundaries.

Recognizing the transformational potential of 21st century ID systems for the delivery of basic services to the poor, the World Bank recently launched its Identification for Development (ID4D) agenda. The goal is “making everyone count” by “providing an identity and delivering digital ID-enabled services to all.”

As a stepping stone towards that vision, this study, developed in collaboration with Accenture Development Partnerships, helps in conceptualizing the design and implementation of ID4D programs in a highly integrated, interoperable and scalable manner that can produce huge savings for citizens, government and businesses.
Pooled approaches and federated ID systems at the regional or sub-regional level can also help in strengthening the value proposition of ID4D programs. Trust in data security will be critical to achieving tangible results. Harnessing the power of ID4D systems will require strong political will and leadership, and a supportive institutional environment.

Randeep Sudan
Practice Manager
Information and Communication Technologies
Transport & ICT Global Practice
The World Bank
ACKNOWLEDGMENTS

This report has been made possible with funding from the World Bank Group Global Engagement contingency and the International Finance Corporation (IFC) Trust Fund TF0121681.

As part of its work on the Identification for Development (ID4D) Integration study, the World Bank Group has partnered with Accenture Development Partnerships\(^1\) – world leader in providing strategy advice and consulting services to the development sector on a non-profit basis.

The project has been lead by Mariana Dahan (Task Team Leader and ID4D Working Group Coordinator at the World Bank). The report benefited from extensive comments received from colleagues from within and outside of the World Bank Group. These include the core members of the ID4D Working Group, representing World Bank Global Practices responsible for Finance and Markets, Governance, Health, Information and Communication Technologies, Social Protection, Trade and Competitiveness, along with the Legal and Development Economics Groups, Gender Cross-Cutting Solution Area, IFC, Multilateral Investment Guarantee Agency (MIGA) and the Consultative Group to Assist the Poor (CGAP). Valuable feedback has also been received from the World Bank Country Management Units (CMU) colleagues from the countries studied in this report, in particular from the Republic of Guinea, Botswana and Rwanda. Their helpful comments and inputs have significantly enriched this report.

The team is grateful to Pierre Guislain (Senior Director, Transport and ICT Global Practice at the World Bank) and Randeep Sudan (Practice Manager for ICT at the World Bank) for their guidance and support throughout the preparation of the report.

The team also thanks Alan Gelb, from the Center for Global Development and Cyrille Bellier, from Agence Française du Développement, for their help in conducting consultations with key stakeholders and in the dissemination of this report.

\(^{1}\) [http://accenture.com/adp](http://accenture.com/adp)
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAM</td>
<td>Business Activity Monitoring</td>
</tr>
<tr>
<td>CMUs</td>
<td>Country Management Units</td>
</tr>
<tr>
<td>CNIL</td>
<td>Commission Nationale de l’Informatique et des Libertés</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off-the-shelf</td>
</tr>
<tr>
<td>CR system</td>
<td>Civil or Population and Vital statistics registry</td>
</tr>
<tr>
<td>CRVS</td>
<td>Civil Registration and Vital Statistics systems</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Electronic identification and trust services</td>
</tr>
<tr>
<td>ESB</td>
<td>Enterprise Service Bus</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ID4D</td>
<td>Identification for Development</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IFC</td>
<td>International Finance Corporation</td>
</tr>
<tr>
<td>IPRS</td>
<td>Integrated Population Registration System</td>
</tr>
<tr>
<td>IQS</td>
<td>Image Quality Specification</td>
</tr>
<tr>
<td>KPIs</td>
<td>Key Performance Indicators</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-to-Machine</td>
</tr>
<tr>
<td>NFIQ</td>
<td>Fingerprint Image Quality</td>
</tr>
<tr>
<td>NIEM</td>
<td>National Information Exchange Model</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NPR</td>
<td>National Population Register</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PPP</td>
<td>Public-Private Partnerships</td>
</tr>
<tr>
<td>SDGs</td>
<td>Sustainable Development Goals</td>
</tr>
<tr>
<td>SLA</td>
<td>Service-Level Agreement</td>
</tr>
<tr>
<td>SOA</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>SPDI</td>
<td>Sensitive Personal Data or Information</td>
</tr>
<tr>
<td>SPV</td>
<td>Special Purpose Vehicle</td>
</tr>
<tr>
<td>STORK</td>
<td>Secure idenTities acrOss boRders linKed</td>
</tr>
<tr>
<td>STQC</td>
<td>Standardized Testing and Quality Certification Directorate</td>
</tr>
<tr>
<td>TTL</td>
<td>Task Team Leader</td>
</tr>
<tr>
<td>UIDAI</td>
<td>Unique Identification Authority of India</td>
</tr>
<tr>
<td>WDR</td>
<td>World Development Report</td>
</tr>
</tbody>
</table>
INTRODUCTION

RATIONALE FOR THIS STUDY

This study is part of the Identification for Development (ID4D) agenda of the World Bank Group. ID4D is a cross-sectoral initiative that unites teams from different sectors of the World Bank Group. These sectors include Global Practices responsible for Finance and Markets, Governance, Health, Information and Communication Technologies, Social Protection, Trade and Competitiveness, along with the Legal and Development Economics Groups, Gender Cross-Cutting Solution Area, International Finance Corporation (IFC), Multilateral Investment Guarantee Agency (MIGA) and the Consultative Group to Assist the Poor (CGAP). This agenda has strong links to the World Bank Group’s twin goals of fighting extreme poverty and promoting shared prosperity. It is also aligned with the Sustainable Development Goals (SDGs) agenda, specifically target #16.9: “provide legal identity to all, including birth registration, by 2030”.

Proof of identity is critical for the poor to gain access to basic services, such as healthcare, social benefits and financial services. Similarly, identities are important for the bottom 40% of the population to have better access to job opportunities, services and finance. Yet hundreds of millions of children and adults worldwide do not have any form of recognized identification (ID). As further described in Annex 1 - Unique Identity is paramount. In many countries, the design and implementation of civil registration and identification programs are shaped by cultural preferences, regulatory requirements, technological maturity and privacy needs. Identification programs, sometimes implemented as digital ID programs, are often approached from different points of entry, which might include broad national ID initiatives or more narrow sectoral approaches (for example, in healthcare, social welfare or finance).

In the absence of a unifying vision or coherent strategy, parallel use of different points of entry can result in duplication and waste of public resources. And while each country context is unique, it is important to develop systematic approaches to avoid such duplication and waste. In pursuing sectoral initiatives relating to identification, countries tend to develop parallel systems, which oftentimes are neither connected nor interoperable. Therefore, nations seeking to roll out ID initiatives can benefit from adopting a standards-based approach and by linking

---

2 (Dahan and Gelb, Role of Identification in the Post-2015 Development Agenda, 2015)
national ID programs and sectoral interventions. This can result in enhanced interoperability of systems and use cases. Such approaches need to take into account various technological options that are currently available. In addition, regulatory and institutional realities also need to be accounted for and, potentially, adjusted to the new integrative approach. Selecting the right business model can further help ensure sustainability of programs and returns on investments made.

With an eye toward developing such a comprehensive ID4D Integration approach for client countries, the World Bank has partnered with Accenture Development Partnerships to develop the present study.

**OBJECTIVES OF THE STUDY**

The main objective of this study is to provide guidance for the design and implementation of ID4D programs, with the goal of fostering convergence among disparate sectoral and national ID initiatives. Through extensive research and consultations with stakeholders, the study describes an ID4D integration model for three different country categories that can benefit from a more effective approach to ID4D programs. The study offers a specific strategy and roadmap for each country category, drawn from a representative client-country study, and provides recommendations in areas including policy, processes, technology and business models. The technical specification of solutions is not in the scope of this report, nor is the corresponding investment plan, as this would be country specific. Given the momentum, aspects relating to regional integration and pooled approaches are also explored, though not in detail, rather as a way to outline future research questions.

**METHODOLOGY**

The study is based on a comprehensive research methodology that combines quantitative and qualitative approaches over a number of stages as provided in Table 1.

**STRUCTURE OF THE REPORT**

This study comprises three main sections:

- Benchmarking Report
- Scoping Report
- Strategy and Roadmap for Implementation
<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Inception / Conceptual Model Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Data analysis and literature review</td>
</tr>
<tr>
<td></td>
<td>- Experts’ meeting : Accenture Capability Network focus group discussions</td>
</tr>
<tr>
<td></td>
<td>➤ ID4D integration model</td>
</tr>
<tr>
<td></td>
<td>➤ Replication for 3 categories:</td>
</tr>
<tr>
<td></td>
<td>1. Advanced</td>
</tr>
<tr>
<td></td>
<td>2. Intermediate</td>
</tr>
<tr>
<td></td>
<td>3. Greenfield</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 2</th>
<th>Benchmarking</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Identification of countries in each category</td>
</tr>
<tr>
<td></td>
<td>- Selection of countries to be studied in depth</td>
</tr>
<tr>
<td></td>
<td>➤ Validation of choices with World Bank Task Team Leads (TTLs) and analysis of data/documentation available for each country</td>
</tr>
<tr>
<td></td>
<td>- Selection of countries to be analyzed as part of the benchmarking exercise</td>
</tr>
<tr>
<td></td>
<td>➤ Benchmarking countries from list of World Bank focus countries, plus internationally recognized “best-in-class” countries</td>
</tr>
<tr>
<td></td>
<td>Total of 15 countries selected:</td>
</tr>
<tr>
<td></td>
<td>• 12 benchmark countries</td>
</tr>
<tr>
<td></td>
<td>• 3 countries studied in depth (one from each category)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 3</th>
<th>Scoping</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Appraisal of existing, parallel ID-related initiatives in client countries</td>
</tr>
<tr>
<td></td>
<td>- Identification of opportunities for ID4D integration</td>
</tr>
<tr>
<td></td>
<td>- Interviews with key stakeholders</td>
</tr>
<tr>
<td></td>
<td>➤ Confirmation of findings with World Bank TTLs and government officials from the client countries studied</td>
</tr>
<tr>
<td></td>
<td>- Assessment of:</td>
</tr>
<tr>
<td></td>
<td>• Technology platform and processes</td>
</tr>
<tr>
<td></td>
<td>• Institutional</td>
</tr>
<tr>
<td></td>
<td>• Legal/regulatory</td>
</tr>
<tr>
<td></td>
<td>• Business models</td>
</tr>
<tr>
<td>Stage 4</td>
<td>Validation</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>- Validation of the ID4D integration model for each country category identified with World Bank TTLs and government officials from client countries studied</td>
<td></td>
</tr>
<tr>
<td>- Meetings organized during ID4Africa Forum in Tanzania and afterward (June 2-5, 2015)</td>
<td></td>
</tr>
<tr>
<td>- Conference calls and online exchanges post-event, back to Washington, DC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 5</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Formulation of integration strategy and roadmap for each country category, with recommendations for overcoming bottlenecks to development of national ID system and for leveraging existing initiatives and legacy systems</td>
<td></td>
</tr>
<tr>
<td>➤ Elaboration of a dedicated ID4D integration model for each of the three countries studied, with focus on:</td>
<td></td>
</tr>
<tr>
<td>• Technology platform and processes</td>
<td></td>
</tr>
<tr>
<td>• Institutional</td>
<td></td>
</tr>
<tr>
<td>• Policy, legal/regulatory</td>
<td></td>
</tr>
<tr>
<td>• Business models</td>
<td></td>
</tr>
<tr>
<td>- Discussion of the proposed ID4D Integration Approach and consultation with key stakeholders, including donor partners, civil society, think tanks and private sector during a dedicated session on Digital Identity/ID4D at the 2016 WDR event in Paris on June 23-24, 2015.</td>
<td></td>
</tr>
</tbody>
</table>

Other relevant reports and documents are presented in the Compendium of Case Studies, which includes:

- 12 benchmarked country profiles
- 3 in-depth country case studies

A comprehensive References list is presented at the end of the consolidated deliverable, corresponding to sources used for each report, case study and country profile.
BENCHMARKING REPORT
The Benchmarking Report defines the key features of a highly integrated, unified ID system and categorizes countries into different levels of maturity based on the degree to which they demonstrate these features. Reference literature\(^3\) highlights the fact that countries develop *foundational ID systems*, which provide general identification covering the entire population (and can include civil registries and unique national IDs) and *functional ID systems*, which cover population subsets and are introduced in response to a demand for a particular service or transaction transaction (such as voter registration). Developing countries often have both types of systems in operation. This report aims to review and analyze the level of integration between these different systems, on the assumption that operating disparate, disconnected and parallel ID systems within a country may lead to duplication and waste of resources.

The reviewed evidence shows that the vast majority of countries have fragmented, single-purpose ID systems\(^4\):

<table>
<thead>
<tr>
<th>Coverage Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>8% No Digital ID</td>
</tr>
<tr>
<td>12% Digital ID used for identification only</td>
</tr>
<tr>
<td>72% Digital ID used for one or more services</td>
</tr>
<tr>
<td>7% Fully integrated, multi-purpose ID systems</td>
</tr>
</tbody>
</table>

*198 countries were included in this assessment*

As more developing countries seek to establish integrated national ID systems, it is important to understand which category they are in so the appropriate strategies and technological recommendations can be applied. The countries for analysis have been divided into three categories, grouped as shown in Table 2.

---

\(^3\) (Gelb & Clark, Identification for Development: The Biometrics Revolution, 2013)

\(^4\) Graphic generated from the ID4D Global Dataset and Stocktaking Analysis done in 2014 by the ID4D Working Group, World Bank.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Category 1: Advanced| - Country has developed a digital ID system with the majority of the features characterizing a high level of integration, but may be lacking maturity in a few features.  
- May have strong foundational registries, an integrated framework and specific plans to address weak points. |
| Category 2: Intermediate| - Country has taken measurable steps to develop a digital ID system, but still has significant improvements to make to ensure that the system is scalable and can be integrated with existing disparate registries.  
- May have a foundational database (registry) in place or efforts in progress to strengthen and/or digitize one. |
| Category 3: Greenfield| - Country has rudimentary or no registry integration -either directly, through custom interchanges, or through a service-oriented architecture (SOA).  
- May have the most room for improvement and typically has a “blank slate” from which to launch a digital ID program. |

These categories will help the World Bank and its client countries tailor ID4D integration strategies to each nation’s level of maturity regarding its ID programs.
When defining a highly integrated national ID system, it is important to look at not only the ID system (and the technology behind it) but also the surrounding policy, regulatory and institutional structures that support enforcement of the system. Although each country context is different, a framework for such a system has the features shown in Table 3, which are described in subsequent sections in this report.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maturity of foundational registries                  | • Country has a digital (electronic) civil registry (typically, population or birth/death) that can serve as the backbone of the national ID system.  
• A high percentage of the population is represented in the system. |
| National ID system                                   | • Country can provide registrants with unique IDs that are verifiable/de-duplicable using biometrics.                                         
• System is integrated with a stable foundational registry (existing or created as part of the national ID system). |
| Level of registry integration                        | • National ID system is integrated with multiple functional registries, reducing possibilities for duplication and waste.                         |
| Policy and legal regulations                         | • Regulations are in place to protect data privacy and electronic transactions.                                                             
• Mandatory birth and death registration laws are in effect and enforced. |
| Institutional structure                              | • An overarching agency is responsible for the national ID system.  
• Government mandates exist to integrate the national ID system and support the governance body.                                          |
| Accessibility                                        | • Country has built or implemented a plan to achieve full population coverage in its national ID system (including strategies to reach marginalized and rural populations). 
• Country has defined a strategy (such as expanding mobile or Internet connectivity) for enabling more registrants to access benefits. |
| Ability to provide physical credentials for individuals | • Country has a method of distributing verified physical credentials to individuals (such as e-passports or national ID cards).            |
The majority of developing countries will need to address a number of areas before they reach a highly integrated state. These countries can be grouped into the three categories described earlier: Advanced, Intermediate and Greenfield.

The Compendium of Cases Studies contains profiles of 15 countries categorized by the criteria in this Benchmarking section. Additionally, a reference table summarizing the categories in detail is provided in the Benchmark Summary of this report.
BENCHMARKED FEATURES

This section details each benchmarked feature of a national ID system and considers differences in progress between a highly integrated state system and systems falling into one of the three aforementioned categories.

MATURITY OF FOUNDATIONAL REGISTRIES

One key feature of a robust and integrated national ID system is that it is based on unique ID credentials, commonly achieved using strong biometric identifiers such as 10 fingerprints and / or 2 irises. Facial biometrics are often added for human adjudication and, in some cases, disambiguation in automated recognition systems. In countries using unique IDs, each registry contains the ID to confidently link an individual’s identity across disparate registries. In most cases, a country’s civil or population and vital statistics registry (CR system) is the foundational registry. This registry contains core population information (such as births and deaths) and unique IDs to link identity to all other registries. Consequently, it is important that civil registry systems be as complete and accurate as possible, aiming for 100% participation from the population and digitization of the system (i.e., all corresponding records are available electronically in the civil registry).

However, some countries may develop a foundational registry even if their CR system is not robust. They can do so by directly building a registry from an expansive and accurate national ID enrollment. For example, India’s Aadhaar program lacks a fully mature birth/death registry system and about 80% of the nation’s population is registered. But the country has been able to build a foundational registry from scratch, thanks to its massive enrollment campaign. Because Aadhaar enrollment requires capturing a participant’s biometrics and biographical data (such as birth date, gender and address), India has developed the basis for a foundational registry without having to achieve a robust CR system.

Countries that fall in the Intermediate category generally lack a strong foundational registry, but are working to improve their existing registries. If their civil registries are digitized (some may still be paper-based but undergoing conversion), they will likely have moderate population coverage. Kenya, for instance, has a 58.4% birth registration participation rate and still uses paper-based certificates. However, administrators manually enter all data into Kenya’s Integrated Population

5 (Unique Identification Authority of India (UIDAI), 2015)
Registration System (IPRS) – which will serve as the primary foundational database for its ID system.

Greenfield countries lack a robust CR system, making it difficult to effectively track birth and death rates or keep accurate population records. Guinea, for instance, has low birth-registry participation (only 58%), and the registry is entirely paper-based; thus the system is subject to inaccuracies and data loss. Such countries have no immediate option for using their CR system as a foundational registry for a national ID system.

**NATIONAL ID SYSTEM**

A highly integrated national ID system:

1. Includes the entire population.
2. Has the ability to use biometrics to de-duplicate the target population; that is, create a unique ID and, in some cases, a token or personal identification number (PIN) for identity verification, typically in the form of a national ID card or e-ID/digital ID.

Highly integrated national ID systems are built on foundational registries that aim to include the country’s entire population. Although India’s Aadhaar program is not considered highly integrated, it does seek to include not just citizens but anyone living in the country: the end target is 1.2 billion registrants. By having a unique ID that does not necessarily entitle the user to citizenship or benefits, Aadhaar can include registrants regardless of status. Later in this report, we discuss how countries with minimally developed ID systems can begin strengthening them by targeting subsets of populations and then building from there.

Unique IDs are critical for reducing fraud and preventing duplicate entries into the system. They thus help ensure accuracy of data and minimize leakage of benefits (such as rations), because intended recipients can be identified and verified using biometric identifiers. India’s Aadhaar program, for example, captures fingerprint, face and iris data to de-duplicate residents and typically uses a single biometric identifier for verification. To ensure accurate de-duplication and verification, quality biometric samples are imperative. Quality is measured using proprietary and standards-based algorithms such as the U.S.-based National Institute of Standards and Technology’s (NIST) Fingerprint Image Quality (NFIQ) and ISO 29794-X (where X varies based on biometric modality). Standards also

---

6 (UNICEF, 2014)
exist for determining whether the biometric capture device can produce images of sufficient quality for automated comparison. These include the Federal Bureau of Investigation’s (FBI) Image Quality Specification (IQS) in the United States and the Unique Identification Authority of India’s (UIDAI) Standardized Testing and Quality Certification Directorate (STQC).

Countries in the Intermediate category generally have a national ID system in place, but it is not integrated with a strong foundational registry. Rwanda, for example, has a CR system that is not yet digitized (efforts are in progress), but it uses birth certificates (subject to inaccuracies) as a form of requirement for receiving a national ID card.7

Greenfield countries typically lack a unique ID system or foundational registry altogether. Alternatively, they may have functional registries that capture Unique IDs for a population subset (such as registered voters), which they can use as a springboard for building a foundational registry/database later. For instance, Guinea has worked to develop a digital electoral/voting register. To date, roughly 5 million people (about 87% of the voting population) are in the Election Register, and the government has collected biographic and biometric (4-10 fingerprints and a photograph) for each registrant. Guinea chose to issue unique IDs to a subset of its population, and it may be able to use this database in the future to include the remainder of the population.

**LEVEL OF INTEGRATION BETWEEN FOUNDATIONAL & FUNCTIONAL REGISTRIES**

Highly developed ID systems are useful to governments and citizens because they are typically integrated with a multitude of functional registries – and they have interoperable databases and systems. Such systems may include those needed to manage social security benefits, food or fuel subsidies, government payroll and passport issuance, to name just a few. Countries that have integrated their ID systems with their functional registries can more easily track benefits accessed by each user and can minimize benefits leakage (in forms such as “ghost” payroll payments or duplicated subsidy payments).

*Figure 1* depicts the ID4D integration model discussed in detail in the ID4D Integration Technology section.

---

7 (Nyamulinda, 2015)
The Unique ID system and Civil Registry are integrated through the ID4D Integration layer. This architecture preserves the modular nature of the model versus customized direct interactions.
In this model, the ID4D integration layer, which is standards-based, secure, modular and open-source, enables:

1. Stakeholders to interact through the ID4D Integration Layer, which is used for the common interchange of information among the constituent registries.

2. Stakeholders to provide (expose) services for others to use (consume) in the areas of: data management, matching (e.g., identification, verification), operations management and reporting.

3. Uses such as dynamically processing requests, receiving transactions, dispatching services, and temporarily persisting data. The ID4D Integration Layer receives service requests through the ID4D Integration Layer Adapter from the stakeholder institutions’ applications.

Estonia is an example of a country that has used a highly scalable integration layer to link its foundational systems (the National Population Register, or NPR, and national ID system) to functional applications using “X-Road” middleware. All such applications depend on data stored in the NPR, and can execute services based on relevant data extracted from the NPR. As a result, Estonian citizens can access a number of economic, social and political services using their national e-ID card, which acts as their primary form of identification. Estonia has thus established a highly integrated national ID system without the use of biometrics; it relies solely on a PIN, digital signature and encryption features to authenticate user identity.

Intermediate and Greenfield countries generally lack integration between functional registry systems. In many such nations, each registry provides its own type of ID to registrants, and any biographic or biometric data captured by these registries are not shared or linked across registries. In Sierra Leone, for example, fingerprint data captured as part of the country’s new national ID program (which covers 5% of the population) is not currently integrated with Sierra Leone’s existing social security program (16.7% of the population), which can capture both biographic and biometric data (fingerprints, irises and photographs). Consequently, there is likely overlapping data.

---

8 (e-Estonia, 2015)
9 (World Bank, 2014)
POLICY & LEGAL REGULATIONS

Mature ID systems are supported by a strong backbone of data privacy and e-transaction laws as well as policies mandating participation in the country’s civil registries. These policies are enforced by stop-gap implementations or clear penalties. The assumption is that participants’ private information will be available to multiple stakeholders. Thus any compromise of this data would significantly reduce public faith in the system. Data is protected when stored (and only for the duration disclosed) and while in transit, and is accessible only to those with appropriate credentials. Only relevant basic biographic information is collected, and it does not include data that could be used to profile and possibly discriminate against a target population.

In India, government regulators revisited its Information Technology Act (2000) in 2011 to clarify its rules surrounding security practices regarding sensitive personal data or information (SPDI) and ensure that as the *Aadhaar* program continued to grow, there would be scalable laws applicable to corporate organizations and individuals. As time progresses, it is important that countries revise existing laws to keep up with the proliferation of SPDI so that their national ID systems remain trustworthy as an enabler for access to services and not a detractor of personal freedom. Many Intermediate countries have data-privacy and e-transaction laws that are in the process of being passed or that require revisions to reflect the growing volumes and use of SPDI in government programs. In Kenya, for instance, an uptick in cyber-crime has prompted the government to mandate additional measures for digital certification in online transactions and to establish a National Cyber Security Strategy.

Greenfield countries generally lack data-protection or e-transaction laws, partly because they have limited digital registries.

INSTITUTIONAL STRUCTURE

Highly integrated national ID systems generally have become so because their countries have established an independent governing body or agency that oversees the system, or designated a ministry (such as the Ministry of the Interior or the Prime Minister’s office) to “own” the system or oversee multiple government registries.

By giving an overarching agency jurisdiction over the national ID system, a country can ensure that the system is developed independently of individual department interests. It is also important to establish a government mandate encouraging all departments to contribute (if necessary) and to cooperate to ensure that the national ID program operates at intended.
Consider Botswana, whose Omang national ID card program is run by the Ministry of Labor and Home Affairs (which includes the CR system and citizenship program). Botswana also has a strong government mandate to integrate its national ID card with a number of other registries. As a result, the Omang card is “organically linked” across registries from birth through death and can thus be easily integrated with diverse government services such as voter registration and passport enrollment.

Contrast Botswana’s experience with that of Guinea, where the Ministry of Communication & New Information Technologies is responsible for improving information and communication technologies (ICT) in each government sector. However, the government provides no overall direction for digitizing Guinea’s registries, and each ministry is responsible for maintaining its own registry. As a result, the Ministry of Communication & New Information Technologies has no real authority to drive improvements in the existing registries (including the civil registry) that could lay a foundation for a strong national ID system.

ACCESSIBILITY

Another important feature that defines the success of a national ID system is its accessibility and usability by its registrants. To ensure this, it is important for a country to develop an attainable plan to:

1. Register all of the country's participants, especially the rural and marginalized populations (“last mile”)

2. Define a strategy for providing its population with consistent access to services

In general, countries can leverage existing public offices/registrars (e.g. schools, post offices, civil registry offices) in order to register their main urban populations. In addition, they can also deploy mobile technologies for registering hard-to-reach people and setting mandates to improve the country’s fiber optics (internet) network and mobile tower capabilities (both of which are typically lacking in developing countries). India’s Aadhaar program, for example, has attempted to address this situation by setting up physical enrollment centers in rural villages (versus pushing online pre-enrollment, which was typical in urban areas). It has also made its banking transaction capabilities mobile phone-based, since cellular phone ownership is more ubiquitous than Internet accessibility.

In Intermediate and Greenfield countries, there is often much work that will need to be done to improve accessibility to the rural and remote communities. These countries often run the risk of further marginalizing parts of their population if their national ID systems are not accessible to their “last mile” groups (especially if there, for example, are security risks with accessing parts of the rural or remote areas).
In those situations, it would be important for the government to establish the necessary rapport with local leaders in order to build support within those hard-to-access communities for participating in a national ID program.

**ABILITY TO PROVIDE PHYSICAL CREDENTIALS FOR INDIVIDUALS**

Finally, some countries prefer to have the ability to provide physical credentials for individuals, such as e-passports or national ID cards. This feature is considered optional given identity can be asserted virtually simply by having the unique ID number, though some countries have historically provided cards and prefer to continue in this manner. Physical credentials are created upon successful enrollment into the Unique Identity System.
**BENCHMARK SUMMARY**

In this Benchmarking Report, we have identified the characteristics of a highly integrated national ID system and described three levels of progress on the ID4D integration maturity scale, which are summarized in Table 4 below and summarizes key concepts from this Report.

<table>
<thead>
<tr>
<th>Benchmarking Feature</th>
<th>Country Category</th>
<th>Greenfield</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil registry (birth/death and/or population)</td>
<td>• Non-digital</td>
<td>• Non-digital</td>
<td>• Yes – may be digital</td>
<td>• Yes – digital</td>
</tr>
<tr>
<td></td>
<td>• Poor population coverage (0-50%)</td>
<td>• Adequate but not comprehensive population coverage (51-89%)</td>
<td>• Adequate but not comprehensive population coverage (51-89%)</td>
<td>• High population coverage (90%+)</td>
</tr>
<tr>
<td>National ID system</td>
<td>• Does not exist, or:</td>
<td>• Exists but limited integration with foundational registry</td>
<td>• Exists but limited integration with foundational registry</td>
<td>• Exists and is integrated with foundational registry</td>
</tr>
<tr>
<td></td>
<td>• Has a limited start using a functional registry (covering population subset)</td>
<td>• Limited de-duplication capabilities</td>
<td>• Limited de-duplication capabilities</td>
<td>• Supports ability to de-duplicate/verify users using biometrics</td>
</tr>
<tr>
<td>Level of integration</td>
<td>• None – generally disparate functional registries</td>
<td>• National ID system has minimal to no integration with other functional systems/registries</td>
<td>• National ID system has minimal to no integration with other functional systems/registries</td>
<td>• National ID system is integrated with multiple functional registries</td>
</tr>
<tr>
<td>Policy and legal regulations</td>
<td>• None or, if any, they are specific to functional registries</td>
<td>• Exists or is in process</td>
<td>• Exists</td>
<td>• Exists</td>
</tr>
<tr>
<td>Institutional structure</td>
<td>• Lacking</td>
<td>• Exists</td>
<td>• Exists and is enforced</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4: Country Category Summary**
<table>
<thead>
<tr>
<th>Benchmarking Feature</th>
<th>Country Category</th>
<th>Greenfield</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility</td>
<td></td>
<td>• Lacking – though work may be in progress to expand network</td>
<td>• Exists for majority of population</td>
<td>• Exists for nearly 100% of population</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Least accessible regions may not have coverage</td>
<td>• Plan in place to reach the least accessible regions</td>
</tr>
<tr>
<td>Ability to provide physical</td>
<td></td>
<td>• Does not exist</td>
<td>• Exists (via ID card, e-passport, etc.)</td>
<td>• Exists (via ID card, e-passport, etc.)</td>
</tr>
<tr>
<td>credentials for individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The remainder of this study provides recommendations for improving the national ID systems of countries at each level. For more information on the countries referenced as examples in this Benchmarking Report, please see the Compendium of Case Studies, accompanying this report.
SCOPING REPORT
SCOPING REPORT OVERVIEW

The Scoping Report assesses mechanisms needed to support ID4D integration. A successful integration is contingent on a country’s ability to reshape existing mechanisms or create new ones as needed. Necessary mechanisms can be organized into the following categories:

- Policy, legal and regulatory considerations
- Institutional structures
- Business models
- ID4D Integration technology
- Standards for integration at a regional level

Below, we examine the key components of each category and describe strategies for overcoming common challenges.

POLICY, LEGAL & REGULATORY CONSIDERATIONS

To support a scalable, secure and efficient national ID system, countries need a clearly defined and enforceable legal framework. Because biographic and biometric data is sensitive, proper safeguards will increase reliability of the data, decrease redundancy and widen the system’s applicability.

A policy is a proposed or recommended action to achieve certain goals. In the context of national ID systems, a policy documents aspirations regarding the establishment of such a system. The most useful policies clearly define the vision, extent of coverage and scope of implementation of the national ID system. To ensure that the suggested policy is implemented as intended, countries need a legal safeguard, which can establish penalties for deviations from proposed procedure. Regulatory mechanisms ensure ongoing execution of legal safeguards. To establish such mechanisms, countries may create governing bodies, empower enforcement individuals or allow controlled use of power.

At minimum, countries must define laws that:

1. Keep data private and protect SPDI.
2. Regulate electronic transactions.
3. Mandate citizen and government participation in critical registries (typically the CR) that serve as foundational registries for the nation.

4. Define penalties and regulations for violation of laws.

Data-privacy and SPDI-protection laws

In effective national ID systems, the government can uniquely identify its registrants. To support this ability, the system stores enrollees’ private data in a foundational database that is then regarded as the single source of “truth” from which the country provides services. **Table 5** shows three core principles essential for data privacy and SPDI protection. Greenfield countries will likely need to start fresh in terms of their data-protection laws, while Intermediate countries can benefit from reviewing their policies’ comprehensiveness and strengthening them as needed.

<table>
<thead>
<tr>
<th>Principle</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose limitation</td>
<td>A data controller (government entity or private company) uses or collects data only for a specific purpose, predefined to the user. Data may not be used, shared or stored for any reason beyond the specific purpose.</td>
</tr>
<tr>
<td>Data protection</td>
<td>The data controller is responsible for embedding the appropriate technology and taking adequate measures to prevent unauthorized persons from accessing the data or to prevent data from being accessed for unauthorized reasons.</td>
</tr>
<tr>
<td>Consent to data collection and processing</td>
<td>The data controller informs system users that data is being collected from them (and subsequently used) and explains how long it will be used and who has access to it.</td>
</tr>
</tbody>
</table>

a  (European Digital Rights (EDRi) Papers)

Countries in the Advanced category that have established adequate and enforceable data-protection laws may consider expanding their policies to include international or cross-border transfers of personal information. South Africa, for example, passed new data-protection laws in 2013 that mirrored the framework of the European Union (EU), considered among the more stringent frameworks in the developed world. South Africa also created a data-protection authority and established international data-transfer and direct-marketing rules.\(^{10}\)

---

\(^{10}\) (Dhont & Woodcock)
Regulation of electronic transactions

As National ID Systems become increasingly automated, electronic transactions will continuously need to be monitored. Regulation and control of data in an electronic form is of complex nature, and needs increased Machine-to-Machine (M2M) communication for enforcement agencies to automatically get notifications of violations. Some fundamental components like identification and accountability must be well defined and ingrained when setting up enforcement laws for National ID systems. The regulation of e-transactions must follow certain fundamental principles enlisted in Table 6 below. These are indicative in nature and help gauge the types of principle that countries should consider.

<table>
<thead>
<tr>
<th>Principle</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic record definition</td>
<td>An electronic record is defined as one that is created, sent, stored, generated or received by electronic means.</td>
</tr>
<tr>
<td>Electronic signature definition</td>
<td>An electronic signature is defined as any sound, process or symbol associated with the electronic record with intent to sign it.</td>
</tr>
<tr>
<td>Legal recognition of electronic signatures,</td>
<td>Electronic records, contracts and signatures are stipulated as applicable to legal effect in the same way that physical equivalents are.</td>
</tr>
<tr>
<td>records and contracts</td>
<td></td>
</tr>
</tbody>
</table>

These laws should essentially stipulate that e-transactions are held to the same legal standards as written/physical transactions. Greenfield and Intermediate countries should put such regulations in place in conjunction with their data-privacy laws.

Mandated participation in critical registries

Although regulations and enforcement are important for national ID systems, it is equally critical to enact laws making participation mandatory for citizens. Without wide participation in critical civil registries (most importantly, birth and death), nations cannot confidently rely on “breeder documents” for foundational registries.

While many nations already have laws mandating birth and death registration, Greenfield countries need to establish them. Countries that have low registration participation even though they have defined such laws (they may fall into the Greenfield or Intermediate categories) can benefit by:

1. Understanding what is preventing citizens from participating in registration.
2. Developing temporary or permanent methods for enforcing the law.
Rwanda, for example, has a relatively low death-registration rate despite laws mandating participation. Yet it relies heavily on its civil registry to distribute its national ID cards. To improve death-registry participation, Rwanda intends to make a death certificate a requirement for burial.\textsuperscript{11} 

### Regulation and enforcement

Once policies are in place and a country has framed them with legal obligations, regulation and enforcement mechanisms are needed to sustain the ideals laid out in the policy and legal safeguards. Such mechanisms can take forms including compliance reports, audits and progress monitoring. In France, for example, the Commission Nationale de l'Informatique et des Libertés (CNIL) (National Data Protection Authority) is authorized to enforce data-privacy laws. CNIL agents perform online inspections and issue compliance orders to companies that have violated the law. In accordance with French Criminal Code, a misdemeanor is punishable by up to five years’ imprisonment. Table 7 summarizes principles for designing effective policy, legal and regulatory frameworks.

Setting up national ID systems is a complex activity and cuts across many areas of governance. As the examples cited here suggest, there is no single “correct” approach, given that countries at different maturity levels have diverse priorities. Advanced nations have opportunities to reinforce their approaches by better protecting citizens’ privacy and their right to “be forgotten.” Intermediate countries can make their current systems more efficient by incorporating automation while keeping electronic transactions secure. Greenfield nations can learn from the successes of Advanced and Intermediate nations and use the resulting insights to build and scale their systems quickly.

An example of an advanced approach to establishing a regulatory environment is the European Commission’s Electronic identification and trust services (eIDAS), which “aims at boosting the user convenience, trust and confidence in the digital world, while keeping pace with technological developments, promoting innovation and stimulating competition.” This initiative recently gained political level agreement, and related policies and regulations will be developed once formally adopted in September.\textsuperscript{12}

\textsuperscript{11} (Nyamulinda, 2015)  
\textsuperscript{12} (European Commission Directorate General)
<table>
<thead>
<tr>
<th>Table 7: Principles of Policy, Legal and Regulatory Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Legal</td>
</tr>
<tr>
<td>Regulatory</td>
</tr>
</tbody>
</table>
INSTITUTIONAL STRUCTURES

Once a country has defined mandates for establishing a national ID system, it must designate an appropriate governing body to oversee implementation and maintenance of the system. This arrangement varies across countries with an ID system, but ideally the system is run by one of two bodies:

1. An autonomous technical agency or governing body, which has overarching jurisdiction over multiple ministries.

2. A ministry (such as the Ministry of the Interior, Home or Justice) that has jurisdiction over multiple registries (most importantly, the civil registry).  

Although both scenarios offer different advantages, they share several key success factors. First, the national ID system is owned by an entity that has the authority to carry out its mandate without being hindered by bureaucratic obstacles or conflicting ministry priorities. If the governing body lacks authority over the activities of other ministries, taking an integrated approach to developing the national ID system may prove challenging.

Second, both scenarios integrate the operations of the digital ID program with civil registration activities. This is valuable because a country’s civil registry usually constitutes the backbone of a digital ID program, thus both programs need to be aligned. Typically, countries in the Advanced and Intermediate categories build their digital ID programs as part of a campaign to improve their existing Civil Registration and Vital Statistics systems (CRVS) (deemed “first generation” cases), or use their digital ID programs to build a new population database from the ground up (“second generation” cases).  

Nevertheless, countries need to take care to minimize situations in which inter-agency competition may erupt. In India, for example, the Aadhaar program is overseen by the Unique Identification Authority of India (UIDAI), an independent agency. Aadhaar began in 2009 and was launched almost in parallel with India’s National Population Register (NPR), which began in 2010. The NPR sought to register only Indian citizens rather than including migrants and temporary residents, which Aadhaar includes. Over the years, controversies have arisen frequently between the NPR and UIDAI, owing to the fact that both request overlapping data

13 (Gelb & Clark, Identification for Development: The Biometrics Revolution, 2013)
14 Idem.
(biometric and biographic) from residents and seem to have duplicative objectives. Consequently, even today, political debate persists on whether to eliminate one of the two programs.

Greenfield countries may not have an overarching mandate to develop a national ID program. In such cases, it may be more realistic (though not as ideal) to have a single functional registry (such as social security or an elections commission) own the registration and data collection of target users. This, however, is not generally recommended for the following reasons:

1. Some agencies are more stringent than others regarding credential validation (also frequently known as “breeder document” authentication), and different agencies may have different motives for collecting biometric and biographic data. If the government requires these registries to expand to include the entire population, much rework will have to be done to collect a second round of enrollment data.

2. There is, from the outset, a lack of integration with other key registries, which can prove difficult to overcome when the country seeks to scale its ID system to a national level.

---

15 (Unique Identification Scheme (UID) & National Population Register (NPR), and Governance)
Three critical aspects of designing an appropriate business model for developing nations are:

1. Developing a fair fee structure to the resident that allows financial independence to the system
2. Enabling a variable fee structure allowing free national ID to marginalized populations
3. Leveraging the ID system capacities to prevent fraud, reduce leakage and enforce policy resulting in public savings to sustain the overall costs

Countries can implement national ID and information and communication technology (ICT) systems through public contracts, such as public procurement and public-private partnerships (PPPs). National legislation may offer additional options that are fit for purpose. Public procurement and PPPs involve similar business models, but PPP projects differ from traditional procurement projects in a number of ways. Specifically, in PPP projects:

- **All phases of a project are awarded to a single contractor**, while in many countries traditional procurement may force awards to different companies (across design, build and maintenance phases). The traditional approach thus adds complexity, which can lead to difficulties as the project moves from phase to phase.

- **The contractor bears most of the project costs**. The government and the business model implemented will repay the sum on the basis of the agreed outputs. Typically, the contractor or consortium will form a special company called a “special purpose vehicle” (SPV) to develop, build, maintain and operate the ID system for the contracted period. The contractor through the SPV is responsible for the initial investment with a combination of equity and private debt, which usually result in higher financial costs due to higher rates and dividend distribution.

- **Project costs are predetermined**. The contracting authority (the government) undertakes to pay a specific sum if outputs are delivered as agreed. These costs reflect the risk evaluated by the private contractor and the financial costs of private funding.

- **The procurement process is more time consuming and complex** than traditional procurement processes. Therefore, the PPP model is best suited for
projects requiring a certain level of investment (for example, more than US$10 million).

Below, we take a closer look at the two business models.

**Public procurement**

Governments may choose to fund all of the capital expenditures and operational expenses for improving the transparency of and retaining the national ID system in the public domain, and look to the private sector to bring in needed expertise and efficiencies. The contractor is paid a lump sum for completed stages. This approach is recommended when public funding is available, and only if the public authority has enough expertise and resources to manage the selected contractor(s).

Generally assimilated to a public and noncommercial asset, the ID system can also be funded by tax payers at its inception, and then by public spending after implementation. For example, additional funding can come from fees paid by citizens for document issuance (passports, national ID cards).

It is of interest to consider the two different models described below:

<table>
<thead>
<tr>
<th>1. Implementation of <em>Aadhaar</em> in India</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Unique Identification Authority of India was established in 2010 as an attached office of the Planning Commission of India, which aims to provide a 12-digit unique <em>Aadhaar</em> number to all citizens of India. By the end of July 2015, the government will have spent a total of <strong>US$940 million</strong>. Integration of schemes’ subsidies as well as certain housing, education and health programs is one of the <strong>main sources of revenue for <em>Aadhaar</em></strong>. According to a cost benefit analysis study done by the National Institute of Public Finance and Policy (NIPFP) in 2012, the investment on the Aadhaar project would provide a return of as high as <strong>52.85% to the government</strong>.</td>
</tr>
</tbody>
</table>
2. Implementation of NADRA in Pakistan

Pakistan is an example of an Advanced country with a sound business model that meets the above critical success factors. Pakistan established the National Database and Registration Authority (NADRA) in 2000.

- NADRA operates on a chargeback model, whereby it charges a fee to the government and other organizations for services provided. For example, banks are charged around 35 rupees each time they request NADRA to authenticate an individual when they open an account. With around 55 million such transactions that leverage NADRA’s systems and generate income, NADRA has become financially self-sustaining.

- NADRA competes for projects both within and outside of Pakistan. Income from foreign projects amounted to USD $17.6m in 2013, which was reinvested back into the corporation’s operations and infrastructure. In this way, NADRA has been able to operate without a regular budget from the Pakistan government for a number of years. NADRA has delivered projects for Kenya, Sri Lanka, Sudan, Nigeria, Bangladesh and also for the UNHCR (Biometric Refugee Registration System).

An underlying assumption of the pay-per-transaction business model is that the benefits of registering for a national ID are clear and convincing to the population encouraging them to register and assert their identity to access various services.

Public-Private Partnerships (PPP):

PPPs can enable governments, particularly those lacking in-house technology expertise, to deploy and sustain modern ID systems. This model involves financing from various private sources, in some combination of equity and private debt. The ratios depend on negotiations between lenders and shareholders.

- The private contractor leverages the value of the ID system to introduce a fee system based on authentication requests raised by private companies (financial sector, tourism, travel agencies, etc.) or public sector. It would be a good practice to decrease the fees in this model by leveraging savings from fraud mitigation, subsidies and grants scheme optimization.

Chargeback models have immediate effect after implementation, while policy efficiency increases over time, saving substantial public funds. Governments may also decide to mix these two options to decrease costs to residents, and to introduce a variable fee structure allowing free national ID cards for marginalized populations.
The legal form of the contract used to support the chosen business model will depend on four factors:

- Available public funding
- In-house expertise and resources
- Overall estimated costs
- Risks and ethics issues related to transferring management of the ID system to a private company

In conclusion, both procurement options have unique benefits. The PPP remains a powerful operational instrument, but to use it, countries must address ethical issues and transparency limitations first. For example, Governments could invest in the SPV equities to increase their level of control.
Technology options for integration across the country categories were developed from the model shown in Figure 1: ID4D Integration Model in the Benchmarking Report. Vital events (such as birth, death, marriage, divorce and adoption) and the institutional stakeholders responsible for registration of these events (for instance, social protection institutions, courts and electoral commissions) are captured at the top of the diagram. These functional components are envisioned as integrated with back-end technical components (including foundational registries, vital statistics and credential issuance).

**HIGHLY INTEGRATED IDENTIFICATION REFERENCE MODEL**

The model depicted in Figure 1: ID4D Integration Model serves as a target for countries as they move to integrate their existing registries into a holistic framework supported by the foundational registries. The model logically groups external stakeholder organizations separately from country-specific identity technologies that will serve as the infrastructure for delivering services to residents.

Key components of the model are defined below. Additional details are provided in Annex 2: ID4D Integration Model.

- **Functional registries** – systems developed for specific applications (elections, tax, social protection, pensions)
- **Law enforcement integration** – integration with local, national, regional and international policing agencies to strengthen national security
- **Other country integration** – integration with neighboring countries to form a regional identity system that can address matters of policing, national security and servicing of migrant populations
- **Residents and private institutions** – resident and private institution access to the government’s foundational registries; residents include citizens and non-citizens (such as refugees), who may seek (and be eligible for) benefits
- **ID4D integration** – a top-level integration layer, with standardized services that orchestrate all transactions processed in the foundational identity management system(s)
- **National identity** – universal, multi-purpose system capable of supporting all legal identity needs across applications
- **Civil registration** – legal registry of all births and deaths that occur in the country as well as during foreign missions
- **Vital statistics** – data mart of vital events (birth, death, marriage, divorce, adoption) gathered from various functional registries.
- **Credential issuance** – creation of a token (national ID card, voter ID, ePassport) used by individuals to affirm their identity

The model can be used to develop a country-specific integration strategy and roadmap linking existing components in a scalable, methodical way. These topics are covered in the next section of the study, Strategy and Roadmap for Implementation.

**ID4D INTEGRATION LAYER**

ID4D integration is achieved through a lightweight abstraction layer that orchestrates all transactions (e.g., enroll identity, retrieve information, and authenticate identity) within the Identity ecosystem. This layer serves as a gateway between institutions’ registries, the foundational registry(ies), and other stakeholders (e.g., the public). The intent of the integration layer is that there are no direct links between any of the databases. Rather, the integration layer serves as the common link between all registries.

It is important to note that the civil registry serves as the foundation for the Unique Identity System, but there is no direct connection shown on the reference model since this interaction occurs through the integration layer. An example of the linkage is upon birth, a request is received by the civil registry to create a record for the subject, but no Unique ID is established until a biometric enrollment is processed by the Unique Identity System. Once the Unique ID is created for this record, it is provided to the civil registry through the use of pre-determined secondary identifiers (e.g., name, DOB, record ID).

Similarly, the vital statistics registry utilizes the ID4D Integration Layer for data operations – that is, to extract requisite data exposed by the registry(ies).

The ID4D Integration Layer, as described in more detail below, is used as a means to standardize the interchange between each functional registry and each foundational registry. This is achieved by Service-Enabling each registry through an ID4D integration Adapter so that each functional and foundational registry ‘speaks’ the same language.

The ID4D Integration Layer Architecture – that is, what the ID4D Integration Adapters do and how they do it, is detailed in the Technology Options section.

Stakeholders interact using a standardized ID4D Integration architecture responsible for common management of all underlying information exchanges. As such, this layer acts as an abstraction layer for all compliant stakeholder
subsystems and is responsible for dynamically processing the requests, receiving the transactions, dispatching services, and managing any temporary or persistent data in the foundational system(s).

The ID4D Integration Layer consists of a series of adapters, depicted in Figure 2 below, and underlying monitoring and configuration components.

**DESIGN PRINCIPLES**

An effective ID4D integration layer is based on the following design principles, which are indicative (not prescriptive):

- **Standards based** – leveraging RESTful or SOAP / XML standards
- **Open source** – using open-source technologies where possible
- **Secure** – encrypting data at rest and in transit; supporting certificate verification and non-repudiation
- **Modular** – allowing for scalability and high availability by having redundant modules and avoiding a single point of failure
- **Decentralized** – having the bulk of the ID4D integration logic reside in ID4D integration adapters

**Figure 2: ID4D Integration Layer Adapter Functional Diagram**

<table>
<thead>
<tr>
<th>Stakeholder Institutions’ Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Registries</td>
</tr>
<tr>
<td>ID4D Adapter</td>
</tr>
</tbody>
</table>

**ID4D Integration Layer**

e.g. HTTPS Transport Layer Security (REST or XML/SCAP based)

<table>
<thead>
<tr>
<th>ID4D Adapter</th>
<th>ID4D Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration System Notional Services</td>
<td>Civil Registration System Notional Services</td>
</tr>
<tr>
<td>Registration Operations</td>
<td>Data Operations</td>
</tr>
<tr>
<td>Operational</td>
<td>Reporting Functions</td>
</tr>
<tr>
<td>Registration Operations</td>
<td>Data Operations</td>
</tr>
<tr>
<td>Operational</td>
<td>Reporting Functions</td>
</tr>
</tbody>
</table>
The central elements of the ID4D Integration Layer are limited to:

1. **Monitoring** – Transactional information (no data) available for reporting and dashboarding

2. **Service Registry** – Component in charge of providing the list of services available for each registry that is integrated

3. **External Integration** – Certification Authority integration for authentication, where applicable

The bulk of the logic in the ID4D Integration Layer resides in the ID4D Integration Adapters, which is described in the following section and depicted in **Figure 3** below.

---

**Figure 3: ID4D Integration Layer Adapter Detailed Diagram**

The core components of the ID4D Integration Layer Adapter are:

- **Message queue client** – a third-party client library that implements commercial off-the-shelf (COTS) message-oriented middleware.
- **Message consumer** – listener of inbound messages of the message queue broker.
- **Broker connection** – aids in connecting to the message queue broker and maintains connection details in a configuration file.
- **Gateway manager** – coordinates components of the ID4D integration layer adapter and pushes response back to the outbound message queue.
- **Data parser/transformer** – is responsible for input payload parsing and for constructing the response message; uses certain utilities for decoding and transforming.

- **Logger** – handles all logging required during processing (time stamping, transaction, message, reference ID, function call, parameters, results). Log levels are maintained and enabled via a separate configuration file.

- **Registry adapter** – handles registry-specific data access.

For information on specific technology options and a general process for technology selection, see the Technology Options section.

At a high level, ID4D integration adapter logic flows through the following steps:

1. De-queue inbound messages from the message queue.

2. Log the messages and reception/processing times in the data store for service-level agreement (SLA) measurements and further analytics. Logging happens at each processing step, to ensure that steps and results are captured.

3. Decode the messages to understand the function to be performed and to verify integrity of the message.

4. If required by the function, gather biographic and/or biometric data required to perform the function from the back end.

5. Call the registry for the result.

6. When the registry returns the result, package the result, conforming to the Interface Control Document (ICD) into a response message. Place this message in the message queue.

7. Log transaction times and results for further auditing.

**TECHNOLOGY OPTIONS**

The **ID4D Integration Layer Adapter** will be a hybrid of custom-developed and commercial off-the-shelf (COTS) products – as shown in Table 8. The technology stack for the ID4D Integration Layer will be defined based on stakeholder-specific requirements. As a result, key considerations for evaluating and selecting COTS products include the following.

- Current stakeholder technologies in place and level of interest in maintaining, enhancing/updating or replacing these technologies.
- **Requirements**
  - **Performance, scalability and availability** – Modular, redundant queue infrastructure will allow for scaling to meet throughput demands and will avoid a single point of failure.
  - **Network infrastructure restrictions** – End-to-end communications infrastructure, along with specific firewall rules (such as port utilization), will be identified and included in the ICD for information exchange.
  - **Security by design** – Security requirements will be agreed to and documented in the ICD, and role-based access will be enforced by the service provider (such as a registry).
  - **Cost (open source versus COTS, along with corresponding support)**

The technology options for the Integration Layer Adapter are provided below.

<table>
<thead>
<tr>
<th>Table 8: ID4D Integration Layer Adapter Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
</tr>
<tr>
<td>Message Queue</td>
</tr>
<tr>
<td>Message Consumer</td>
</tr>
<tr>
<td>Broker Connection</td>
</tr>
<tr>
<td>Gateway Manager</td>
</tr>
<tr>
<td>Data Parser/Transformer</td>
</tr>
<tr>
<td>Logger</td>
</tr>
<tr>
<td>Registry Adapter</td>
</tr>
</tbody>
</table>
ADDITIONAL INTEGRATION APPROACHES

The ID4D Integration model supports other integration approaches given the modular nature of the architecture. The Centralized model described above can be adapted to accommodate Regional, Federated, or Hybrid models as well.

Regional

Once a country has accomplished its ID4D integration objectives and has an appropriate foundational ID system in place, it may consider integration at a regional level, linking its system with those of neighboring countries. The data exchanged will depend on policy and could be limited to biometric information, to exclude of biographic data, in order realize cost savings resulting from common Identity Services (e.g., de-duplication, verification). Owing to the sensitive nature of data sharing beyond country borders, data is encrypted such that only parties with the corresponding keys may access the information. Alternatively, personally identifiable information is not exchanged; extra-jurisdictional systems (acting as identity service providers) only provide a means to verify a citizen’s claim of identity to a third party (the service provider). The sections below describe two examples of this approach to regional identity integration.

Federated

In this model, each partner country has its own functional registries but offers partners the ability to federate biometrics-based and / or biographics-based searches against each other’s identity systems. This will enable agencies to more accurately identify migration, fraud, and illegal activities of persons in their domain.

Hybrid

This approach combines elements of the previously described integration approaches.
Project STORK (Secure idenTities acrOss boRders linKed)\textsuperscript{16}

Project STORK was established as a European e-ID interoperability platform that lets citizens access electronic information across borders by using their national e-ID for authentication. Initiated in 2007, the project involves 14 EU member states. Cross-border user authentication was tested through five pilot projects that used existing government services in member states. The expectation is that additional service providers will connect to the platform, increasing the number of cross-border services available to European users (such as those seeking to obtain university papers without needing to do so in person). Users enter their personal data using their national e-ID, and the STORK platform obtains the required authentication from the issuing government.

The STORK platform identifies users who are in a session with a service provider, and sends this data to the service. While the service provider may request various forms of data, users control the data that is sent. Users’ explicit consent is required before data can be sent to the service provider. This user-centric approach meets the legislative requirements of the countries involved, which mandated concrete measures to guarantee protection of citizens’ fundamental rights. Building on the success and results of STORK, the STORK 2.0 project has introduced four new pilots.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{STORK Platform Model}
\caption{STORK Platform Model}
\end{figure}

Users enter an online session with a service provider and provide personal data using their national e-ID. The STORK platform requests their permission to relay the personal data to their national eGovernment portal for identity authentication. Once authentication is provided, it is relayed back to the service provider. The STORK platform does not store any personal data, so no data can be lost.

\textsuperscript{16} (STORK, 2012)
**X-Road EU**

Estonia’s integration platform, X-Road, is described in Estonia (and shown in Figure 18) as the heart of the nation’s eGovernment offerings. X-Road EU (depicted in Figure 5) uses the same architecture to also serve cross-border functions not served by existing regional initiatives. It does so by using web services to allow different public-sector information systems to exchange data safely and according to predefined standards. The proven X-Road core technology used by Estonia since 2002 was the basis of X-Road EU. In the X-Road EU model, encrypted data is directly transferred through secure servers, ensuring that data is exchanged only with relevant parties. The center stores only audit log information about the data transfer, not the data itself. The central server also handles certification management, including checking integrity of the secure servers’ logs. X-Road EU enables owners of any two (or more) information systems to communicate with one another in a repeatable, scalable way and fosters speedy integration. X-Road EU therefore serves as a model for regional integration, especially where there is no agreed-upon approach for organizational data exchange.

---

**Figure 5: X-Road EU Model**

---

17 (X-Road Europe, 2015)
STRATEGY AND ROADMAP FOR IMPLEMENTATION
STRATEGY OVERVIEW

The high-level strategy for ID4D integration is a phased approach starting with existing registries and corresponding data sets and providing a means to service-enable them in order to achieve integration through shared services.

The roadmap offers ID4D Integration guidance for each country category in order to provide stakeholders with secure and efficient access to information.

HIGH-LEVEL STRATEGY

The ID4D integration strategy places unique identity at the center of disparate government ministries and agencies, enabling government functions to share information more efficiently, securely, and cost effectively. Thus, it also creates a more resident-centric approach to facilitating access to government services while also reducing both exploitation and systems redundancy.

The ID4D Integration strategy consists of three modular phases, as shown in Figure 6.

Phase 1 begins with conducting a country-specific assessment to understand the existing state of integration between the functional and foundational registries. Once current state is understood, plans are made to establish a time-phased integration timeline for the country’s registries – ideally starting with those that are most achievable, impactful, and of highest priority to residents. Once initial plans for integration are defined, ensure the Governing Body is in place. This Governing Body will ultimately sign-off on technology decisions and confirm the pre-requisites are in place (funding via an appropriate business model for the country and political support). The architecture of the integration approach is tailored to country-specific needs, paving the way for the technology selection process. In regions where communications infrastructure is limited, the technical solution should consider an offline operational capability in which transactions are stored and then forwarded when connectivity is available.

Phase 2 includes execution of an initial expansion to validate the decisions made in Phase 1. Specifically, the effectiveness of the Governing Body, the technology choices (data model, security and so forth), and the integration timeline are validated based on this lower scale (Pilot) implementation exercise. The output of Phase 2 is an updated timeline for integration based on learnings from this phase.
Phase 1: Planning/Establishment

- Capture specifics of country’s existing state of integration
- Establish time-phased goal for increased integration
- Establish Governing Body – including identification of key decision makers
- Determine architecture integration approach
- Make appropriate technology selection

Phase 2: Initial Expansion

- Lower scale implementation to validate:
  - Effectiveness of governance and delivery group
  - Technology - Data Model, Security, and SLA decisions
  - Expected timeline that can be reasonably achieved for subsequent integration and capability expansion

Phase 3: Increased Integration Capability

- Production scale implementation:
  - Starting with Integration of the most critical registries
  - Using the refined timeline from Phase 2

Phase N: Increased Integration Capability

- Repeat this phase for remaining registries until target integration levels are achieved

KPIs will measure improvement over time (such as # registries integrated, % population coverage, % marginalized covered, transaction volumes (de-duplicate, verify))

Phase 3 (onwards) includes the production scale integration of the registries accordingly to the refined plan from Phase 2. Given some countries may have a number of registries left to integrate, Phase 3 would be repeated until target integration levels are achieved.

In every phase, effective change management and communication/outreach are critical for successful uptake of services by residents.

The following best practices can help ensure successful passage through the phases. Note that having a strong foundation for integration is critical in ensuring success for the country’s identification ecosystem.
- **Regulation** – Integration of information sources, especially when the information spans jurisdictions, may require data sharing and/or data access legislation and corresponding ID4D Integration Model information technology to enforce such regulations.

- **Data Protection** – In conjunction with data sharing policies, data protection that governs how data is to be protected as a result of the integration process will need to be accommodated through ID4D Integration Model information technology.

- **Exchange Definition** – Whether through national or international standards (e.g., National Information Exchange Model or NIEM) or through bi-lateral agreements (i.e., Interface Control Documents or ICDs), what information is exchanged and how it is exchanged must be defined.

- **Service Discovery** – the ID4D Integration Model is built using Service Oriented Architecture patterns in which integration is achieved through exposing and consuming services.

The Exchange Definition is at the heart of the ID4D Integration strategy. It provides a means of integrating various repositories so that government and private sector stakeholders can efficiently access data that they are authorized to receive.

The overall strategy for building out ID4D Integration technology is transposable to every context; however, the roadmap to achieve the desired result differs based on the characteristics of the target environment, which have been categorized into three areas. The ID4D Integration Roadmap for each is provided in the next section.
GREENFIELD INTEGRATION

As described in the Benchmarking Report, a Greenfield country has rudimentary or no registry integration (either directly, through custom interchanges, or through an SOA). Services are not contemplated, and it is likely that no public-facing presentation capability exists. Speedy integration of a national ID infrastructure (such as the country’s foundational registry) into the identity system is critical.

As shown in Figure 7, a Greenfield country will aim to improve its civil registry as a first priority, then strengthen integration across all registries by introducing a Unique Identity System (such as a national ID).

Registries or functionalities that are to be integrated using the ID4D Integration model will need to be service-enabled. This is typically done through an adapter which brokers queries between a registry (database) and the requestor – directly or through a security layer. The adapter queries the database using a language native to the database (e.g. SQL) to retrieve the information requested and then creates an ID4D Integration compliant message in SOAP/XML or RESTful JSON format.

The integration process necessitates that both the provider(s) and the consumer(s) of information agree on the content and mechanism by which information is exchanged. This is established and maintained through a Service-Enablement Governance Process. Key steps are outlined below, in which stakeholders and ICT organizations come to an agreement on what, and how, information is integrated/shared. As stated above, this is typically formalized in an Interface Control Document (ICD) through national standards such as the National Information Exchange Model (NIEM), and international standards (ISO 19794-X for...
biometric exchanges). Service-Enablement Governance Process Steps are shown in Table 9.

<table>
<thead>
<tr>
<th>Key Activity</th>
<th>Associated IT Tasks</th>
<th>Key IT Outcomes/ Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Define service(s)</td>
<td>1. What service offerings and corresponding data elements (i.e., source registry(ies))&lt;br&gt;2. Access grants (who will have access)&lt;br&gt;3. Service consumers</td>
<td>• Design Document</td>
</tr>
<tr>
<td>2. Define data access</td>
<td>1. How will registry data be accessed to be made available through the service(s) (e.g., SQL, LDAP)</td>
<td>• Design Document</td>
</tr>
<tr>
<td>3. Define integration technology</td>
<td>1. What messaging protocol will be used (e.g., SOAP/XML, REST)&lt;br&gt;2. Through what means (e.g., Enterprise Service bus (ESB))</td>
<td>• Technology selection</td>
</tr>
<tr>
<td>4. Define audit logging</td>
<td>1. What transactional artifacts will be logged (typically level-based: Off, Minimal, Verbose)</td>
<td>• Design Document</td>
</tr>
<tr>
<td>5. Define presentation layer</td>
<td>1. Portals&lt;br&gt;2. User Interfaces</td>
<td>• Design Document</td>
</tr>
<tr>
<td>6. Establish certificate authority</td>
<td>1. Public key cryptography will be used to secure data at rest in transit and along with the public key infrastructure needed for ePassports, eIDs, and machine certs, etc. One or more Root CAs will need to be established through government procurement or through a 3rd party – accredited by the cognizant government authority.</td>
<td>• Design Document</td>
</tr>
<tr>
<td>7. Integrate with credential service personalization service providers (optional)</td>
<td>1. Many countries issue credentials to citizens and/or residents&lt;br&gt;2. Examples are eID, ePassports, driver’s licenses, health IDs, etc.&lt;br&gt;3. Personalization may be decentralized or decentralized</td>
<td>• Design Document</td>
</tr>
<tr>
<td>8. Publish interchange standards</td>
<td>1. As interchange details are defined they should be captured, signed-off and published</td>
<td>• Interface Control Document (one per stakeholder)</td>
</tr>
</tbody>
</table>

Table 9: ID4D Service-Enablement Governance Process Steps
INTERMEDIATE INTEGRATION

As shown in the roadmap in Figure 8 below, an Intermediate country may have some registry integration through direct, custom interchanges, but likely not services enabled through an SOA.

Such countries will aim to improve integration of such registries using the ID4D integration layer, based on a common service catalog.

![Figure 8: Intermediate Country Integration Roadmap](image)

- Increase Civil Registry
- Achieve 90% registration of Unique IDs
- Continue to integrate functional & foundational registries

These countries have likely established ICDs and achieved service-enablement. However, depending on their circumstances, they may not have portal integration of services, whereby access to information by government agencies, businesses and/or the public is done through self-service portals in which registries follow ID4D integration patterns.

Countries can choose from multiple portal technologies available for the presentation layer – not just from big players such as IBM and Oracle, but also from open-source suppliers like Apache and Red Hat / JBoss. As the portal is the “front door” to the integrated national ICT, role-based user provisioning is essential. Typical roles include General Population, Commercial, Public Servant and Public Servant Supervisor.

ADVANCED INTEGRATION

An Advanced country will have registry integration through an SOA and will seek to expand its service catalog, extend its messaging layer and expand its stakeholder base, as shown in Figure 9.

Estonia is categorized as Advanced and has provided integration services used throughout the nation. That being said, the Estonia integration model requires
that registry owners extend core integration services to meet needs including the following:

- **Guaranteed delivery** – Requestors must “re-ask” for information that is not received the first time, even if there is acknowledgement that the message was received.

- **High-availability** – Integration is achieved through modularity to avoid single points of failure. Redundancy and fail-over mechanisms should be considered.

- **Publish / subscribe** – The integration layer typically supports point-to-point registry integration as defined in an ICD. Advanced countries may wish to offer a means for stakeholders to subscribe to a registry (or entity therein) such that when the registry owner Creates, Updates or Deletes the entity, that action is published and all subscribers are informed in near real-time. This mechanism can be part of the integration layer – the advantage is that the impact of code modifications to registry owners is minimized; the disadvantage is that the integration layer becomes more complex.

- **Role-based access control** – The registry owner defines who may access what information in the registry. This is typically enforced through an identity and access management mechanism at the registry. However, it could be established at the integration layer through the service-enablement governance process.
Countries can measure their ID4D integration progress for effectiveness, by assessing factors related to coverage, integration level, cost and integration performance, among others. Figure 10 shows a scorecard that nations can use to track these aspects of program effectiveness.

<table>
<thead>
<tr>
<th>ID4D Integration Balanced Scorecard</th>
<th>2015</th>
<th>2016</th>
<th>YoY Change</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Coverage &amp; Growth</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Population Coverage (%)</td>
<td>%</td>
<td>%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Unique Users</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of Births Registered in Current Year</td>
<td>%</td>
<td>%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of Registered Births in which Birth Certificate was Issued</td>
<td>%</td>
<td>%</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level of Integration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Registries Integrated</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Unique Services Provided</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Self-Service Portals</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cost Benefits</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average E2E Cost per User in System</td>
<td>$</td>
<td>$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of Operations Saved by Gov to Date</td>
<td>$</td>
<td>$</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integration Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Transaction Volume (per day)</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Response Time (per transaction)</td>
<td>--</td>
<td>--</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Service Uptime (per month)</td>
<td>%</td>
<td>%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The intent and description of the 4 main scorecard categories are as follows:

1. **Coverage & Growth** – Measures the ID4D system’s coverage of the country’s population. Important for assessing inclusion of hard-to-access populations as well.
2. **Level of Integration** – Measures the number of registries, services and portals that have been integrated (such as passport services, social security and food or fuel subsidies).

3. **Cost Benefits** – Measures ongoing savings. Over time, economies of scale can help lower in average E2E cost per user. Additionally, governments may operate with fewer costs, thanks to more efficient distribution of benefits and services (including the ability to cut off excess payments such as ghost payrolls).

4. **Integration Performance** – Provides key performance indicators (KPIs) for the system’s technical performance. KPIs suggested in the scorecard are summary indicators, but countries can choose to measure a large variety of performance and service-related SLAs, as defined below.

**Performance Service Level Agreements (SLAs)**

By using industry standard Business Activity Monitoring (BAM) methods, countries can monitor the performance effectiveness of their systems. Countries can utilize open-source software to analyze their ID4D Integration layer messages for:

- Transaction volumes
- Transaction types
- Response times
- End-to-end process timing
- Error log / error type and severity

Performance-based Service Level Agreements, such as those listed above are monitored through the ID4D integration layer, where message queues manage discrete transactions. Performance metrics should include baseline characteristics such as CPU usage, memory usage, response time, transaction volume, etc.

ID4D Integration performance can be further analyzed by time of day, day of week, etc., by registry, and by requestor. With this type of information, it becomes much easier to identify bottle necks and to adjust accordingly and to measure success.

**Service SLAs**

The following metrics are typical service availability level agreements that could apply to ID4D Integration services and corresponding systems. Each commitment is listed along with a brief description:

1. **Service hours:** days of the week and hours per day that each defined
2. **Service availability**: minimum agreed availability level for the service component. This is the average amount of time each month the defined service is available to end users (expressed as a percentage).

3. **Scheduled downtime**: hours during which the service is routinely scheduled to be unavailable to end users. For identity applications, this typically represents nightly downtime to perform batch processing, system back-ups and other tasks. During these times, the system may be accessible to end users. However, the operations team has the option of making the service unavailable and does not measure or report.

4. **Measurement period**: time during which service level is measured.

5. **Target definition**: criteria determining whether a service is available.
CONCLUSION

The report stresses that digital identification is a vital component to any country identification ecosystem. Providing unique identification services to stakeholder entities in a standards-based, secure manner will increase information exchange and decrease costs through process automation and self-service capabilities. The study recommends that digital identities, and the corresponding Unique Identification System, should be kept separate from specific registries, applications and use cases; the ID4D Integration Model will provide the means to associate Unique IDs with the corresponding registry(ies) without ‘hard-coding’ the identity information with any specific registry or application.

Countries, regardless of their maturity with respect to digital identity, will benefit from standardized integration service offerings in multiple ways, including:

1. **Lower Total Cost of Ownership:** ID4D Integrated services allow stakeholders to access information directly, without, manual processing of requests

2. **Fraud Reduction:** Services offered through the ID4D Integration layer are authenticated and audited reducing both internal fraud (e.g., leakage) and external fraud (e.g., identity spoofing)

3. **Security:** The ID4D Integration framework support secure data interchange and, when PKI is incorporated, allows for additional measures such as non-repudiation and certificate revocation

4. **Facilitation:** Stakeholders, including the public, can easily and securely access ID4D Integrated services

5. **Interoperability:** Domestic stakeholders along with regional and international partners can more efficiently exchange information through ID4D Integration; this includes both civil and criminal information

Finally, it is envisioned that through the use of distributed, secure, identification services, global initiatives such as ID4D can help achieve the Sustainable Development Goal of “providing legal identity for all, including birth registration, by 2030.”
ANNEXES
The ability to uniquely identify people is an essential part of establishing a trusted (secure) foundation for both public and private interchanges. Unique identification begins with interactions where identity claims are made, often biographic in nature, and is enhanced through the use of biometric identifiers, typically when applying for an identity credential. Each identity event helps to build a stronger view of the identity over time, where the ‘true’ identity emerges as depicted in Figure 11 below.

Multi-factor authentication is a means to establish one’s identity; in the security context, the term three-factor authentication is synonymous with strong authentication where the three factors are something you have (e.g., ID card), something you know (e.g., PIN), and something you are (e.g., biometric identifier). Two other dimensions add to the strength of the authentication: what you do (e.g., how you move your mouse) and where you do it (e.g., geo location) as described in Figure 12 which follows.
Biometric identifiers are the root of a unique identity, which is a key enabler in the digital identification process; as such, the quality of the biometric samples enrolled is fundamental to the effective operations of a Unique Identity System. The quality of biometric samples used to authenticate an identity claim are important as well although slightly less critical because only a one-to-one comparison is required versus a one-to-many (where many may be in the 10s of millions).
Annex 2: ID4D Integration Model

INTRODUCTION

The ID4D Integration Model is shown in Figure 13. Vital events (e.g., birth, death, marriage, divorce, adoption) and the institutional stakeholders responsible for registration of these events (e.g., social protection institutions, courts, electoral commissions) are captured at the top of the diagram. These functional components are envisioned to be integrated with the backend technical components (i.e. foundational registries, vital statistics, and credential issuance).

HIGHLY INTEGRATED IDENTIFICATION REFERENCE MODEL

The Highly Integrated Identification Reference Model serves as a target for countries as they move to the next phase of integration of their existing registries into a holistic framework that is supported by the foundational registries. It logically groups external stakeholder organizations separately from country-specific identity technologies that will serve as the backbone infrastructure to deliver the functional services to the end users (e.g. residents).

Key components of the Highly Integrated Identification Reference Model are defined in Table 10, along with further context within each component.

The Highly Integrated Identification Reference Model can be used to develop a country specific integration roadmap showing how to link existing components in a scalable, methodical way. Further discussion on the ID4D integration layer, both architecture and key features, is provided herein. The strategy and roadmap for integration are covered in the next section of this report, Strategy and Roadmap for Implementation.
The Unique ID system and Civil Registry are integrated through the ID4D Integration layer. This architecture preserves the modular nature of the model versus customized direct interactions.
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Context</th>
</tr>
</thead>
</table>
| Functional Registries         | Systems developed in response to a specific application (e.g., elections, tax, social protection, pension, etc.) | • Functional Registries are integrated with Foundational Registries through secure, standards-based services  
• Services are provided and responses will be viewable based on role / attribute  
• Through service calls, Functional Registries provide the minimal data required to complete the operation based on the corresponding data model  
• Stakeholders can 'subscribe' to an identity in order to receive notifications for any identity update |
| Law Enforcement Integration   | Integration with local, national, regional, and international policing agencies to strengthen national security | • Authorized users can request Watch List status (Hit / no Hit)  
• Law Enforcement records may be linked via Unique ID and tagged in National ID as derogatory information  
• Law Enforcement data will not reside in Foundation Registries; rather, identities may be tagged in order to indicate that derogatory information is on file and by whom |
| Other Country Integration     | Integration with neighboring countries to form a regional identity system that can address matters of policing, national security, and servicing migrant populations | • Authorized representatives from other countries may provide birth/death Acknowledgement* information related to citizenry  
• Host country may provide birth/death Acknowledgement  
*Note that Acknowledgements are shared so that births/deaths are not double counted; that is, attributed to one country and reconciled in more than one. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Context</th>
</tr>
</thead>
</table>
| Residents and Private Institutions       | Providing residents and selective access to registries. Residents may include both citizen and non-citizen populations. Non-citizens, such as refugees, may seek (and be eligible for) benefits in the country of residence.                                                                                                                                                                                                                                                                                                                                                     | • Residents may access services through a Citizen Portal to initiate applications, vote, pay taxes, etc.  
• Residents may also be able to initiate Demographic Update, Redress, and Authentication Requests through the ‘citizen portal’  
• Residents and can use eIDs to secure gov and non-gov interactions                                                                                                                                                                                                                                                                                                                                                         |
| ID4D Integration                         | A top-level Integration Layer, with standardized services that orchestrate all transactions processed in the foundational identity management system(s)                                                                                                                                                                                                                                                                                                                                                     | • Integration is achieved through secure, standards-based services, data models, and governance  
• Services and Responses will be Role-Based and potentially Attribute-Based (e.g., supervisor versus non-supervisor)  
• Data required to complete the service request will be minimal and tailored per the data model for the operation  
• Authorized stakeholders can subscribe to identities; corresponding updates will be published to all authorized subscribers                                                                                                                                                                                                                                                                                                                                                                          |
## Table 10: Key Components of the Highly Integrated ID4D Identification Model

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Context</th>
</tr>
</thead>
</table>
| **National Identity** | Universal, multi-purpose system capable of supporting identity services for multiple stakeholders (National, Regional, or International) | • National ID system provides foundational identity services as follows:  
  • Unique ID (derived from biometric de-duplication) will be used as the primary key to link identities in disparate databases  
  • Demographic information remains in stakeholder systems; not copied to National ID system beyond the ID4D schema  
  • Enrollment quality will be assessed to identify quality trends / issues  
  • Retention policies enforced through rules-driven 'Deletes'  
  • Privacy enhanced through separation / anonymization of biometric information |
| **Civil Registration** | A legal registry of all birth and death events that occur in the country as well as foreign missions | • Civil Registration system provides foundational identity services as follows:  
  • Core demographic repository  
  • Identities linked through the Unique ID |

**UNIQUE IDENTITY SYSTEM**
- Enrollment
- Identification (de-duplication)
- Authentication (verification)
- Update / Delete

**CIVIL REGISTRY**
- Birth Registry
- Death Registry
- Population Registry

---

**BIOMETRIC IMAGES**
- Vital Statistics
  - Compilation
  - Processing
  - Validation
  - Dissemination

**RESIDENTS**
- Authentication
- Applications
- Updates, Redress

**PRIVATE INSTITUTIONS**
- Telcos
- Financial Services
- Insurance Providers

**HEALTH SERVICE INSTITUTIONS**
- Live Birth
- Health

**CERTIFIER OF CAUSE OF DEATH**
- Death
- Fetal Death

**SOCIAL PROTECTION INSTITUTIONS**
- Aid Agencies
- Food subsidies
- Non-citizen services

**COURTS / JUDICIAL INSTITUTIONS**
- Marriage, Divorce
- Annulment, Judicial Sep.
- Adoption
- Legitimation, Recognition

**ELECTORAL COMMISSION**
- Elections

**OTHER COUNTRIES**
- Birth Abroad Ack
- Death Abroad Ack

**LAW ENFORCEMENT / BORDER MANAGEMENT**
- Derogatory Information
- Wanted / Warrants

**FUNCTIONAL REGISTRIES**
- Civil Registry
  - Birth Registry
  - Death Registry
  - Population Registry

**CREDENTIAL ISSUANCE**
- eID
- Voter ID
- ePassport
- Multi-function

**STATS DB**
- Birth Records
- Death Records
- Population Records

**UID DB**
- Unique ID Repository
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Context</th>
</tr>
</thead>
</table>
| Vital Statistics           | Data mart of vital events (e.g., birth, death, marriage, divorce, adoption) gathered from various functional registries | • Civil registry will provide notifications for each vital event through a subscription service  
• Dissemination through reporting services |
| Credential Issuance        | Creation of a credential (e.g., national ID card, voter ID, ePassport) that is used by an individual to assert their identity | • Credential personalization requests will be initiated after the application process is completed and the applicant is fully vetted  
• Credential activation through biometric verification, where required, and confirmation of receipt will complete the process  
• Cryptographic keys will be used in electronic identification documents to digitally sign correspondence, to encrypt correspondence, and other operations as required |
This chapter is work in progress and is being provided to the public for information purposes only, in order to facilitate the debate on the latest trends and issues in the area of identification systems and ID4D programs.

Because it is a work in progress, there could be some inaccuracies in the data presented in this section and there could be some parts that are either missing or will be revised. Permission to cite any part of this work must be obtained from the authors.

Information for each country case study was gathered using publicly available records, and any qualifications or key challenges described in the assessments are based on the target Integration model, as laid out in the main ID4D Integration Approach report.

Reference to names of firms and commercial products and processes does not imply their endorsement by the World Bank Group.
This Compendium contains 15 case studies, conducted as part of the ID4D Integration Approach study, with the objective to uncover, understand and benchmark the different trends observed in different countries around the world. As an addendum to the main report, this Compendium is comprised of 12 benchmarked countries’ profiles and 3 in-depth analyses.

All the countries were placed into each of the country categories – “Advanced”, “Intermediate”, or “Greenfield” – because they provide good examples for the level of national identification maturity within each category. The below table provides a high level overview of the attributes of each category:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description of Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1:</td>
<td>An “advanced” country is defined as a nation that has the majority of the features that encompass a highly integrated state, but may be lacking maturity in a few of them. They will have strong foundational registries and an integrated framework, and generally have specific improvement plans to address their weaker points.</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>Category 2:</td>
<td>An “intermediate” country is defined as one that has taken measurable steps to develop a digital ID system, but still has some significant improvements to make in order to ensure that the system is scalable and can be integrated with existing disparate registries. It will either have a foundational database (registry) in place, or have efforts in progress to strengthen and/or digitize one. It typically will require improvements in its networking infrastructure and community outreach strategy in order to ensure that access to a national ID is possible for the majority of its population.</td>
</tr>
<tr>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Category 3:</td>
<td>A “greenfield” country is defined as country which has rudimentary or no registry integration either directly, through custom interchanges, or through an SOA. These countries have the most room for improvement and typically have a “blank slate” to start a digital ID program.</td>
</tr>
<tr>
<td>Greenfield</td>
<td></td>
</tr>
</tbody>
</table>

The Benchmarked Countries were analyzed in less depth than the Studied Countries. The focus of the analysis was on their current state registration landscape and key challenges. Like the Studied Countries, only the country’s main registry systems and their corresponding registration processes were analyzed.

The twelve Benchmarked Countries covered in the assessment are organized by category and ordered as follows:
### Advanced
1. Estonia
2. Portugal
3. Belgium
4. Pakistan

### Intermediate
5. Kenya
6. Mexico
7. Nigeria

### Greenfield
8. Sierra Leone
9. Liberia
10. Djibouti
11. Laos

### Distinct Scenario – Not Categorized
12. India

The three “Studied Countries” of interest in this particular assessment are the following:

13. Guinea - **Greenfield**
14. Rwanda - **Intermediate**
15. Botswana - **Advanced**

The following standard parameters were addressed for each country:

1. Maturity Assessment: Greenfield / Intermediate / Advanced
2. Registry Assessment
3. Legal Framework
4. Institutional Structures
5. Identification Processes
6. Current Challenges

In-depth research was conducted to fully understand each studied country’s current state identification landscape – including main registry systems, legal protections, governing bodies, and registration processes. Only the country’s main registry systems and their corresponding registration processes were analyzed because these are the most critical for the citizen’s identity architecture. Furthermore, this exercise with the studied countries has served to validate the **Highly Integrated Identification Reference Model** for each country category by covering the key concepts with the country delegations. In addition, in the three studied countries – Guinea, Rwanda and Botswana – the existing challenges with the current system were defined and an action plan suggested in order for the country to reach its next level of integration. However, the recommendations and subsequent action plans are specific to each country and encapsulate technology, process, and institutions in one integrated plan.
STUDIED COUNTRY PROFILES
GUINEA

MATURITY ASSESSMENT

Categorization: Greenfield

REGISTRY ASSESSMENT

Guinea has three basic registries currently in place: Birth Registry, Election Registry, and e-Passports. The registries are not integrated with each other or highly used by Guinea’s population. Of the three, the Election Registry has the highest usage and includes biometric and biographic data, making it the most “complete” registration system in Guinea.

Guinea developed a strategy for building a foundational national identification system in 2011 by leveraging its Election Register. This Election Register underwent one major overhaul after Guinea switched solution vendors and contracted Waymark to update its original register to include more comprehensive biometrics (10 fingerprints instead of the original 4 from the first iteration of the register). Although Guinea intended for the electoral data to become integrated with the national ID register, its plans were put on hold after the Election Register became mired in political controversy (it was disputed that the pockets of people enrolled were biased toward one political party). As of 2015, Guinea has again switched contractors (using an open bidding process to select Gemalto) and intends to have this company update the Election Register once again in time for the 2015 elections.
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth Registry</td>
<td>Foundational</td>
<td>58% of population [6,185,000]</td>
<td>Birth details, Parent information</td>
<td>Paper-based certificates</td>
<td>Difficult to integrate with other registries because it is not digitized and a relatively low % of the population is registered</td>
</tr>
<tr>
<td>Election Register</td>
<td>Functional</td>
<td>83% of eligible population [~5,000,000 out of 6,000,000 adults 18+]</td>
<td>Biographic and biometric data (either 4 or 10 fingerprints and high quality picture)</td>
<td>Cardboard voter cards</td>
<td>Most comprehensive registration system. Currently being updated and intended to eventually integrate into the National Identity Register</td>
</tr>
<tr>
<td>Electronic Passports</td>
<td>Functional</td>
<td>0.4% of population [50,000]</td>
<td>Biographic data, some biometrics</td>
<td>e-Passport</td>
<td>Not well integrated. E-passports were Introduced very recently and have very low usage</td>
</tr>
<tr>
<td>National Identity Register</td>
<td>Foundational</td>
<td>N/A</td>
<td>Biographic and biometric data (10 fingerprints and high quality picture)</td>
<td>National ID Card (2D barcode)</td>
<td>Election Registry data is being used to build the National Identity Register</td>
</tr>
</tbody>
</table>

**LEGAL FRAMEWORK**

Guinea lacks any data protection laws and has no independent data protection authority. Each state ministry is responsible for regulating its own data privacy. Its government authorities have access to personal data, but there are no laws governing this access. While it does have a civil code requiring birth and death registration, participation remains low.18

---

18 (Privacy International, 2014)
INSTITUTIONAL STRUCTURES

The Election Register is owned by the Independent National Electoral Commission (CENI), which is a separate organization set up in 2012 to manage the national elections.

The Ministry of Communication & New Information Technologies is responsible for implementing/improving ICT solutions across all of the government sectors. It, however, does not have ownership of any particular registry. As such, it does not have the appropriate influence or authority to mandate digitization of any ministry’s registries – including the civil registry.

Guinea’s civil registry system is centrally owned by the Direction National de l’Etat Civil (DNEC), an arm of the Ministry of Territorial Administration & Decentralization, but is in reality managed by local governments. This results in little to no uniformity in the way that each district’s civil registrars are maintained. The DNEC is responsible for the technical and administrative aspects of the CR system, but is severely underfunded and understaffed.19

IDENTIFICATION PROCESSES

Birth Registration

Birth registration is done in person at any of Guinea’s 348 local offices. Upon registration, a paper birth certificate is issued. The birth record is kept at the local precinct (on paper) and not synchronized with information from any of the other offices.

19 (UNICEF, 2014)


**Election Register**

Persons of voting age register themselves at any of the mobile enrollment stations set up prior to an election. At registration, a voter’s fingerprints and face are captured. AFIS is then used after all of the captures are completed to de-duplicate the data.

**CURRENT CHALLENGES**

Guinea lacks an option for using an existing foundational registry for its national due to its paper-based and ineffective civil registry. Its existing institutional structure does not allow for effective data sharing between registries or a unified approach to future data integration (should the national ID system go into effect). Its starting base for a national registry, the Election Register, has been marred by political controversy and is a continuous point of contention; as a result, each election since 2008 has seen a re-do of the Register using a new contractor.

**INTEGRATION MODEL AND ROADMAP**

Guinea has an opportunity to utilize data already captured as part of its Election Register to springboard it into a viable national register. In order to facilitate a successful migration to a national ID system, Guinea should complete the following activities which are highlighted in Figure 14:

1. Establish a governing body to oversee the roll-out of the national ID system (currently, the CENI - Elections Commission is responsible for the Election Register, which is the “nest egg” from which the national system will be built). This governing body should be independent of functional ministries and be given the authority to work across ministries to accomplish its tasks.

2. Kick off the process for establishing the adequate data protection and e-transaction laws such that, at latest, legislation in place by the time a national register is established.

3. Assuming that conversion of existing paper-based birth registry data to an actual database is not feasible, consider building the foundational database of a national registry utilizing data from the Electoral Register.

4. It is not known at the moment what percentage of biometric captures in the Election Register are of high quality versus those that would need to be re-taken. For the latest iteration of the Electoral Register, consider re-capturing the data of each registrant again to ensure that it is of sufficient NIST Fingerprint Image Quality (NFIQ) and ICAO compliant quality for face photos. This will minimize error matching rates in the future.
5. Additionally, it is recommended that there be a multimodal approach to capturing biometrics from users (e.g. fingerprints, face, iris). This will be helpful in the event that a registrant is unable to provide viable biometrics of a particular type (for instance, a face and iris scan will be the sole identifiers if registrants have prints that cannot be captured).

6. From a government standpoint, establish a plan for addressing the registration of non-citizens. One recommendation would be to register the entire population (whether a citizen or not) and have undeclared people/ noncitizens receive a separate type of designation in the registry. This would allow everyone to be included in the registry, but would mean that inclusion in the registry does NOT automatically entitle a person to citizens’ benefits.

7. Ensure that the existing e-passports data is interoperable with the technology implemented for the latest Electoral Register (Sagem ID database). If not, consider migrating the data to an alternate database technology to accomplish this task (especially since e-passport participation is still low, and any technology switches would be less costly done as upfront as possible). For any future registry improvements, ensure that the chosen technology is interoperable with the databases in existence.

8. Develop a plan for enrolling and updating children, whose biometric data is subject to change as they get older. Consider capturing an iris and face scan, and modify the data capture such that the parents’ ID information is linked to the child’s. For children, consider a more frequent biometric capture given their biometric features change rapidly in those years. For example, several countries employ a passport renewal policy for adults that requires renewal every 10 years and for children it is every 5 years.

9. Use the enrollment kits originally used for election registration for the national ID registration (similar to the Aadhaar initiative in India). Guinea already has over 5000 kits, and can develop a plan to reach its entire population by:
   a. Deploying the enrollment kits to easy-access municipal locations (e.g. post offices, schools)
   b. Setting up mobile stations in hard-to-access rural areas

10. In order to incentivize the population to register, link the registration to a benefit.
The Unique ID system and Civil Registry are integrated through the ID4D integration layer. This architecture preserves the modular nature of the model versus customized direct interactions.
MATURITY ASSESSMENT

Categorization: Intermediate

REGISTRY ASSESSMENT

Rwanda has a national ID program for adults 16+, and is using the data collected for it to eventually modernize its National Population Registry. Its current civil registry system is still paper-based, and issues physical birth and death certificates to its citizens.

There is a degree of interlinkage between the functional and foundational systems, as the National ID (which captures biometric data) is used to authenticate identity across several services (e.g. social security and tax registration) and enable a national mandatory mobile SIM card registration program. National IDs also enable Rwandans to travel anywhere in Rwanda, Uganda and Kenya, per the EAC Common Market Protocol. Rwanda has plans to issue an e-Passport in the future, which will also capture some biometric data in addition to the biographic data.

Efforts are underway to further modernize civil registration and provide a digitized identification system for children under 16 years of age. These activities are a key priority as part of the second National Strategy for Development of Statistics (NSDS2).
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>National e-ID / Indangamuntu</td>
<td>Foundational</td>
<td>91.5% of eligible (adult) population [6.15 million]</td>
<td>Biographic data, Signature, Biometric data (photo, fingerprint)</td>
<td>National e-ID Card</td>
<td>Integrated data: passport, driver’s licence, family dependants, Social Security (RSSB), Health insurance, Tax ID number (TIN), SIMTEL (mobile payment processing). Enables travel across EAC without visa.</td>
</tr>
<tr>
<td>National Population Registry (civil registry)</td>
<td>Foundational</td>
<td>Estimated 79% of population registered [9.34 million] 82% of births registered</td>
<td>Births, Deaths, Residence (sector-level), Adoptions, Marriages</td>
<td>Paper-based certificates</td>
<td>N/A</td>
</tr>
<tr>
<td>Social Security (RSSB) / Health Insurance (Mutelle de Sante)</td>
<td>Functional</td>
<td>73% of eligible population</td>
<td>Name, DOB, Sex</td>
<td>Health Insurance Card (incl RSSB ID number)</td>
<td>Payment data integrated with National ID</td>
</tr>
<tr>
<td>National Electoral Commission (NEC)</td>
<td>Functional</td>
<td>As of 2013, 6.2 million (~50% of population)</td>
<td>Register based on National e-ID</td>
<td>N/A – National ID card doubles as voter card</td>
<td>Authentication based on National ID</td>
</tr>
<tr>
<td>Tax Identification Number</td>
<td>Functional</td>
<td>113,198 taxpayers</td>
<td>Register based on passport or National e-ID</td>
<td>Tax ID Number (TIN)</td>
<td>Included in National e-ID Card</td>
</tr>
<tr>
<td>Business Registry</td>
<td>Functional</td>
<td></td>
<td></td>
<td>Certificate of Registration/ Incorporation</td>
<td>Integrated with Rwanda Revenue Authority</td>
</tr>
<tr>
<td>Opportunity International</td>
<td>Functional</td>
<td>32,618 micro loans disbursed</td>
<td></td>
<td>Savings card (microfinance)</td>
<td></td>
</tr>
</tbody>
</table>
LEGAL FRAMEWORK

Rwanda has passed laws in regards to access to information and defining the legality of electronic transactions. However, it also grants exceptions when it comes to surveilling its population over matters related to national security. In 2013, Rwanda updated its 40/2008 Interception of Communications law to allow relevant security organizations to apply for interception permits. In general though, Rwanda has passed a number of laws that provide basic data protection and privacy to its users.20

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law No. 03/2013: Access to Information</td>
<td>2013</td>
<td>Prohibits the publication of information by both public and private bodies if it interferes with the privacy of an individual and is not of public interest</td>
</tr>
<tr>
<td>Law No. 18/2010: Relating to Electronic Messages, Electronic Signatures and Electronic Transactions</td>
<td>2010</td>
<td>Establishes the legality of electronic transactions, and electronic messages and protects against unauthorized access of information / access with intent to commit crimes.</td>
</tr>
<tr>
<td>No. 48/2008: Interception of Communications</td>
<td>2008</td>
<td>Prohibits the surveillance of any data or voice communications for which the user has no knowledge of or has not given permission to do so</td>
</tr>
<tr>
<td>Birth Registration Law</td>
<td>2008</td>
<td>Stipulates that all children born in the country be registered within 15-30 days after birth and issued with a birth registration certificate. Violators are subject to fines.</td>
</tr>
</tbody>
</table>

20 (Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (HIVOS), 2014)
INSTITUTIONAL STRUCTURES

Rwanda’s national ID program is overseen by a NIDA steering committee, which has representatives from all of the following offices:

- President’s Office
- Various Government Ministries
- Police (National and Traffic)
- National Institute of Statistics
- Information & Technology/Authority
- Social Security
- Central Bank

This model allows for all of the various government interests to play a role in the direction and scope of the national ID, and gives NIDA the appropriate influence in all government functions.

IDENTIFICATION PROCESSES

National ID

Citizens interested in a national ID card must register in person at a local designated office (those abroad can register at the NIDA headquarters). At the time of registration, biometric and biographic data is captured. Those who are over the age of 16 receive an ID card within one month of application. At this time, children under 16 are not issued an ID card, though they may apply for one and receive an 8-digit application number. This application number is used once the child turns of age to generate a national ID number (which is 16 digits).

Birth Certificate

To obtain birth certificate, a child’s parents must go to a physical civil registry office, present proof of ID, and submit a claim for a certificate. The birth certificate must be signed by the Executive Secretary of the sector prior to issuance. To date, these birth records are not entered into a database, but kept as a physical record only.

21 (National Identification Authority (NIDA) Rwanda, 2013)
CURRENT CHALLENGES

Rwanda has integrated its national ID system with several other functional registries at this point, but still does not have a strong foundational database (civil registry) from which to baseline its enrollment. Without strong birth or death data, it:

1. Is hard to verify birth dates even during national ID enrollment, and

2. Will become a problem in the future when users of the national ID card pass away and their data across systems has to be updated accordingly.

A second major challenge is the fact that Rwanda’s national ID system currently only covers citizens 16 and older. There is not a clear plan as of yet to enroll children, and a plan needs to be put in place to register them, even if the majority of their benefits do not apply until adulthood. There is the additional factor of deciding which biometric data to collect for these children, since fingerprints and irises develop through adulthood and, if collected up front, would need to be re-collected at a later time.

Rwanda’s next main focus should be to (1) improve and digitize its civil registry system, and (2) develop a plan to enroll children under 16.

INTEGRATION MODEL AND ROADMAP

For its next national ID iteration, Rwanda should focus on its current challenges as well as work to expand the national ID to encompass additional government functions. The list that follows, as highlighted in Figure 15, describes the suggested actions for Rwanda:

1. Expand the storage capacity and robustness of the national ID registry to include civil registry data. In this way, Rwanda can digitize its civil registry utilizing biographic and biometric data already captured as part of its national ID campaign.

2. Digitize its birth and death registries, and consider issuing a national ID number at the time of birth certificate issuance.

3. Make death registration a required component for burial (to essentially mandate registration participation), and integrate this registration with the national ID registry. It is important that Rwanda has a reliable method of archiving data for deceased participants such that services related to the archived citizen can be stopped or modified.

4. While the national ID card is used as a form of authentication for other services (e.g. voting, social security), there is no registry linkage between
the NID database and other functional databases. These systems should be integrated to allow better integration so that ID verification can take place at the time of service issuance.

5. Consider increasing the accuracy of the national ID system by expanding the capture of fingerprints for the national ID card from 2 fingerprints to 10. Ensure that these fingerprints are of sufficient NIST Fingerprint Image Quality (NFIQ).

6. There is currently a stop-gap method for providing children under 16 with IDs (using Application # as a temporary ID until the child reaches 16). There is no biometric data captured for these children. Rwanda should consider developing a program to enroll all children (e.g. via schools), capture at minimum a face image, and to map these national ID accounts to those of their parents. The national ID database will likely need to be modified to allow capture of these additional fields.
The Unique ID system and Civil Registry are integrated through the ID4D Integration layer. This architecture preserves the modular nature of the model versus customized direct interactions.
**Maturity Assessment**

**Categorization:** Advanced

**Registry Assessment**

Botswana has a national ID system (the Omang) that is completely integrated with its digitized birth and death registry system (BDRS). The BDRS and national registration share one registrar. A unique ID number is issued at birth and is used across various government registries. Data transfer is automated and changes made at the regional office level are transferred to a central office in real time. Botswana is noted for having an integrated system that is able to update every registry upon issuance of a person’s death certificate, so that services across sectors can be stopped for the deceased individual.\(^{22}\)

Citizens use the Omang card as identification to access the following public services, entitlements, and benefits: social assistance, social insurance, driver’s license, voting, education, health, and passport issuance. Although biometrics (2 thumb prints are captured during registration), the current Omang card is not a Smart Card. However, the national ID number is mapped within each of the functional databases for verification and transaction history. Botswana intends to migrate to the issuance of Smart Cards starting in 2016.

Botswana also collects biometric information as part of its e-passport registration. In that process, all 10 fingerprints are collected using AFIS technologies.

<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth and Death Registry (BDRS)</td>
<td>Foundational</td>
<td>72% Births [1,552,000] 53%-75% Deaths [1,143,000-1,617,000]</td>
<td>Biographic data, birth and death details</td>
<td>Paper and electronic certificates/records</td>
<td>CRVS linked with national ID. Central data repository connected to outstations with changes and updates occurring real time.</td>
</tr>
</tbody>
</table>

\(^{22}\) (Lepang, Universal Birth and Death Registration for Secure Identity System: Understanding the Business, 2014)
Legal Framework

Botswana’s Omang system derives its mandate from a number of laws. The National Registration Act (1986) requires that all Motswana on or over the age of 16 must apply for a national ID. The Births and Deaths Registration Act (1969) requires that all births and deaths be registered within 60 and 30 days, respectively. Failure to register in time results in a fine.

Despite a fairly robust national ID system, Botswana does not have a comprehensive data protection law in place. It has had freedom of information, data protection, and electronic transaction bills drafted in recent years, but none have passed to date. Botswana hopes to pass these bills as part of its next steps in furthering its national ID system.

Legal Framework

Botswana’s Omang system derives its mandate from a number of laws. The National Registration Act (1986) requires that all Motswana on or over the age of 16 must apply for a national ID. The Births and Deaths Registration Act (1969) requires that all births and deaths be registered within 60 and 30 days, respectively. Failure to register in time results in a fine.

Despite a fairly robust national ID system, Botswana does not have a comprehensive data protection law in place. It has had freedom of information, data protection, and electronic transaction bills drafted in recent years, but none have passed to date. Botswana hopes to pass these bills as part of its next steps in furthering its national ID system.

(23 Lepang, Interview with Botswana’s Director of Civil Registration, 2015)
INSTITUTIONAL STRUCTURES

Botswana’s Omang program is managed by the Ministry of Labour & Home Affairs, which is responsible for the segments of government provided in Figure 16 which follows:

Figure 16: Botswana’s Ministry of Labour and Home Affairs Jurisdictions

It is not a governing agency that sits above the other ministries, but the Ministry is responsible for civil registration, citizenship, and migration, making it easier for civil registration and the Omang system to integrate with each other.

REGISTRATION PROCESSES

National ID - Omang

All persons born in Botswana are issued a birth registration and an Omang number. Citizens are issued a 9-digit number, and non-citizens are issued a 7-digit one. This ID stays with the person throughout life. Adults who are 16 and older are required by law to apply to receive a physical Omang card, which is a Smart Card that contains biographic and biometric (2 thumb prints) data of the holder. This card is then used for identity and verification purposes across multiple government services.

Birth Certificate

Birth certificates are generated digitally. Registration is easier if the birth is done in a hospital, as the doctor/midwife can automatically file for one. In remote areas in which births are done at home, the government has rolled out a “remote area
development program” in which it partners with district commissioners in rural communities to have parents register their children.

**CURRENT CHALLENGES**

Although Botswana’s Omang card has been established for over 10 years and is a fairly mature program, it still faces a number of challenges:

1. Botswana does not have any passed data privacy, e-transaction, or right to information laws, despite having an immense database of citizens’ information.

2. It is still not considered a complete registry – many residents delay registration, which undermines the data integrity of the system and reduces citizens’ access to public services.

3. There are still many unreported historical deaths, meaning that the government is unable to close the loop on a number of Omang IDs.

4. There have been issues with counterfeit documents, and in recent years an investigation unit has been established to combat these issues.

**INTEGRATION MODEL AND ROADMAP**

In order to address the issues listed above and to continue to improve the services that the Omang card can provide, Botswana should consider completing the actions which follow as depicted in **Figure 17:**

1. Prioritize the passage of the bills that remain open regarding data protection, e-transaction, and right to information. This will be especially important if Botswana intends to expand its national ID program to link to private corporate systems (e.g. banking).

2. There is still approximately 28% of the population that is still not in its BDRS, which includes people in both urban and rural areas. The government should set up an outreach program in the cities (public campaign) and consider customizing a plan to reach non-citizens (e.g. migrants) through incentivized programs.

3. In order to counter fraud and counterfeit IDs, Botswana should consider mandating that all Omang card registrants provide 10 fingerprints instead

---

24 (UNICEF, 2014)
of the original 2. This will not only make de-duplication easier, but reduce drastically reduce any error matching rates. The Ministry of Labour & Home Affairs should also take caution to ensure that the fingerprints captured are of sufficient NIST Fingerprint Image Quality (NFIQ). It should be noted that e-Passport holders already have to provide 10 fingerprints, so it is possible to leverage some of this passport data for the overall national registry.

4. Botswana likely has already considered the idea of expanding its Omang ID system to be integrated with key private institutions, like banks. It should develop a business plan to determine the cost of operating a central repository to support this, and consider having this development partially funded by collecting nominal transaction fees from subscribers. This would provide a sustainable income from which the government could use to maintain its growing databases.

5. In order to improve the cross-border sharing of information, Botswana should set up bilateral agreements with its bordering countries to define an interoperable framework for purposes such as outside-of-country births/deaths, and persons of interest / watch lists.
The Unique ID system and Civil Registry are integrated through the ID4D Integration layer. This architecture preserves the modular nature of the model versus customized direct interactions.
BENCHMARKED COUNTRY PROFILES
MATURITY ASSESSMENT

Categorization: Advanced

REGISTRY ASSESSMENT

Estonia has established a comprehensive identification system, with two foundational systems as its backbone: the National Population Register and the National ID system. It has linked these foundational registry systems with a variety of economic, social and political applications via the ‘X-Road’ middleware (architecture shown in Figure 18). A variety of other state systems depend on the data contained in the National Population Register for their services. For example, when applications are received for childbirth allowances, study allowances or concession public transport tickets, the relevant data is extracted from the National Population Register without the need to complete additional documentation. Meanwhile, the National e-ID Card is the primary form of identification used to authenticate to services from voting and tax to even online banking and shopping. The card contains a PIN, digital signature and encryption features to enable secure authentication.

The uptake of the foundational systems is exemplary (100% coverage of birth and death registration) and the considerable level of integration with other public and private e-services makes Estonia’s identification system one that other countries aspire to.
<table>
<thead>
<tr>
<th>Registry/ID Type</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captureda</th>
<th>Outputb</th>
<th>Level of Integrationc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System (National Population Register)</td>
<td>Foundational</td>
<td>100% Births(d) [13,531](e) 100% Deaths [15,244](f)</td>
<td>Names, birth/ death details, places of residence, nationality, native language, education, profession. All 10 fingerprints for non-citizens.</td>
<td>ID code (electronic)</td>
<td>Connected to numerous other systems via the X-Road – allows data to be retrieved automatically from the Register without need for additional forms (e.g. voting verification, applications for allowances and benefits(g)). Citizens can notify of changes to their data by sending a digitally signed document.</td>
</tr>
<tr>
<td>National ID System</td>
<td>Foundational</td>
<td>83% of population (h) [1.1million](b) National e-ID cards are for individuals above 15 years of age</td>
<td>Data stored on the card: ID code, legally binding digital signature, personal data file, certificate for authentication, private PIN-protected key, permanent email address for communications with public sector</td>
<td>National e-ID card (physical)</td>
<td>Linked to Population Register using ID code as reference. Primary document which facilitates secure authentication and provides a legally binding digital signature for public and private online services.</td>
</tr>
<tr>
<td>Mobile-ID</td>
<td>Functional</td>
<td>SIM Card stores digital signature</td>
<td>SIM Card</td>
<td>SIM Card</td>
<td>Alternative form of authentication in addition to National e-ID Card, accepted by government e-services</td>
</tr>
<tr>
<td>ePassport</td>
<td>Functional</td>
<td>Biographic data, ID code, photograph, fingerprints, citizenship, signature</td>
<td>Biometric passport (physical)</td>
<td>Data on border crossings is maintained electronically in the Database on Border Crossings (Police and Border Guard).</td>
<td></td>
</tr>
<tr>
<td>Registry/ID</td>
<td>Type</td>
<td>Usage</td>
<td>Data Captured(^a)</td>
<td>Output(^b)</td>
<td>Level of Integration(^c)</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voting</td>
<td>Functional</td>
<td>88% of voting age population [899,793]</td>
<td>N/A – National Population Register acts as voting register, e-ID used for verification. Voter card contains instructional information only (^i).</td>
<td>Voter Card (paper or electronic by request)</td>
<td>National e-ID card can be used at polling stations with a card reader to verify voter identity. Voter eligibility is checked against the National Population Register, vote is cast and is digitally signed via the e-ID card. The signature is removed at vote count to ensure anonymity (^k).</td>
</tr>
</tbody>
</table>

\(^a\) (ePractice EU, 2015), \(^b\) (ePractice EU, 2015) \(^c\) (ePractice EU, 2015) \(^d\) (UNICEF, 2013) \(^e\) (UN Statistics Division, 2013) \(^f\) (UN Statistics Division, 2013) \(^g\) (e-Estonia, 2015) \(^h\) (e-Estonia, 2012) \(^i\) (IDEA, 2015) \(^j\) (National Electoral Commission of Estonia, 2015) \(^k\) (e-Estonia, 2015)

**LEGAL FRAMEWORK**

Estonia has a number of instruments in place that provide for the creation and maintenance of a national population register, the security and protection of the personal data contained therein, and the process to request and receive access to information stored in government databases. Furthermore, its current legal framework also facilitates the high level of interoperability between various government services that is a strong point of the Estonian identification system; for example, through rendering digital signatures legally binding, establishing central ICT governance, and providing for the maintenance of common infrastructure such as middleware, networks and document exchange.
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Information Act</td>
<td>2000</td>
<td>The Act covers State and Local Agencies, legal persons in public law and private entities that are conducting public duties (e.g. educational, health care, social or other public services). Any person may make a request for information and the holder of information must respond within five working days. The entities are also required to ensure that the information is not &quot;outdated, inaccurate or misleading.&quot; In addition, email requests must be treated as official requests for information. The Act is enforced by the Data Protection Inspectorate.</td>
</tr>
<tr>
<td>Personal Data Protection Act</td>
<td>1996</td>
<td>Protects the fundamental rights and freedoms of persons with respect to the processing of their personal data (including biometric data). Requires processed personal data to be protected by documented organizational and technical measures. Chief processors (i.e. controllers) must register the processing of sensitive personal data with the Data Protection Inspectorate. The Act also allows individuals to obtain and correct records containing their personal data.</td>
</tr>
<tr>
<td>Population Register Act</td>
<td>2000</td>
<td>The Act provides for the composition of data in the population register, the procedure for its introduction and maintenance, processing of data and access, entry of data on residence and exercise of supervision over the maintenance of the register.</td>
</tr>
<tr>
<td>Electronic Communications Act</td>
<td>2004</td>
<td>The Act creates the necessary conditions to promote the development of electronic communications networks and communications services while ensuring the protection of the interests of users of such services</td>
</tr>
<tr>
<td>Digital Signature Act</td>
<td>2000</td>
<td>Grants similar legal value to digital and handwritten signatures while setting an obligation for all public institutions to accept digitally signed documents</td>
</tr>
<tr>
<td>System of Security Measures for Information Systems</td>
<td>2008</td>
<td>The Act describes the organizational, physical and IT security measures required to protect data contained in state and local government databases and for related information assets</td>
</tr>
</tbody>
</table>

a  (ePractice EU, 2015)  
b  (Population Register Act, 2000)
INSTITUTIONAL STRUCTURES

The Ministry of the Interior administers and develops the National Population Register, as well as National ID Card and ePassport programs. ePassports are administered by the Police and Border Guard within the Ministry.

The Ministry of Economic Affairs and Communications is responsible for the coordination of State ICT systems, as well as ICT strategic planning, setting priorities and ensuring financing for these, creating cooperation networks while ensuring their functionality, drafting IT legislation, as well as elaborating IT standards. It is also responsible for the development and operation of the shared components of Estonia’s national eGovernment infrastructure (i.e. the e-services portal, the middleware system X-Road, the network EEBone, the administration system RIHA and the electronic document exchange centre).

The Data Protection Inspectorate (DPI) is an independent Agency placed under the authority of the Ministry of Justice ((it was formerly placed under the authority of the Ministry of the Interior). The DPI supervises the legality of the processing of personal data, and enforces the Personal Data Protection Act and Public Information Act.

IDENTIFICATION PROCESSES

Birth Registration

The child’s birth is registered on the basis of application by the parent at the Vital Statistics Office within the first month of the child’s life, does not involve any state fees. The official prepares an entry in the birth register and issues, if desired, a birth certificate. To register a birth abroad in the Population Register, documents that have been translated and certified must be submitted to the Vital Statistics Office. The State and Local Government Offices pull the data from the Population Registry, and so it is not necessary to present the birth certificate to any other office.

The following documents are submitted to register a birth:

- application for registering childbirth;
- medical agency’s certificate regarding the childbirth;
- identity documents certifying the identity of parents;
- marriage document if it has not been entered into a register (if the birth is registered by one of the parents, it must be accompanied by an application by the other parent regarding the desired name of the child);
- application for accepting paternity submitted in person or in notarized form.
**National Population Register**

Updates can be made to a citizen’s National Population Register record in any of the following ways:

- via a Population Register employee at the local government unit
- by using the Population Register e-services in the state portal (ID card required)
- by post
- via e-mail in digitally signed form (ID-card required)

**National ID Card / ePassport**

The service points of the Police and Border Guard Board (within the Ministry of the Interior) deal with applications for and issuing of identity documents for the first time. Submission of the application, paying the state fee and photo/biometric data collection all occurs on the spot. Conversely, replacement or renewals of identification documents can be initiated via email with digital signature, or via post.

When applying for an identity document for the first time, the following must be submitted:

- application in the required form;
- identity document;
- documents that substantiate that the applicant holds Estonian citizenship (where applicable) and copies of these documents;
- 1 colour photo;
- document certifying that the state fee has been paid, or data regarding payment of state fees

---

25 (Estonia, 2015)
26 (Police and Border Guard Board, 2015)
Fees for ID cards and ePassports are shown below:

<table>
<thead>
<tr>
<th>Applying for the ID-card</th>
<th>In Estonia</th>
<th>In foreign representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persons under 15 years of age; Persons with moderate, severe or profound disability; a person who has attained Estonian general pensionable age</td>
<td>7 €</td>
<td>10 €</td>
</tr>
<tr>
<td>Starting from age of 15</td>
<td>25 €</td>
<td>50 €</td>
</tr>
<tr>
<td>ID-card in expedited order</td>
<td>45 €</td>
<td>Cannot be applied</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applying both for the ID-card and passport together</th>
<th>In Estonia</th>
<th>In foreign representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persons under 15 years of age; Persons with moderate, severe or profound disability; a person who has attained Estonian general pensionable age</td>
<td>25 €</td>
<td>25 €</td>
</tr>
<tr>
<td>Starting from age of 15</td>
<td>50 €</td>
<td>80 €</td>
</tr>
</tbody>
</table>

All residents over 15 years of age have ID cards, which are used extensively across services such as health care, online banking, shopping, signing contracts, as tram tickets, to vote, and more.²⁷

**CURRENT CHALLENGES**

Estonia’s existing implementation meets a wide variety of its needs, but there are a few technological considerations that should be mentioned:

- The registry provides general organizational access, but does not allow for role-based access control (this was not part of the original architecture)
- It does not allow for a subscription / notification capability to its stakeholders
- Built on a standard protocol, but all of the data models are customized to each stakeholder’s requirements.

²⁷ (The Economist, 2014)
PORTUGAL

MATURITY ASSESSMENT

Categorization: Advanced

REGISTRY ASSESSMENT

Portugal’s identification system centers around a national ID called a Citizen Card, which combines and replaces five different ID cards into one secure smart card solution. The card combines five different forms of identification including civil identification, taxation, voting, social security and healthcare cards. The goal behind consolidating multiple functional registries into one card was to simplify the way that Portuguese citizens interact with the government, and to embrace the new digital age by moving to electronic transactions and advanced biometric authentication.

The Citizen Card is extremely integrated with other registries and utilized by 99.7% of Portugal’s population\(^2^8\). The back of the card contains numbers for the five forms of identification it replaces. Additionally, the card has a chip with facial and digital biometric\(^2^9\) that enables citizens to use their fingerprint for identification and provide their signature electronically.

<table>
<thead>
<tr>
<th>Registry/ID Type</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>Foundational</td>
<td>100% Births [10,459,806](^a)</td>
<td>Biographic data, birth and death details(^b)</td>
<td>Paper certificate, electronic record</td>
<td>CRVS directly linked with national ID.</td>
</tr>
</tbody>
</table>

\(^2^8\) (UNICEF, 2014)
\(^2^9\) (Gemalto)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>National ID (Citizen Card)</td>
<td>Foundational</td>
<td>99.7% of population [10,427,000]</td>
<td>Biographic data, ID numbers that the card replaces (civil ID, voting, social insurance, tax payment, and health card), chip with facial and digital biometrics (face photo and fingerprints), electronic signature</td>
<td>National ID Card (Smart Card with a chip)</td>
<td>The Citizen Card replaces five other forms of identification. It is highly utilized and integrated in public services.</td>
</tr>
<tr>
<td>Electronic Passport</td>
<td>Functional</td>
<td>19% [2,000,000]</td>
<td>Biographic data, Biometrics (face photo and fingerprints)</td>
<td>Passport number, e-Passport</td>
<td>Directly linked with Citizen Card. E-ID can be used to travel to EU.</td>
</tr>
<tr>
<td>Voting</td>
<td>Functional</td>
<td>98% of voting population [9,624,354]</td>
<td>Biographic data</td>
<td>Voter ID number, Voter ID Card</td>
<td>Directly linked with Citizen Card – ID number printed on card</td>
</tr>
</tbody>
</table>

**LEGAL FRAMEWORK**

Portugal’s constitution includes a strict provision for data protection and privacy. This becomes a legal barrier when new programs are introduced to change or update the system. Additionally, Portugal is part of the EU and has to abide by any relevant EU regulations.

In general, data protection and privacy is well integrated into Portugal’s legal code, and privacy laws are enforced.

---

*a* (UNICEF, 2014)  
*b* (www.irn.mj.pt/sections/cidadaos)  
*c* (UNICEF, 2014)  
*d* (Gemalto)  
*e* (http://www.pep.pt/)  
*f* (http://www.idea.int/vt/countryview.cfm?id=34)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Information</td>
<td>1993</td>
<td>Article 268 of the 1989 Constitution. Establishes full constitutional recognition of a public right of access to information(^a)</td>
</tr>
<tr>
<td>Data Protection Act</td>
<td>1995</td>
<td>The National Data Protection Commission passed Portugal’s data privacy and protection act, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.(^b)</td>
</tr>
<tr>
<td>Use of computerized data</td>
<td>1993</td>
<td>Article 35 of the Constitution. Establishes citizens’ rights in accessing the personal computerized data kept by the Portuguese government. Only citizens have a right to their own data, and they must be informed of the use for which the data is intended.(^c)</td>
</tr>
<tr>
<td>Regulation of Access to Administrative Documents</td>
<td>2012</td>
<td>Everyone shall have the right of access to information by way of access to non-nominate administrative documents. The right of access to documents includes the right to obtain reproductions of documents, the right to consult documents free of charge and the right to be informed of the existence and the contents thereof</td>
</tr>
</tbody>
</table>

\(^a\) (Global Right to Information Rating)  
\(^b\) (CNPD)  
\(^c\) (CNPD)

**INSTITUTIONAL STRUCTURES**

The main agency in charge of implementing and managing the Citizen Card is the **Agency for Public Reform**. However, implementation of the card required communication between all Ministries whose cards were replaced – the Ministries Finance, Health, Social Security, Internal Administration and Justice.\(^30\)

On an ongoing legal basis, the **Comissão Nacional de Protecção de Dados (CNPD)** is the governing body responsible with supervising and monitoring compliance with the laws and regulations in the area of personal data protection, with “strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law” The CNPD is responsible for the Data Protection Act and the use of computerized data clause in Portugal’s Constitution.\(^31\)

\(^30\) (Accenture, 2012)  
\(^31\) (CNPD)
IDENTIFICATION PROCESSES

Citizen card and e-ID can be used for most e-Services. The Card contains a smart chip that stores a fingerprint for national identification purposes, along with electronic signature capabilities. Citizens enter a pin code to the card, which generates a digital signature that can be used to access secure government services portals.

Portugal’s goal is to be the world leader in digital security and make e-government services customer centric. In the past 5 years, the Portuguese government has undergone many effective initiatives to make the Citizen Card more user friendly and digitally accessible. In country, the government provides “Citizen Shops” which contain many information stations whose role is to provide information at the request of users. Concurrently, public services and information is getting moved online on national eGovernment portals. For example, a national electronic one-stop shop, called The Entrepreneur’s Desk, enables businesses to access 462 government services, over 130 of which can be completed completely online. Additionally, a new integrated citizen’s portal was launched in 2006 to improve citizen e-access.

CURRENT CHALLENGES

Portugal’s civil and national registration systems are fairly well integrated. An area where Portugal could progress is by executing on the next level of the Secure identity across borders linked (STORK) program for inter-European ID authentication. STORK is currently in pilot phase, but moving the pilot to implementation would be advantageous for offering the next generation of electronic services.

Problems faced in the STORK pilot that will need to be addressing moving forward include:

- System integration with legacy systems and standardization across countries
- Need for a strong governance model and ongoing operational management
- Ensure that the proper data protection laws are in place for all countries involved

---

32 (Gemalto)
33 (Irish Presidency)
Belgium’s civil registration and identification systems are well-established and have succeeded in covering an extremely high proportion (if not all) of the population. The two main foundational registries are the National Population Register, which has close to a 100% population registration rate and has effectively replaced the need for a census, and the National e-ID Card, which is mandatory for all residents over the age of 12 and must be carried at all times. It has been suggested that one of the reasons that these foundational programs have been so successful with respect to population coverage is because pre-existing programs (such as the previous ID card and the Crossroads Bank for Social Security) had already introduced citizens to the concepts of civil registration and the use of a single identity credential to access a range of public services. A level of trust between citizens and government had already been established in this respect.

A unique identification number is issued to each Belgian citizen called the National Registration Number or RRN, which corresponds to their record in the National Registry. The RRN is integrated by default on the e-ID, as the RRN was already being used as a means of identification by different administrative services prior to the development of the new e-ID card. At present, over 600 online services are currently offered by the government that leverage the e-ID card and National Registry data. However, there are some services that remain separate and not integrated due to process or privacy concerns. For instance, the integration of drivers license into the e-ID was rejected as citizens must carry their e-ID cards at all times, which would render the police unable to confiscate drivers licenses in case of a severe driving offence. Also, the government decided against integration of the SIS social security card into the e-ID as, although technically possible, it was considered to be too significant of a risk to personal privacy and anticipated to be politically unpopular.

34 (Economie Belgium, 2013)
35 (Mariën & Audenhove, 2010)
36 (Mariën & Audenhove, 2010)
37 (Mariën & Audenhove, 2010)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
</table>
| National Register| Foundational | >99% of population [11,190,845\textsuperscript{a}]  
100% birth registration\textsuperscript{b}  
[129,300\textsuperscript{c}]  
100% death registration\textsuperscript{d}  
[109,334\textsuperscript{e}] | Biographics, civil status, employment\textsuperscript{f}, family constellation\textsuperscript{g} | Unique National Registration Number (RRN), and identity record in central electronic database | RRN linked to e-ID, used as a method of identification across a number of services.  
Voters are automatically registered if they have a record in national population register\textsuperscript{h}. |
| National e-ID Card | Foundational | >90% of population over 12 years old [>9 million cards issued]\textsuperscript{i} | Biographics, signature, photograph, national registration number (RRN)  
The design purposefully omits an address from the card to avoid the need to replace the card when individuals move. | e-ID: personal data embedded in a chip, plus two digital certificates: one for authenticating and one for signing. Digital certificates are included by default, however individuals can opt out if they choose\textsuperscript{j}.  
Kids e-ID: optional unless the child needs to travel abroad\textsuperscript{k}. The e-ID for children does not contain a digital certificate for signing since children cannot enter into legally binding contracts in Belgium\textsuperscript{l}. | Linked to RRN.  
Can be used to authenticate across numerous public and private services (e.g. tax, social security, voting, online transactions, library membership, etc.)  
Can be used to travel anywhere within the EU. |
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crossroads Bank for Social Security (CBSS)</td>
<td>Functional</td>
<td></td>
<td>Biographics, employment information, RRN$^n$</td>
<td>Electronic record in a central data repository Previously issued an SIS-card, however e-ID card now replaces the need for SIS-card as it contains the individual’s unique RRN$^n$.</td>
<td>Repository contains information about which social security institutions are relevant to each individual and the data held by each one. Follows the principle that institutions can only ask for the same data from an individual once.</td>
</tr>
</tbody>
</table>

| a | (General Directorate Institutions and Population - Belgium, 2015) |
| b | (UN Statistics Division, 2015) |
| c | (UNICEF, 2015) |
| d | (UN Statistics Division, 2015) |
| e | (UN Statistics Division, 2014) |
| f | (General Directorate Institutions and Population - Belgium, 2015) |
| g | (Mariën & Audenhove, 2010) |
| h | (Elections Directorate - Belgium, 2013) |
| i | (Mariën & Audenhove, 2010) |
| j | (General Directorate Institutions and Population - Belgium, 2014) |
| k | (Mariën & Audenhove, 2010) |
| l | (Castro, 2011) |
| m | (Mariën & Audenhove, 2010) |
| n | (Mariën & Audenhove, 2010) |
| o | (Crossroads Bank for Social Security, 2014) |
Another notable feature of Belgium’s system compared to other countries in the Advanced category is that biometric data in the form of fingerprints and iris scans is not collected. One reason was that the cost of implementing the necessary scanning equipment, processes and software would have been too high considering that the National Register and unique RRN already existed and worked well, with strong central data management. Another reason was again the perceived political backlash that might follow such an idea.38

LEGAL FRAMEWORK39

Belgium has taken quite a stringent approach to data protection and privacy, with the establishment of the Commission for the Protection of Privacy (CPP). The CPP imposes a rigorous authorization process whenever an entity seeks to use or develop services based on access to personal identification data. This has come with certain challenges, such as the unwillingness of some private entities to invest in the development of services that integrate with the National Register or e-ID due to this rigorous CPP process.

Alongside its privacy and data protection framework, Belgium has instruments that allow for the access of public information, as well as the collection of data in a simplified, harmonized and integrated manner.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constitution of Belgium</td>
<td>2007</td>
<td>Article 32 relating to Freedom of Information: “Everyone has the right to consult any administrative document and to obtain a copy, except in the cases and conditions stipulated by the laws, federate laws or rules”</td>
</tr>
<tr>
<td>Act of 8 August 1983</td>
<td>1983</td>
<td>Provided for the establishment of a National Register of natural persons, and enshrines the principle of single collection (i.e. entities that have systematic access to the National Register cannot approach individuals to request any data that is already recorded in the Register.</td>
</tr>
</tbody>
</table>

38 (Mariën & Audenhove, 2010)
39 (General Directorate Institutions and Population - Belgium, 2014)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Law of 8 December 1992</td>
<td>1992</td>
<td>Protects privacy with regard to the processing of personal data. Established the Commission for the Protection of Privacy (CPP), which adheres to a very strict interpretation of allowed use of personal data and the RRN based on the principle of proportionality - i.e. no more data should be obtained than what is indispensable for the purpose of use.</td>
</tr>
<tr>
<td>Law of 15 August 2012</td>
<td>2012</td>
<td>Provided for the creation and organization of an integrator of federal services.</td>
</tr>
<tr>
<td>Act of 5 May 2014</td>
<td>2014</td>
<td>Guarantees the principle of single data collection in the functioning of the public services and agencies, and on the simplification and harmonization of electronic and paper forms.</td>
</tr>
</tbody>
</table>

**a** *(Mariën & Audenhove, 2010)*

### INSTITUTIONAL STRUCTURES

**General Directorate Institutions and Population** is responsible for the:

- Management of the National Registry
- Production and issuance of the electronic identity cards (e-ID)
- Organization of federal, regional and European elections

**Commission for the Protection of Privacy (CPP)** was established in order to supervise the use and the exchange of personal data. A number of sectoral committees within the CPP are required to authorize all exchanges of personal data, regardless of whether the requests originate from the government, administration or private sector. This means that organizations or entities seeking to use the e-ID or develop services based on the e-ID need to first request permission from the Privacy Commission.

---

40 *(General Directorate Institutions and Population - Belgium, 2014)*
41 *(Mariën & Audenhove, 2010)*
IDENTIFICATION PROCESSES

Birth registration

According to Belgian law, the birth of a child in Belgium must be registered within 15 days at the Town Hall (Maison communale/Stadhuis) of the place of birth. To register the birth the following are needed:

- A medical certificate issued by the hospital or medical practitioner
- The parents’ marriage certificate, if there is one, or a parent certificate for the father
- Both parents’ ID cards

In return parents are provided with various forms which they can then use to apply for benefits.

National Register

Through an online application called ‘My Folder’ accessible from the e-government website, individuals can view the information held about them in the National Register. If they find any error in this data, they can report it via the same application42.

e-ID card43

Applicants are required to:

- Report in person to the Registry Office of their principal place of residence
- Present a recent passport photo and their current identity card (or the replacement certificate from the police if it has been lost or stolen)
- Pay a fee of 10-15 Euros (the price may vary from one municipality to another as each municipality is entitled to charge an extra local tax. Some municipalities do not charge for the eID at all)

The waiting time for a new card is three to four weeks, after which the individual will receive a letter stating that their new eID is ready to collect from their local Registry Office. When collecting their new identity card, they must return the old card (or the replacement certificate from the police). The eID is valid for ten years, and towards the end of this period, the individual will automatically receive a notification in the mail to apply for a new card.

42 (General Directorate Institutions and Population - Belgium, 2014)
43 (Government of Belgium, 2015)
For Kids-ID application with the municipality, an adult is required to:

- Exercise parental authority over the child
- Accompany the child to the municipal Registry Office
- Provide a recent photo of the child

The waiting period for obtaining a Kids-ID is three weeks, although this can be expedited for a fee.

Some of the current challenges faced by Belgium include the following:

- **Relatively low uptake of the multiple uses of the e-ID:**
  
  - **Complex technology requirements:** The Belgian government offers over 600 online services that can be leveraged with the e-ID, including applications such as “Police on the Web” (allows citizens to interact with local police to report crime) and online transactions using the digital certificate and signature features. However, reported usage of e-IDs is relatively low, potentially due to the additional hardware and software required to make use of these features (e.g. card readers, software to support digital signing etc.). It has been suggested that these applications are not user-friendly for some individuals who may not be as technologically literate as others.

  - **Federal Token still used:** Also some users are still using the Federal Token, which is a personal card with 24 unique codes securing access to e-government services without the need for additional hardware or software. The concept of the Federal Token was introduced in 2003 as an intermediate solution for providing citizens access to e-ID services and applications without the e-ID. However, although almost all citizens possess an e-ID a large group still prefers the use the Federal Token instead of buying or using a card reader.

  - **Low uptake of digital signature:** existing order forms for online transactions are still considered binding. Private companies consider therefore that there is no stringent need to change the existing online

---

44 (General Directorate Institutions and Population - Belgium, 2015)
45 (Mariën & Audenhove, 2010)
transaction structures by introducing the process of authentication via the e-ID or a legally binding signature via the e-signature. The financial input for doing so is seen as too high compared to the possible return on investment in terms of higher legal security.

- **Extensive processes designed to protect privacy limits private sector innovation:** very few private organizations develop or implement e-ID based services or online e-ID data capturing features. The necessary effort to navigate the authorization process mandated by the CPP is considered too high compared to the return on investment.

- **Federated governance structure has led to piecemeal development of services:** Belgium is a Federal Constitutional Monarchy where specific competencies are dispersed across three governmental levels. The Federal Government cannot influence or oblige regional governments to implement specific applications. Each governmental entity develops applications according to its need and financial means. This has resulted in a somewhat scattered landscape of initiatives and networks, with different parts of Belgium offering different services. However, this level of localization within a nationally coordinated system may also be viewed as a strength, as the services offered in each area may be those that are most relevant to residents of that area.

- **Low levels of innovation leveraging identity services:** innovation on the platform enabled by the e-ID and National Registry requires participation on the part of both the citizens consuming the services, as well as the government and private entities developing the services. Increasing this participation through stronger communication and advocacy, easy-to-use hardware and software add-ons, and easily navigable privacy processes for the private sector may foster a higher level of innovation than Belgium has seen to date.
PAKISTAN

MATURITY ASSESSMENT

Categorization: Advanced

REGISTRY ASSESSMENT

Pakistan’s foundational national population database is managed by the National Database & Registration Authority (NADRA), and covers approximately 98% of the entire population. It is the single source of truth for identification data, and is linked to a Computerized National Identity Card (CNIC) which acts as the nation’s primary form of identity verification. It is also linked to the Civil Registration Management System (CRMS), which allows for electronic records to be created for vital events such as births, deaths, marriages and divorces.

Registration for the National Database was technically voluntary, but it was established as a prerequisite for accessing a number of other services such as obtaining passports and utilities connections. These requirements made it very difficult to refrain from enrolling and compelled citizens to register. Biometric data, namely the ten fingerprints and facial images, are collected during the registration process and are also stored on the CNIC chip (‘match on card’). The biometric and Automatic Fingerprint Identification System (AFIS) technology employed by NADRA enabled full de-duplication of the national database and greatly reduced the prevalence of dual identities and identity theft. Additionally, NADRA’s data collection and management processes are compliant with international standards such as ICAO and ISO enabling greater interoperability – for instance, the CNIC can be used as a valid travel document as it is ICAO compliant.

NADRA has employed an exemplary business and service delivery model that has enabled it to achieve a high coverage of the population in a financially self-sustaining way. The Government of Pakistan initially loaned NADRA some seed money to enable it to become financially independent. NADRA operates on a chargeback model, whereby it charges a fee to the government and other organizations for identity services provided. For example, banks are charged around 35 rupees each time they request NADRA to authenticate an individual when they open an account. With around 55 million such transactions that leverage NADRA’s systems

46 (Malik, 2014)
47 (NADRA, 2015)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>NADRA Civil Registration Management System (CRMS)</td>
<td>Foundational</td>
<td>34%+ of Births [1,563,796+] 35%+ of Deaths [approx. 356,836+]</td>
<td>Births, deaths, marriages, divorces</td>
<td>Paper-based certificates (birth, death, family registration, child registration, electronic record in NADRA population registry, unique identification number</td>
<td>Linked to NADRA National Database</td>
</tr>
<tr>
<td>NADRA National Database</td>
<td>Foundational</td>
<td>98%+ of population [approx. 178,458,000]</td>
<td>Biographics, all ten fingerprints, photograph</td>
<td>Electronic record in central database; Computerized National ID Card (CNIC)</td>
<td>National Database is the single source of truth for identity data, and CNIC is the primary form of identification used to authenticate across a number of public and private services: e.g. Financial, Social Protection, Insurance, Education, Healthcare, voting, Licenses, Tickets, Loyalty Programs. Card includes digital certificates, match-on-card (i.e. storage of biometrics in card chip) 36 security features, and QR code. Features deduplication based on biometric data (AFIS), and provides identity verification services to a number of public and private entities, billed according to a chargeback model.</td>
</tr>
<tr>
<td>Registry/ID</td>
<td>Type</td>
<td>Usage</td>
<td>Data Captured</td>
<td>Output</td>
<td>Level of Integration</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Benazir Income Support Program (BISP), Internally Displaced Person program, Citizen Damage Compensation program, Pakistan Card</td>
<td>Functional</td>
<td>8,540,000&lt;sup&gt;g&lt;/sup&gt;</td>
<td>N/A – not a separate registry, CNIC used as basis for identification</td>
<td>Various cards/credentials depending on the support program: BISP smart or debit card, IDP card, CDCP card, Pakistan Card&lt;sup&gt;h&lt;/sup&gt;</td>
<td>Linked to NADRA National Database. Identity verification for these financial support programs is based on National ID Card (biometric matching)&lt;sup&gt;i&lt;/sup&gt;</td>
</tr>
<tr>
<td>NADRA ePassport</td>
<td>Functional</td>
<td>&gt;7 million&lt;sup&gt;j&lt;/sup&gt;</td>
<td>Biographics, biometric data (facial and fingerprint)&lt;sup&gt;k&lt;/sup&gt;</td>
<td>Multi-Biometric passport&lt;sup&gt;l&lt;/sup&gt;</td>
<td>Established NADRA National Database Registration and CNIC as prerequisites for obtaining a passport&lt;sup&gt;m&lt;/sup&gt;</td>
</tr>
<tr>
<td>Voter Registry</td>
<td>Functional</td>
<td>86,189,802&lt;sup&gt;n&lt;/sup&gt;</td>
<td>N/A – based on National Database&lt;sup&gt;o&lt;/sup&gt;</td>
<td>N/A</td>
<td>Registry prepared based on NADRA National Database, and re-verified with door-to-door outreach. CNIC was required to vote. Planned for next election (with support from all political parties): biometric voter identity verification&lt;sup&gt;p&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

a (UNICEF, 2013)  
b Out of total 4,599,400 (UNICEF, 2013)  
c (UN Statistics Division, 2013)  
d Based on approx. total deaths 1,019,533 (UN Statistics Division, 2009)  
e (Malik, 2014)  
f (World Bank, 2014)  
g (World Bank, 2014)  
h (World Bank, 2014)  
i (World Bank, 2014)  
j (NADRA, 2015, p. 81)  
k (NADRA, 2015)  
l (NADRA, 2015)  
m (Malik, 2014)  
n (International Institute for Democracy and Electoral Assistance (IDEA), 2013)  
o (Malik, 2014)  
p (Malik, 2014)
and generate income, NADRA has become financially self-sustaining. NADRA also competes for projects both within and outside of Pakistan. Income from foreign projects amounted to USD $17.6m in 2013, which was reinvested back into the corporation’s operations and infrastructure. In this way, NADRA has been able to operate without a regular budget from the Pakistan government for a number of years.

**LEGAL FRAMEWORK**

Although Pakistan has established a central database that holds personal and biometric data on close to 100% of its citizens, it does not yet have an official data privacy law. The current legal framework does not provide for data controllers, data protection officers, nor a national data protection authority. So far, the protection of personal data collected for the NADRA National Database has largely relied on the robust data management practices of NADRA itself. Although Pakistan has ratified international treaties that recognize privacy as a fundamental human right, and its Constitution recognizes it as an inviolable right, the current legal framework does not yet enable the true spirit of these instruments to be enforced.

Pakistan has passed legal instruments that provide for Freedom of Information at a federal and provincial level, and a draft bill to enable the government to address electronic crimes is to be tabled later in 2015.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constitution of Pakistan</td>
<td>1973</td>
<td>Establishes the principle that privacy is linked to the dignity of a person. Article 14 (1) Inviolability of dignity of man: “The dignity of man, subject to law, the privacy of home, shall be inviolable”.</td>
</tr>
<tr>
<td>Freedom of Information Ordinance</td>
<td>2002</td>
<td>Provides for transparency and freedom of information to ensure that the citizens of Pakistan have improved access to public records and for the purpose to make the Federal Government more accountable to its citizens.</td>
</tr>
</tbody>
</table>

---

48 (Malik, 2014)  
49 (Malik, 2014)  
50 (Vohra & Akhlaq, 2012)  
51 (Malik, 2014)  
52 (Bytes for All Pakistan, 2014)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punjab Transparency and Right to Information Act</td>
<td>2013</td>
<td>Provincial Freedom of Information Laws enacted pursuant to the 2002 Freedom of Information Ordinance</td>
</tr>
<tr>
<td>NADRA Ordinance</td>
<td>2000</td>
<td>Provides for the establishment of a national population database and a primary identification credential. Details a comprehensive blueprint for how to register individuals into a national database. The Ordinance later became an act of Parliament under the 18th Amendment to the Constitution.</td>
</tr>
<tr>
<td><strong>DRAFT BILL: Pakistan Electronic Crimes Act</strong></td>
<td>2014</td>
<td>The proposed bill would ensure that information systems including private information are safeguarded against illegal access from both within and outside of the organizations that hold the data.</td>
</tr>
</tbody>
</table>

a (Bytes for All Pakistan, 2014)

INSTITUTIONAL STRUCTURES

National Database & Registration Authority (NADRA) is a division of the Ministry of the Interior (MOI) but is an independent corporate body. NADRA Technologies Limited is registered with the Securities and Exchange Commission of Pakistan, and is wholly owned by NADRA. Although it sits within the MOI, it operates autonomously of the government with respect to finance and management (as provided for by the NADRA Ordinance), and receives no government funding. By virtue of his post, the chairman of NADRA is also the registrar general of Pakistan. NADRA is responsible for registration of the national population and issuance of identity cards.

Electoral Commission of Pakistan (ECP) manages the voter registry, which used to be maintained through door-to-door re-verification exercises based on the previous electoral roll. In the most recent elections, the NADRA database was used initially as a source for identification data on the population eligible to vote, with re-verification by the Electoral Commission carried out after the initial lists.

---

53 (Malik, 2014)  
54 (NADRA, 2015)
were compiled. For the next elections, the Electoral Commission may leverage the NADRA National Database for biometric voter identity verification.\textsuperscript{55}

IDENTIFICATION PROCESSES

\textit{Birth registration}\textsuperscript{56}

Informants present in person to the Union Council, fill out a form, and provide their identification. The Union Council issues the birth certificate and creates a record in the NADRA National Database, using the computers and software provided by NADRA. This process must be completed within 2 months of the child being born.

The process for late registration is more complex, requiring two affidavits and the presentation of the child to the District Health Officer (DHO). The DHO then issues a letter to the concerned Union Council authorizing the late entry. Once this process has been completed, the informant can go to the Union Council for registration per the usual process.

\textit{NADRA mobile birth registration}\textsuperscript{57}

NADRA developed a program with NGOs and the telecom sector in Pakistan to develop a mobile application to facilitate preregistration. Pakistan has a high density of mobile phone users, and any midwife or parents can use the mobile application to pre-register a birth in the NADRA National Database. NADRA's infrastructure, such as mobile vans, can then be mobilized to go and register the child and take this record to the Union Council.

\textit{ID card (CNIC)}\textsuperscript{58}

- CNIC applicant must present in person to a registration center and produce proof of identity (one of the following documents): Birth Certificate, old NIC, Matriculation Certificate, CNICs of immediate/blood relatives, or Citizenship certificate issued by MOI
- Data Acquisition occurs at Data Acquisition Unit (DAU) and photo, fingerprint and signature captured
- Data is automatically checked for deduplication and then uploaded to NADRA Data Warehouse

\textsuperscript{55} (Malik, 2014)
\textsuperscript{56} (Canada: Immigration and Refugee Board of Canada, 2013)
\textsuperscript{57} (Malik, 2014)
\textsuperscript{58} (NADRA, 2015)
- CNIC produced and delivered to the registration center where the applicant can collect it

Delivery times: Normal - 30 days, Urgent - 15 days, FastTrack - 15 Days

Fees: free for first-time applicants. Replacement card fees are shown below\(^{59}\):

<table>
<thead>
<tr>
<th>Application type</th>
<th>Normal</th>
<th>Urgent</th>
<th>Executive</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNIC</td>
<td></td>
<td></td>
<td>1500</td>
</tr>
<tr>
<td>CNIC</td>
<td>200</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>CRC</td>
<td>50</td>
<td>-</td>
<td>500</td>
</tr>
<tr>
<td>FRC</td>
<td>500</td>
<td>-</td>
<td>1000</td>
</tr>
<tr>
<td>Death certificate</td>
<td></td>
<td></td>
<td>50</td>
</tr>
</tbody>
</table>

**Increasing registration in remote or marginalized populations**

NADRA employed a number of creative outreach methods to dramatically increase the coverage of the National Database:

- Combination of static registration centers, mobile vans and semi-mobile units that could all transmit data back to the centralized database
- Mobile registration vans with women drivers sent into hujiras (areas reserved for women) or areas ruled by warlords, as well as incentivizing women to register by offering grants from the Benazir Income Support Program (BISP).
- Registration with NADRA and ownership of an ID card were established as pre-requisites to participating in programs such as BISP, and to signing up for a passport. This means that if women wanted to embark on their hajj pilgrimage, they would need a passport and therefore need to be registered with NADRA.
- Introduced motorcycle registration units to complete registration in remote areas that were beyond the reach of mobile vans. Hired hikers, mountaineers and skiers to proceed into the mountain areas and communicate with the communities there.

\(^{59}\) (Malik, 2014)
CURRENT CHALLENGES

Some of the current challenges faced by NADRA include:

- Collection of service fees from the government in return for identity services that have been provided by NADRA. The Government of Pakistan currently owe NADRA billions of rupees in unpaid fees\textsuperscript{60}.

- There are many potential future applications that could leverage NADRA to increase transparency in the dealings between citizens and government (e.g. justice system). However, in some cases, there are entities with more to gain from lack of transparency that might seek to block progress\textsuperscript{61}.

- The lack of data protection and privacy laws is a notable gap in Pakistan’s legal framework, considering the amount of personal (including biometric) data is held by the government. It may consider establishing a privacy commission or a national data protection authority.

\textsuperscript{60} Malik, 2014

\textsuperscript{61} Malik, 2014
KENYA

MATURITY ASSESSMENT

Categorization: Intermediate

REGISTRY ASSESSMENT

Kenya has three foundational identity systems in addition to numerous functional programs covering services such as voting, social security, compulsory health insurance, tax and immigration. The Integrated Population Registration System (IPRS), launched in 2015, is designed to be the central repository of all identification data, linking the functional systems with the main foundational registries. The IPRS consists of two parts: 1) the National Population Register component will contain data on all Kenyan citizens and aliens, and 2) a unique 11-digit PIN assigned to a person’s record will act as a reference for all transactions involving that person. Their digital file will be continually updated with digital copies of documents attributable to that individual over their lifetime (e.g. National ID, NSSF card, NHIF card, marriage certificates, driving license, passport). The IPRS allows updating of information by various agencies within the legal framework that is in place. Data is accessible to these authorized agencies via web portal, SMS or email.

Integration of the IPRS with a range of functional services is currently underway – data relating to approximately 57% of the population has been entered into the registry from the existing primary registration databases (CRVS, National ID register, immigration/refugee departments). Kenya aims to have all remaining agencies integrated into the IPRS by 2016. In terms of eGovernment, online application functionality is already available via the eCitizen portal for business registry, marriage certificates, passport applications, visas and title searches, with birth/death certificate application functionality to be made available soon.

The primary form of authentication for services is the National ID Card, with the new e-ID card incorporating biometric data as well as biographical data. The National ID Card is also a pre-requisite to create an account for the M-Pesa money transfer platform, which is being increasingly used to process transactions between individuals and government agencies in Kenya (e.g. NSSF, NHIF). Additionally, a KRA PIN is also required to authenticate to some services (Tax and NSSF).
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration (CRD)</td>
<td>Foundational</td>
<td>Births: 58.4%[^929,400]=929,400; Deaths: 45.6%[^141,565]</td>
<td>Births and deaths</td>
<td>Paper-based certificates, data manually entered into IPRS</td>
<td>Record is created in IPRS for every new identity registered (manual). Death registration data is not reflected in any other registries.</td>
</tr>
<tr>
<td>Integrated Population Registration System (IPRS)</td>
<td>Foundational</td>
<td>57% of entire population [24 million over 18, 1 million newborns] 17m children under 18 to be enrolled in next 6 months – this will bring the usage to ~95%</td>
<td>Unique PIN, Biographics, Marital Status, Occupation, Biometrics, Family Relations, Issued Documents, Date of Death (where applicable)</td>
<td>Digital record; Unique ID (11-digit PIN)</td>
<td>Central electronic repository – data is pulled in from other registries rather than acquired through enrolment. Currently integrated with databases of CRD, National Registration Bureau, Dept of Immigration and Dept of Refugee Affairs. Planned: future integration with IEBC, NSSF, KRA, NHIF</td>
</tr>
<tr>
<td>National ID Card Register (National Registration Bureau)</td>
<td>Foundational</td>
<td>34% of population over 18 [8,713,000]</td>
<td>Existing ID cards: biographics, health, finance / payments, tax / customs New e-ID cards: + Fingerprint + Photograph + Company certificates of incorporation + Title deeds</td>
<td>National e-ID Card</td>
<td>Used to authenticate across a number of functional services, as well as M-Pesa money transfer platform[^9]. Can be used to travel within the EAC. Data is de-duplicated using AFIS.</td>
</tr>
<tr>
<td>Registry/ID</td>
<td>Type</td>
<td>Usage</td>
<td>Data Captured</td>
<td>Output</td>
<td>Level of Integration</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------</td>
<td>--------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voter Registry (IEBC)</td>
<td>Functional</td>
<td>14,352,545 out of the ~21m voting population in 2003</td>
<td>Biographics, National ID card/passport number, Telephone number, photograph, fingerprints</td>
<td>Voting register stored on a central database and used for online/SMS verification during voting. Physical copies printed as a backup.</td>
<td></td>
</tr>
<tr>
<td>Social Security Fund (NSSF)</td>
<td>Functional</td>
<td>4,272,853 in 2010</td>
<td>National ID and fingerprints; OR National ID and Unique ID (PIN)</td>
<td>NSSF card</td>
<td>KRA PIN used to authenticate for NSSF services</td>
</tr>
<tr>
<td>Tax (KRA)</td>
<td>Functional</td>
<td>10% of population [4.5 million]</td>
<td>National ID number (or National ID number of parent/s)</td>
<td>KRA PIN</td>
<td>KRA PIN used to authenticate for NSSF services</td>
</tr>
<tr>
<td>Hospital Insurance Fund (NHIF)</td>
<td>Functional</td>
<td>10% of population [4.5 million]</td>
<td>National ID, photo, copies of birth certificates for dependents</td>
<td>NHIF card</td>
<td></td>
</tr>
<tr>
<td>Passport</td>
<td>Functional</td>
<td>Name, DOB, Place of Birth, Sex, Nationality, Photograph</td>
<td>Machine Readable Travel Document (MRTD)</td>
<td>Integrated with IPRS.</td>
<td></td>
</tr>
<tr>
<td>Aliens Registry</td>
<td>Functional</td>
<td>Biographics, travel document details, photographs, fingerprints</td>
<td>Aliens card</td>
<td>Records are not yet digitized. Data is shared with the National Registration Bureau.</td>
<td></td>
</tr>
<tr>
<td>Registry/ID</td>
<td>Type</td>
<td>Usage</td>
<td>Data Captured</td>
<td>Output</td>
<td>Level of Integration</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Business Registry</td>
<td>Functional</td>
<td>Town, Industry, Business Type, Business Name</td>
<td>Paper based certificate</td>
<td>Integrated with IPRS</td>
<td></td>
</tr>
<tr>
<td>Marriage Registry (&amp; Divorce)</td>
<td>Functional</td>
<td>Name, Age, Occupation, Residence, Father’s Name, Father’s Occupation</td>
<td>Paper based certificate</td>
<td>Integrated with IPRS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
</tr>
<tr>
<td>b</td>
</tr>
<tr>
<td>c</td>
</tr>
<tr>
<td>d</td>
</tr>
<tr>
<td>e</td>
</tr>
<tr>
<td>f</td>
</tr>
<tr>
<td>g</td>
</tr>
<tr>
<td>h</td>
</tr>
<tr>
<td>i</td>
</tr>
<tr>
<td>j</td>
</tr>
<tr>
<td>k</td>
</tr>
<tr>
<td>l</td>
</tr>
<tr>
<td>m</td>
</tr>
<tr>
<td>n</td>
</tr>
<tr>
<td>o</td>
</tr>
<tr>
<td>p</td>
</tr>
<tr>
<td>q</td>
</tr>
</tbody>
</table>
LEGAL FRAMEWORK

Kenya has a number of legal instruments in place that establish the compulsory nature of birth and death registration, protect the right to privacy and security of personal data, enable the public to access information contained in government databases and have any personal information corrected, and finally facilitate the use of technology in key public activities.

Some of the challenges that Kenya has faced in this space include a number of cases identified by the immigration ministry where foreigners had illegally acquired documents (IDs and passports) through corrupt officials. Another concern for Kenya is the rise of cybercrime and cost to the nation each year as a result. The government has taken preventative action in the form of introducing Public Key Infrastructure for digital certification of online transactions, establishing a national Computer Incident Response Coordination Centre, and developing a National Cyber Security Strategy.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Births and Deaths Registration Act</td>
<td>1928</td>
<td>Established compulsory birth and death registration at a national level</td>
</tr>
<tr>
<td>Draft National Registration and Identification Bill (yet to be passed)</td>
<td>2012</td>
<td>Currently under stakeholder consultation. The draft bill proposes to provide for the notification and registration of vital events, the identification of citizens, and issuance of documents of registration and identification. It also proposes to combine the separate processes and institutions that are responsible for birth, death, immigration, issuance of IDs and refugees.</td>
</tr>
<tr>
<td>Registration of Persons Act Cap 107</td>
<td>1949</td>
<td>Provides for the process of registration of persons, the issuance of identity cards, and the appointment of a principal registrar, provincial and county registrars.</td>
</tr>
</tbody>
</table>

62 (Measure Evaluation Kenya, 2013)
63 (Mbote, 2013)
64 (Article 19, 2014)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constitution of Kenya</td>
<td>2010</td>
<td>Established the requirement for citizenship to be conferred at birth (Article 14) and the requirement for citizens to have access to registration services (Article 12). Protects right to privacy, including privacy of communications (Article 31) Mandated the IEBC to regularly revise the voter registry by adding eligible voters, deleting dead voters and effecting transfers and corrections (Article 88)</td>
</tr>
<tr>
<td>Freedom of Information Act</td>
<td>2005</td>
<td>Enables public to obtain access to information held by government agencies and private bodies, enables persons to have inaccurate personal information about them corrected, and establishes systems/processes for the publication of information</td>
</tr>
<tr>
<td>Data Protection Bill (yet to be passed)</td>
<td>2012</td>
<td>Regulates the collection, retrieval, processing, storing, use and disclosure of personal data</td>
</tr>
<tr>
<td>Access to Information Act</td>
<td>2012</td>
<td>Allows the public access to government information, within predefined rules</td>
</tr>
<tr>
<td>Citizenship and Immigration Act</td>
<td>2011</td>
<td>Regulates matters relating to citizenship, issuance of travel documents and immigration (including registration for citizenship at birth, and registration of aliens)</td>
</tr>
<tr>
<td>Election Act</td>
<td>2011</td>
<td>Allows the Electoral Commission “to use such technology as it considers appropriate in the electoral process” (e.g. biometric voter registration, and potentially e-voting in future)</td>
</tr>
<tr>
<td>Cybercrime and Computer Related Crimes Act</td>
<td>2014</td>
<td>Equips law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime</td>
</tr>
<tr>
<td>Income Tax Act (Cap 470 Laws of Kenya)</td>
<td>1989</td>
<td>Section 132 established the requirement to identify a person based on their KRA PIN before the person can transact with the KRA</td>
</tr>
</tbody>
</table>
INSTITUTIONAL STRUCTURES

Ministry of Immigration and Registration of Persons (MIRP)

- Civil Registration Department (CRD): Core functions include the registration of births and deaths, the preservation, security and custody of certificates, and the processing, analysis, and dissemination of vital statistics from birth and death records.
- National Registration Bureau: Responsible for the production and issuance of National ID Cards.
- Department of Refugee Affairs: Responsible for the issuance of ID cards and travel documents to refugees in Kenya.
- Department of Immigration Services: Responsible for the issuance of passports and other travel documents.
- Integrated Population Registry Service: Operates and maintains the IPRS. Enables authorized entities to perform validation checks based on IPRS data.

Ministry of Health (MOH), and in particular the Health Information System unit for vital statistics, is responsible for compiling and analysing maternal health statistics and medically certified cause of death statistics. These statistics are used by the KNBS and IPRS.

Kenya National Bureau of Statistics (KNBS) is responsible for disseminating official vital statistics on births and deaths and for computing annual vital events indicators by province, based on data received from CRD and MOH.

Annual Stakeholders Meeting involves an annual gathering of all civil registration stakeholders.

Technical Working Group (TWG) was formed in February 2011 following a recommendation by the stakeholders meeting. The TWG consists of representatives from Kenyan government departments, UN agencies, and international development partners including World Vision and PLAN. TWG members meet...
monthly to advise the CRD on civil registration strategies and innovations. The TWG also collaborated to produce the draft 2013-2017 Strategic Plan.

**IDENTIFICATION PROCESSES**

**Birth registration**

- **Notification:** Local registration agent completes details on an official registration form which includes a perforated stub which is the ‘notification slip’. This slip and the original notification is given to the parents or relative, while the local agent retains the carbon copy of the notification. The completed form can be considered ‘pre-registration’ until legal registration is completed. For home births, the notification process is completed with the assistant chief of the sub-county where the child was born. For children born in medical institutions, the institution handles the notification process.

- **Legal registration:** The local registration agent submits the completed form to the Civil Registry Office (CRO) to be legally recognised and recorded, followed by the generation of a personal identification code. This constitutes legal registration. The newborn’s parents or relative then produce the proof of notification to the CRO, the notification slip is matched with the registration in the system, and a birth certificate is issued.

- **Fees:** The birth registration process must commence within three months of birth. Notification and registration are both free within that period. After that time, a penalty of 150 Kenyan Shillings is applied.

**‘MOVE-IT’ birth notification**

The MOVE-IT (Monitoring of Vital Events through Technology) program is the result of a partnership between the Civil Registration Department and the Ministry of Health. Community health workers are equipped with software that allows them to report vital events, along with their location, to the local sub-chief by using their mobile phone. The workers, who are often volunteers, are paid a small allowance as an incentive to complete these notifications. The system reflects the vital event information in a central electronic database as well as a real-time dashboard, which shows the number of birth notifications that have been notified via SMS per county and sub-county. This provides a useful baseline against which the registration activities of chiefs/assistant chiefs in a particular county can be tracked.

---

71 (Government of Kenya, 2015)
72 (Measure Evaluation Kenya, 2013)
73 (Muga, 2013)
and checked for compliance. This means that after SMS notification is received, if chiefs/sub-chiefs delay birth registration for any reason, it will show up on the system. A similar RapidSMS birth notification system is also used in Nigeria.

**Integrated Population Registry System (IPRS)**

- Following legal registration of a newborn, birth certificate data is entered into the IPRS system by the CRO.
- Each time a new record is created in the IPRS, a unique 11-digit PIN is allocated to the record. This acts as the individual’s unique identifier for life.
- This electronic record will continually be updated with information and digital copies of documents obtained throughout the course of the individual’s life via the integration with other government agencies (e.g. primary and secondary school certificates, national identity card, drivers license, passport, etc.)
- Currently the main function of the IPRS is to perform identity verification services, although it does not yet charge a fee for these services

**National ID Card**

- The application must present in person to the District Office with proof of age, names and place of birth, and a completed application form signed by the chief or assistant chief of the sublocation within their District
- District Officer signs the application form
- Fingerprints and a passport size photograph of the applicant are taken and sent with the form to the National Registration Bureau for the creation of the national identity card
- The applicant is provided with a temporary card that they can use until their National ID Card arrives (waiting time of up to two months)
- After two months has elapsed, the applicant returns to the District Office to collect their National ID Card

**CURRENT CHALLENGES**

Registration is reliant upon community-based notification, but there is often lack of awareness or belief that registration is not necessary. Also, some Civil Registration Offices (CRO) lack the necessary infrastructure and capacity (i.e.

74 (Mutegi, New digital registry to limit identity theft, catch aliens (Kenya), 2015)
75 (Government of Kenya, 2015)
internet connectivity, installation of software, training/support) and often there are too few CROs to provide timely and quality services to the districts they are tasked to cover\textsuperscript{76}.

Apart from manual registration at CROs, online registration has been enabled for marriages, new businesses, land and re-issuance of drivers’ licenses, via the eCitizen portal, as well as for social security via the NSSF website. Birth/death registration functionality is planned to be delivered in the future as part of the eCitizen portal, which may help to alleviate some of the capacity issues currently faced by the CROs\textsuperscript{77}. However, while part of the process can be completed online through the portal, there are still manual steps that must be taken afterwards. For example, after applying for the renewal of a drivers’ license online, the applicant must still produce a printout of the renewal slip to the government office in order to obtain their new license. Additionally, the eCitizen portal did not receive an official launch – as a result, the public is still relatively unaware of the initiative. When applicants visit Huduma centers for various procedures, they are directed by staff to log in to the portal and access the relevant services online, which is when they come to know about the online system.

To improve the level of community engagement and notification rates for vital events, Kenya is leveraging mobile technology as part of the MOVE-IT program. When text messages are sent by health workers to local authorities to notify of a vital event, the authorities know to kick off the registration process\textsuperscript{78}. However, the uptake of this program is still quite low to date, indicating that perhaps incentives and better communication may be required.

Other challenges include the following:

- **CRVS**
  - Duplicate registrations occur due to immature search functionality
  - Low registration in vulnerable and border populations
  - Cause of death data is not optimally captured
  - Paper-based bound volumes of data are still in the process of being digitized. However, the digital repository is not structured as a relational database.

\textsuperscript{76} (Measure Evaluation Kenya, 2013)
\textsuperscript{77} (Government of Kenya, 2015)
\textsuperscript{78} (World Health Organization (WHO), 2013)
- **IPRS**
  - Yet to be linked with Kenyan embassies to facilitate passport renewal of citizens living abroad
  - Can only verify authenticity of credentials, rather than verify identity of individuals based on biometric scanning and comparison
  - Contains a large amount of personal data that would be of commercial value and interest to a variety of entities, but is currently not adequately protected by the existing legal framework (i.e. requires data protection legislation)

- **National ID**
  - Delays in kicking off registration for new Smart ID Cards in 2015
  - Registration on-site at enrolment centres is required in order to provide biometric data
  - AFIS system can currently only compare ink prints with stored ink images – cannot compare digitally scanned prints with stored images of ink prints

- **Business registry**
  - No Corporate ID as yet
REGISTRY ASSESSMENT

Mexico has several parallel registration systems, from civil registration, to a national ID, to a voter registration card. Though all are used, the voting registry has the largest coverage of the population and has therefore become more of a foundational registry than a functional one. In fact, the voter ID is so widespread that it has become an acceptable way for citizens to identify themselves. It is not uncommon for a voter ID card to be used to open a bank account, travel by air, and purchase alcohol. What started two decades ago as a way to catch fraudulent voters, the voter ID card has become the country’s preferred credential.

The birth registry in Mexico captures 93% of births, however, an estimated 7 to 10 million of Mexico’s 122 million population still remain unregistered. The registration process requires several forms of identification, such as a certificate of live birth, each parent’s birth certificate, a marriage certificate, and sometimes a fee, all of which can inhibit marginalized sectors of the population from registering.

Mexico’s national identification system utilizes the CURP (Clave Única de Registro de Población), a national ID with 18 alphanumeric characters. The characters are built methodically, with the first few letters aligning with the individual’s name, two aligning with date of birth, one aligning with gender, and other coding for the remaining elements. The CURP is required for tax filings, starting a business, enrolling in education, membership in government-run health services, passport applications, and other government services.

The CURP is not fully integrated with the population, as it is not required for children under 18 years of age, so Mexico started issuing biometric IDs in the form of Personal Identity Cards for Minors, and National Citizen ID Cards for people

---

79 (Gelb, Unique Legal Identity and the Spread of Identification Programs, 2015)
80 (Agren, 2012)
81 (Migration Policy)
82 (Universal Domain Exchange)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>Foundational</td>
<td>93% Births&lt;sup&gt;a&lt;/sup&gt; [113,460,000] &gt;90% Deaths [109,800,000]&lt;sup&gt;b&lt;/sup&gt;</td>
<td>Birth details, biographic data, cause of death</td>
<td>Paper and electronic birth certificate</td>
<td>Certificate is required and used for authentication for other forms of identification (CURP, voting, National ID) and public services (formal employment, Popular Health Insurance)&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>CURP (Clave Única de Registro de Población / Unique Population Registry Code / Personal ID Code Number)</td>
<td>Foundational</td>
<td>67.4% of population [81,740,000]</td>
<td>Biographic data, also captures credentials from other form of ID (passport, voter ID, birth certificate, immigration visa) for validation</td>
<td>Front contains Alphanumeric 18 characters&lt;sup&gt;d&lt;/sup&gt;. Date of registration and folio number. Back references the document ID used to obtain CURP. If a birth certificate, will include folio number, issuing municipality, and a barcode.&lt;sup&gt;e&lt;/sup&gt;</td>
<td>The CURP number is used in all civil registrations and also is required to obtain other forms of identification&lt;sup&gt;f&lt;/sup&gt;</td>
</tr>
<tr>
<td>National Citizen Registry (for Citizens 18+)</td>
<td>Functional, but intended to grow to be foundational</td>
<td>N/A</td>
<td>Personal information from birth certificate, Barcode and Biometrics&lt;sup&gt;g&lt;/sup&gt; (10 fingerprints, face picture, 2 iris, digitized signature.&lt;sup&gt;g&lt;/sup&gt;</td>
<td>National ID card with 2D barcode with fingerprints encoded for offline identification&lt;sup&gt;h&lt;/sup&gt;</td>
<td>Integrated with National Youth Registry to form the National Population Registry; information is very well integrated and used by all units of public administration&lt;sup&gt;i&lt;/sup&gt;</td>
</tr>
<tr>
<td>Registry/ID</td>
<td>Type</td>
<td>Usage</td>
<td>Data Captured</td>
<td>Output</td>
<td>Level of Integration</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>National Youth Registry (Personal Identity Card for Minors)</td>
<td>Functional, but intended to grow to be foundational</td>
<td>N/A</td>
<td>Personal information from birth certificate, Collect digital records of iris images, fingerprints, a photograph, and a signature, parents' personal data</td>
<td>Minor Identity Card with barcode</td>
<td>Integrated with National Citizen Registry to form the National Population Registry; information is very well integrated and used by all units of public administration</td>
</tr>
<tr>
<td>Voting (Election Card / Credencial de Elector)</td>
<td>Functional</td>
<td>~100% of voting population [1,210,000]l</td>
<td>Biographic data</td>
<td>Voter ID card</td>
<td>Requires Birth certificate, Photo identification (e.g., passport)</td>
</tr>
<tr>
<td>RFC (Registro Federal del Contribuyente / Federal Taxpayers Registry)</td>
<td>Functional</td>
<td>N/A</td>
<td>Need a CURP to get an RFC</td>
<td>Same format as CURP, issues tax ID number</td>
<td>Can be used to access financial services</td>
</tr>
<tr>
<td>a (UNICEF, 2013)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b (United Nations)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c (Migration Policy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d (e-curp.com)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e (Universal Domain Exchange)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f (Universal Domain Exchange)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g (World Bank, 2015)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h (SEGOB, 2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i (SEGOB, 2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j (SEGOB, 2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k (Electronic Frontier Foundation, 2012)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>l (SEGOB, 2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
over 18 years of age, in 2010. 83 These cards collect biometric data such as iris images, fingerprints, a photograph, and a signature, which has served as a point of contention recently because of the high amount of data collection. The National Citizen Registry and National Youth Registry will integrated for form the National Population Registry. This form of biometric identification is very well integrated and used by all units of public administration. 84 85

**LEGAL FRAMEWORK**

The right to free and universal birth registration was recently passed in 2014. A year later, the challenge currently faced by the Mexican government is setting up the proper procedures and rules to enforce the new public policy. 86 Birth registration is mandatory under Civil Code for each of Mexico’s 32 states 87 The CULP is regarded as the official national ID, however, obtaining a national ID (CURP) is not mandatory by law.

Mexico passed a data protection law in 2010 that is fairly comprehensive. Voting laws in Mexico are set by the federal government and not individual states. 88

The collection of biometric data for Mexico’s new identity card has been controversial. In collecting youth biometrics, concerns have surfaced in collecting so much data, as there are currently no legal protections regulating the use of iris images in Mexico. 89

---

83 (Electronic Frontier Foundation, 2012)
84 (SEGOB, 2010)
85 (SEGOB, 2010)
86 (Center for Migration Studies)
87 (Migration Policy)
88 (Agren, 2012)
89 (Electronic Frontier Foundation, 2012)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
</table>
| Freedom of Information Law             | 2002 | Guarantees the right of citizens to access public information pertaining to their executive branch. It defines all government information as public and requires disclosure of information periodically. Specifically, to “make public administration transparent,” to “encourage accountability to citizens”  

Federal Law on the Protection of Personal Data | 2010 | Law that serves to protect personal data. Grant’s citizen’s rights in the collection and use of their own personal data. 

Right to Free and Universal Birth Registration | 2014 | Article 4 of the Mexican Constitution. The law entered into force in 2014, “explicitly guaranteeing the right of every person to free birth registration”  

Presidential Agreement for the Adoption and Use of the Population Registry Unique Code | 1996 | Provides the issuance of CURP cards as a national ID for everyone in Mexico as well as Mexicans living abroad. 

a (Doyle, 2002)  
b (Mexico Ministry of Interior)  
c (Center for Migration Studies)  
d (Universal Domain Exchange)

INSTITUTIONAL STRUCTURES

The government entity in charge of civil registration in Mexico is the **National Registry of Population and Personal Identification’s General Office (RENAPO)**. All civil registration is handled separately by state. In addition to Mexico’s government office, there are many NGOs and nonprofits in Mexico helping with registration. For example, Be Foundation is a nonprofit organization currently working to eliminate non-registration of births in Mexico.90

**The Office of Immigration (INM)** processes the CURP number. Government immigration offices are scattered throughout the country as to be more accessible.
to the Mexican population. The INM must collaborate with other offices, as CURP numbers are required to apply for many other forms of identification and public service.

**The National Electorate Institute / Insituto Nacional Electoral (INE)** is in charge of managing federal elections as well as issuing election cards. Because voter ID cards have functionally become more of a national ID system, the INE may have to step into more of a far reaching, national registration role in the future.

For the true functional registries, the **Mexican Institute of Social Security** issues the social security card to every working Mexican citizen, and the RFC is issued by the **Mexican Treasury**.

**IDENTIFICATION PROCESSES**

**Birth registration**

A birth certificate will either be issued following registration or through a separate application. All children must be registered within 6 months regardless of place of birth. For institutional births, a physician or midwife provides a “certificate of live birth” that parents present along with other required forms, like parents birth certificates and their marriage certificate, to the office of the civil registrar where the child was born. If the child is born at home, the same process applies.91

The fact that a certificate of live birth, both parents birth certificates, and a marriage certificate are necessary affects many marginalized sectors of the population, including but not limited to street births, single parent families, refugee or nomad births, children of migrants, and others. Additionally, holes in the process, from inconsistent implementation of the birth registration law, to disregard by parents, can lead to non-registration. Failing to register a birth can lead to large fines or judicial action.92

Birth registration is free in 16 states and costs vary in other states. In poor areas, this can serve as a barrier for registration. Initial registration fees are US$12 but late fees can be an additional US$30.

**CURP**

To register for a CURP, citizens must visit the nearest government office or civil registry in person. Mexicans both residing in Mexico and living elsewhere should

---

91 (Migration Policy)
92 (Migration Policy)
enroll for a CURP when 18 years old and older. Registration requires a birth certificate and official identification (e.g., passport, voter ID, proof of residence, etc.). The card used to be printed on green paper but now it is printed on black and white paper and laminated. Both forms are acceptable.

Once obtained, the CURP can be accessed electronically anytime. To check the CURP number or print a copy, citizens can go online to and enter name and birth data and access their record.

**National Identity Card (Youth and Citizen)**

To obtain a national identity card, people attend an enrollment office (or mobile unit) with a birth certificate and CURP card if applicable. The individual’s authentication is carried out via the CURP database and the civil registration database. A variety of biometrics are collected (face photo, 10 fingerprint biometrics, 2 iris images, a digital signature, and a scan of CURP or birth certificate).

**Electoral Card**

To enroll in the electoral register for the first time, it is required to have Mexican citizenship and to be 18 years old or older. Citizens can enroll at a polling station or agency service center and must renew every 10 years. Obtaining a card is considered relatively easy – cards are free and hundreds of issuing agencies exist across Mexico.

**CURRENT CHALLENGES**

Mexico has made significant progress with its registration but still faces a number of challenges:

- The requirements and process for birth registration affects many marginalized groups and leads to increased non-registration
- Half of states (16) charge for birth registration, and segments of the population are unable to pay
- Failing to register a birth is associated with large fines, yet the groups of people who are unregistered are usually effected by poverty

---

93 (e-curp.com)  
94 (Universal Domain Exchange)  
95 (e-curp.com)  
96 (SEGOB, 2010)  
97 (Agren, 2012)
- Registration is often very uneven between states - Chiapas and Guerrero have less than half of births under the age of one registered. Coincidentally, these states are some of the poorest regions in Mexico.

- CURP cards are sometimes printed at home and improper paper is flimsy and easily damaged or lost.

- CURP is not issued at birth or mandated by law, leading to decreased utilization.

- The usage of the Voter ID as the preferred method of identification excludes all children under 18 from participating in Mexico’s most widespread national registry.

98 (Migration Policy)
Nigerian has two foundational registries – the civil registration system to record vital events, as well as the national identity management system. The national identity management system consists of the following components:

- National Identification Number (NIN) System
- National Identity Database (NIDB)
- Automated Biometric Identification System (ABIS)
- Identity Authentication and Verification

The system incorporates standardized data capture processes in compliance with international data standards (ISO, ICAO, IEEE), and implements deduplication processes prior to the inclusion of the data. Biometric data is collected as part of the registration for the NIN – namely ten fingerprints, iris scan and photograph. The primary credential that is issued as a result of this process is a biometric General Multi-Purpose Card (or electronic ID card) that can be used to authenticate an individual’s identity across a number of public and private services. The card was developed in liaison with MasterCard, with Prepaid MasterCard functionality included in the e-ID. Fingerprint data is also stored locally within the card itself rather than in a central data, enabling ‘match on card’ functionality and increasing security.  

Following the launch of the NIN registration in 2014, about 15% of the adult population has been registered. Civil registration of vital events is still relatively low, with only 42% of births registered. The national identification management system is planned to be integrated with a number of public and private services, and eventually with the civil registration system as well.

---

(Onyemenam & Ross, 2014)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>Foundational</td>
<td>42% of births(^a) [3,012,660(^b)]</td>
<td>Births and deaths</td>
<td>Paper-based certificates</td>
<td>Not linked to National Identity Management system</td>
</tr>
<tr>
<td>National Identity Management System</td>
<td>Foundational</td>
<td>15% of adult population [14,491,000(^c)]</td>
<td>Biographics, ten fingerprints, iris scan, photograph(^d)</td>
<td>National e-ID Card (General Multi-Purpose Case – GMPC), unique National Identity Number (NIN), digital record in National Identity Database (NIDB)(^e)</td>
<td>Deduplication conducted prior to inclusion. Can be used as a basis for a number of applications: payments (EMV compliant with Prepaid MasterCard functionality), online banking, digital signature, travel (ICAO compliant), tax, social security, secure email, voting(^f).</td>
</tr>
<tr>
<td>Voter Registry</td>
<td>Functional</td>
<td>74,638,834</td>
<td>Biographics, photograph, ten fingerprints, with optional data fields for national ID card details and telephone number(^g)</td>
<td>Voter Identification Number (VIN) issued in 2011, Permanent Voter Cards (PVC) issued in 2015, however in 2019 National e-ID card will double as voter card(^h).</td>
<td>Deduplication conducted prior to inclusion. Not yet integrated(^i). Planned – e-ID to be used for 2019 elections, and will be compulsory in order to vote(^j).</td>
</tr>
</tbody>
</table>

\(^a\) (National Population Commission & UNICEF Nigeria, 2015)  
\(^b\) Of a total 7,173,000 births - (UNICEF, 2015)  
\(^c\) (World Bank, 2015)  
\(^d\) (National Identity Management Commission Nigeria, 2015)  
\(^e\) (National Identity Management Commission Nigeria, 2015)  
\(^f\) (National Identity Management Commission Nigeria, 2015)  
\(^g\) (Independent National Electoral Commission (INEC) Nigeria, 2015)  
\(^h\) (Independent National Electoral Commission (INEC) Nigeria, 2015)  
\(^i\) (Independent National Electoral Commission (INEC) Nigeria, 2015)  
\(^j\) (Nigeria launches national electronic ID cards, 2014)
Nigeria’s current legal framework provides for a civil registration system, allows for freedom of information held by the government, provides for a national population registry and mandates that the National Identification Number (NIN) be used as a basis for a number of services. However, it lacks legal instruments that support personal data protection and privacy, as well as those that would facilitate the secure electronic transmission of data (although with regards to the latter, bills have been drafted in the past to this end). It has been suggested that in conjunction with the review and update of Nigeria’s Data Protection and Privacy Laws, an independent regulatory body should be established to protect and enforce these rights\textsuperscript{100}.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom of Information Act</td>
<td>2011</td>
<td>Provides for public access to public records and information, as well as the protection of such information as consistent with the public interest and personal privacy</td>
</tr>
<tr>
<td>Draft Data Protection Bill (yet to be passed)</td>
<td>2010</td>
<td>In its current state per Article 2(2)(a), the bill does not apply to any government institution. It provides for the creation of a Privacy Commission, although limits the remedies available to the Commission to enforce the law, and does not specify in the legislation that the Commission needs to be independent.</td>
</tr>
<tr>
<td>National Identity Management Commission Act</td>
<td>2007</td>
<td>Establishes the mandate of the NIMC and provides for the creation of the National Identity Management system</td>
</tr>
<tr>
<td>Federal Government Decree No. 39</td>
<td>1979</td>
<td>Established the authority of the then Federal Military Government to register vital events to the National Population Commission (NPC)</td>
</tr>
<tr>
<td>Federal Government Decree No. 69</td>
<td>1992</td>
<td>States that registration shall be carried out free of charge, within a period of 60 days from the date of birth</td>
</tr>
<tr>
<td>Child Rights Act</td>
<td>2003</td>
<td>Establishes the right of every child to a name and registration of their birth (refer section 5)</td>
</tr>
</tbody>
</table>

\textsuperscript{100} \textit{(Akinsuyi, 2015)}
### Legal/Policy Instrument

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation on the Mandatory Use of the National Identification Number (NIN)</td>
<td>2015</td>
<td>NIMC regulation which states: &quot;From the 1st of July 2015 any government agency/institution, bank, insurance company and all other institutions offering services and or are involved in transactions requiring the identity of an individual as contained in section 27 of the Act, and who so transacts without demanding or using the NIN as contemplated hereunder, has committed an offence under the Act.&quot;</td>
</tr>
</tbody>
</table>

---

### INSTITUTIONAL STRUCTURES

The mandate of the **National Identity Management Commission (NIMC)** includes the following:

- Establish and maintain A Unique National Identity Database in Nigeria
- Register persons covered by the Act, assign a Unique National Identification Number (NIN)
- Issue General Multi-Purpose Cards (GMPC)
- Harmonize and integrate existing identification databases in Nigeria

**National Population Commission (NPC)** was established by the federal government in 1988. The Commission was reconstituted in 2011 with a Chairman and 37 members representing each state of the federation and the Federal Capital Territory. NPC has the statutory powers to collect, analyze and disseminate population/demographic data in the country. It is also mandated to undertake demographic sample surveys, compile, collate and publish migration and civil registration statistics as well as monitor the country's Population Policy.

The activities of the Registrar General of the NPC include the following:

- Issues general directives regarding registration of births and deaths
- Co-ordinates and unifies the activities of all registration officials

There are reports that NPC and the NIMC are currently discussing plans for a

---

101 (Government of Nigeria, 2015)
102 (Government of Nigeria, 2015)
103 (UN Statistics)
centrally managed population database as part of the country’s reform of its CRVS system.\textsuperscript{104}

IDENTIFICATION PROCESSES

Birth registration\textsuperscript{105}

- Institutional births: hospital registers the birth with the NPC
- Home births: parents obtain a sworn affidavit from their local government, stating that the child was born in that local government area. The sworn affidavit can then be taken to the NPC.
- NPC issues a standard birth certificate
- There are several locations at which birth registration takes place, including NPC registration centres, NPC offices at the local government headquarters, NPC desks in hospitals and health centres
- No fee is charged if registration is completed within 60 days of the birth

RapidSMS notification by NPC registrars\textsuperscript{106}

- Since January 2011 the NPC has been implementing decentralized monitoring using the mobile-phone based platform RapidSMS. The system was piloted in 2010 in 19 states, which included 382 local government areas and 1,582 registration centres.
- Presently, RapidSMS reporting is available across all 774 local government areas nationwide, processes more than 6,215 SMS messages per month, and automatically compiles data into an electronic repository of results that can be viewed via an online dashboard. Data is available per registration center, per state, per gender, and per age group.
- Each Registrar has his/her unique ID and reports the number of birth registration cases every fortnight. Those reported cases are all updated on the RapidSMS dashboard which is accessible over the web and visible/monitored by all levels of government. This helps to identify disparities in service delivery and facilitate prompt, evidence-based responses to areas where birth registration levels are low.

\textsuperscript{104} (Willmott-Harrop, 2015)
\textsuperscript{105} (Canada: Immigration and Refugee Board of Canada, 2008)
\textsuperscript{106} (Izumi, 2012)
Retrospective birth registration\textsuperscript{107}

Individuals born prior to 1992 may also obtain an NPC birth certificate. When registering with the NPC, such individuals must present a sworn affidavit from their local government and must undergo an interview prior to being issued a birth certificate.

National Identification Number (NIN)\textsuperscript{108}

- Option 1: applicant can visit the official website of NIMC (http://www.nimc.gov.ng) and pre-enrol online by filing the online Enrolment Form and print out a summary sheet that has a 2D Barcode. It is important to note that the Online Pre-Enrolment an initial step in the Enrolment process. The enrolment is only completed after the applicant gets his or her biometric data (finger prints, headshot photograph and signature) captured and processed by an Enrolment Officer at an Enrolment Centre

- Option 2: applicant presents in person to an Enrolment Centre or Mobile Enrolment Centre and fill an Enrolment Form (hard copy). The completed form is handed over to the Enrolment Office who in turn captures the biometric data of the applicant and processes the data in the completed enrolment form

- Application receives an SMS notification that their E-ID card is ready, after which they can collect it from the enrolment centre

Current Challenges\textsuperscript{109}

Some of the challenges with the current systems include the following:

- Poor coverage in registration of vital events
- Bureaucratic inefficiency
- Poor data management
- Stakeholder engagement and feedback systems not mature
- Poor public awareness and apathy to civic responsibilities among the population
- Legal framework lacks the instruments and institutions to protect personal data

\textsuperscript{107} (Canada: Immigration and Refugee Board of Canada, 2008)
\textsuperscript{108} (National Identification Management Commission (NIMC), 2015)
\textsuperscript{109} (Revamping the Civil Registration and Vital Statistics System in Nigeria , 2011)
Opportunities for improvement:

- Stronger collaboration with other relevant government agencies
- There is a current practice of having a registration desk or focal persons at major hospitals which could be extended to all maternity centers and registered Traditional Births Attendants (TBAs)
- Increase use of mobile registration systems. This may be applicable in remote areas where access to registration centers is difficult (e.g. build further on the existing use of RapidSMS)
- Involvement of community and religious leaders in advocating the importance of civil registration
- Improved training for death certification by physicians and proper use of ICD coding standards

UNICEF predicts that births in Nigeria will account for 10% of the total births in the world by 2050\(^{110}\). This is a strong case for change to uplift the current CRVS, and fortunately there seems to be a high level of political will to improve the system\(^{111}\).

---

110 (Willmott-Harrop, 2015)
111 (UN Statistics)
MATURITY ASSESSMENT

Categorization: Greenfield

REGISTRY ASSESSMENT

Sierra Leone currently has four functional identity programs and one foundational civil registry program, overseen by a number of different government agencies. Each program operates within its own mandate as a result of piecemeal legislation that has developed over time. The processes and technology that support each registry are also unique, and have not been designed to facilitate interlinkage between the systems. For example, data standards relating to identification differ for each registry.

At present, biographical data relating to just over half of Sierra Leone’s population of 6.09 million people has been captured in the foundational system, with a rate of approximately 400,000 new registrations being completed each year. Biometric data is captured as part of the National ID card registration process (6 fingerprints), as well as for Social Security (6 fingerprints) and voting registration (10 fingerprints), but is not captured as part of the foundational registry. Currently, there is no process for information from the various functional registries to be integrated into a central data repository. However, there are plans to establish an Integrated National Civil Registration System (INCRS) which would act as the central foundation registry for the country, be managed by the National Registration Secretariat, and be constituted by integrating data from the two principal functional registries: the NEC voter registry and the NASSIT social security registry.

The Government of Sierra Leone has articulated a clear intention to consolidate its registry systems, which will require funding, infrastructure, and a strong governance model.

112 (World Bank, 2014)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth/Death (MOHS)</td>
<td>Foundational</td>
<td>51% of population [3,060,000] 78% of children</td>
<td>Birth details on paper</td>
<td>Paper birth / death certificates</td>
<td>Not integrated, currently paper based</td>
</tr>
<tr>
<td>National ID</td>
<td>Foundational</td>
<td>5% of population [300,000]</td>
<td>6 fingerprints</td>
<td>National ID Card</td>
<td>Not integrated, planned to serve as central foundational registry in future (INCRS)</td>
</tr>
<tr>
<td>Passports (MOIA)</td>
<td>Functional</td>
<td>5.8% of population [300,000]</td>
<td>Date of birth (electronic), Travel details</td>
<td>ECOWAS-compliant and machine-readable travel document (not ePassport)</td>
<td>Data captured electronically. No integration as yet.</td>
</tr>
<tr>
<td>Social Security (NASSIT)</td>
<td>Functional</td>
<td>16.7% of population [1,00,000]</td>
<td>Date of birth, 6 fingerprints (3 per hand), 2 irises, 1 digital photograph, Social security #, Accurate names</td>
<td>Social Security Card</td>
<td>AFIS used to prevent duplicate enrolment, photograph used for manual verification. Iris currently not used. No integration as yet.</td>
</tr>
<tr>
<td>Voting (NEC)</td>
<td>Functional</td>
<td>45% of population [2,700,000]</td>
<td>Date of birth, 10 fingerprints</td>
<td>Voter ID Card</td>
<td>De-duplication completed on the basis of biometric data. No integration as yet.</td>
</tr>
</tbody>
</table>
LEGAL FRAMEWORK

Sierra Leone currently has legal instruments that provide for the compulsory registration of all citizens and residents, as well as the right of those individuals to access government information. With respect to data protection and privacy, aside from the protections enshrined in the Constitution and despite the intentions captured as part of an ECOWAS supplementary act (to which Sierra Leone was a signatory in 2010), there is still no comprehensive national data protection law, nor has an independent data protection authority been established as yet. Additionally, the need has been called out for a law to establish digital identity as a legally valid form of identification, as well as an information and communication technology (ICT) Act to support privacy and data protection related to electronic data\(^\text{113}\).

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to Access Information Act</td>
<td>2013</td>
<td>Provides for the disclosure of information held by public authorities or by persons providing services for them(^a). Establishes a right to access government information, and requires the government to create, adopt and socialise a plan for making records publicly available. Also includes penalties for non-compliance(^b).</td>
</tr>
<tr>
<td>Constitution of Sierra Leone</td>
<td>1991</td>
<td>Establishes the right to privacy of person, property and communications, with access to these being subject to the consent of the individual.</td>
</tr>
<tr>
<td>Supplementary Act A/SA on Personal Data Protection within ECOWAS(^c)</td>
<td>2010</td>
<td>The Heads of State of ECOWAS (including President Koroma of Sierra Leone) signed the Supplementary Act, which captured the intent for the establishment of a legal framework for personal data protection and privacy (applying to data collection, processing, transmission, storage and use) and an independent data protection authority, in each ECOWAS member state.</td>
</tr>
<tr>
<td>National Registration Act</td>
<td>2008</td>
<td>Provides for the compulsory registration of all citizens and residents in Sierra Leone, and the issuance of identity cards to those registered.</td>
</tr>
<tr>
<td>Birth and Death Act No. 11</td>
<td>1983</td>
<td>Stipulates the procedures and requirements around birth and death registration</td>
</tr>
</tbody>
</table>

\(^{113}\) (World Bank, 2014)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunications (Amendment) Act</td>
<td>2009</td>
<td>Telecommunications Act 2006 established the National Telecommunications Commission (NATCOM)(^4). The Amendment in 2009 added to the functions of NATCOM and tasked the Commission with ensuring that service providers complied with best practices (including data protection)(^6).</td>
</tr>
</tbody>
</table>

\(^a\) (Sierra Leone: New Law Promotes Transparency, 2013)
\(^b\) (Supplementary Act A/SA on Personal Data Protection within ECOWAS, 2010)
\(^c\) (Kargbo, 2011)
\(^d\) (SierraLii, 2009)
\(^e\) (World Bank, 2014)

**INSTITUTIONAL STRUCTURES**\(^{114}\)

**National Registration Secretariat (NRS)** is currently a semi-autonomous division within the Ministry of Internal Affairs (MOIA) that was established to conduct mandatory registration and issue national identity cards. Future plans for the NRS involve establishing it as the autonomous central authority for digital identification, reporting to the President’s office and governed by a Board constituted by stakeholder representatives. NRS would work with agencies such as the NEC and NASSIT to establish and maintain a central digital identity registry, issue birth/death/marriage/adoption certifications, issue ID credentials and provide identity services to other public and private entities.

**National Election Commission (NEC)** is responsible for voter registration and organizing elections. In 2012, the NEC conducted a registration drive that resulted in the capture of identification information (including biometrics) of 2.7 million people.

**National Social Security Insurance and Trust (NASSIT)**, within the Ministry of Labor and Social Security (MLSS), is responsible for issuing social security numbers to working individuals (who contribute to the scheme during employment) and beneficiaries (who receive benefits upon retirement).

**Birth & Death Bureau**, within the Ministry of Health and Sanitation (MOHS), manages birth and death registrations in Sierra Leone.

---

\(^{114}\) (World Bank, 2014)
**Immigration and Passports**, within the MOIA, is responsible for issuing passports in Sierra Leone.

**IDENTIFICATION PROCESSES**

**Birth registration**

The birth registration process is free of charge, entirely paper-based, and is conducted in a decentralized manner across 14 districts around the nation. Registration is completed at Peripheral Health Units (PHU), which are district health management clinics. Every four years, the records at the PHUs are collected and archived centrally at the Birth and Death Bureau. Doubts have been raised by several other agencies with regards to the reliability of the birth certificates, given the manual paper-based nature of the process. However, it is recognized that a lot of valuable data resides in these registries that would require conversion into digital form to support the proposed INCRS.

**Passports**

Passport issuance can be quite a costly and lengthy process, involving vetting and investigation that can take anywhere between ten minutes and one week. Biometric data is not collected as part of the process – a birth certificate must be used as proof of identification. In light of the concerns around reliability of birth registration data (as it is a manual and paper-based process), using birth certificates as a basis for issuing passports then also calls into question the reliability of the resulting passports.

MOIA captures data on passports electronically, meaning that the passport registry is already in the form of a digital database that can be queried.

**CURRENT CHALLENGES**

Below are some of the challenges currently facing the system:

- Little or no coverage of some remote populated areas
- Data capture process is paper-based, not electronic
- Date of birth data is verified against paper-based birth certificates
- Captured data undergoes minimal checks for accuracy

115 (World Bank, 2014)  
116 (World Bank, 2014)
- Lack of central data repository or master data management for identification data (i.e. few de-duplication processes in place at point of entry; lack of uniform standards-based approach)
- No data maintenance processes – i.e. former records are not retrospectively digitized, and current database at risk of going obsolete without plan for regular updates
- A primary ID has not yet been identified to enable multiple functional registries to be linked to the foundational registry using a primary key
- Incomplete ID documentation and gaps/inconsistencies in identification data often cause delays in the provision of important functional services such as social security
- Biometric data is captured for primary social security members only, and not dependents or proxies

A critical success factor in Sierra Leone’s next steps will be digitizing the birth/death registry and verifying the data, as the information contained in the paper certificates (e.g. DOB) is currently used as a basis when including an individual into the other functional registries.
MATURITY ASSESSMENT

Categorization: Greenfield

REGISTRY ASSESSMENT

Liberia has no foundational identity program as yet (although it is planned), and has five main functional identity programs run by different agencies that use various standards and processes. The functional programs provide useful services though are specific to the individual needs of each government agency. At present, there exists a civil registry for births and deaths, a passport program, a HR/payroll system for civil service, a social security program, and a driver’s license system. Interoperability across these programs is not facilitated as yet.

LEGAL FRAMEWORK

Through its recent National Identity Registration (NIR) law, Liberia has provided for a digital identification system, a governing entity to administer and maintain it, and refers to existing privacy protections in the Liberian Constitution as well as recently enacted Freedom of Information laws. Although the law is explicit about the need to control access to biometric information which is collected or used for identification purposes, there is no dedicated legal instrument yet that protects personal data nor right to privacy. The NIR law also currently does not define digital identity as a legally recognized category, though it defines biometric identity as a digital construct of identity. The law is silent on how the digital identity is to be used or asserted, i.e. through online identity services or smartcards. The legal framework around electronic communications is yet to be developed to protect against

117 (World Bank, 2014)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Level of Integration</th>
<th>Output</th>
<th>Data Captured</th>
<th>Usage</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>Foundational</td>
<td>Ministry of Health and Social Welfare maintain electronic database. Not integrated with other agencies.</td>
<td>N/A</td>
<td>Paper-based certificates, data entered into electronic database at later stage</td>
<td>4% Births</td>
</tr>
<tr>
<td>National ID Registry (NIR) – PLANNED</td>
<td>Foundational</td>
<td>Ministry of Foreign Affairs maintains electronic database; deduplication is conducted on basis of biometric data; database not integrated with other agencies</td>
<td>No official identity card is issued yet, and no digital record yet. Both are planned.</td>
<td>10.6% of population (approx. 455,164)</td>
<td>Functional</td>
</tr>
<tr>
<td>Passports</td>
<td>Functional</td>
<td>Ministry of Foreign Affairs maintains electronic database; deduplication is conducted on basis of biometric data; database not integrated with other agencies</td>
<td>Biometric passport</td>
<td>130,000</td>
<td>Functional</td>
</tr>
<tr>
<td>Civil Service Registry</td>
<td>Functional</td>
<td>Civil Service Agency maintains electronic database, used as reference for government services and payroll functions. Not integrated with other agencies</td>
<td>Digital record</td>
<td>150,000</td>
<td>Functional</td>
</tr>
<tr>
<td>Registry/ID</td>
<td>National Social Security and Welfare Corporation (NASSCORP) registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Functional</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Captured</td>
<td>Active contributors: 118,484, Beneficiaries: approx. 7,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active contributors: Bio-graphics only (no biometric data collected)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Beneficiaries: biographics, bank account and biometric data collected (6 fingerprints)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage</td>
<td>14,270</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>Social Security card with photograph and Social Security number; electronic record</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Card with drivers license number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level of Integration</td>
<td>Pays benefits directly into bank accounts of beneficiaries. Electronic database not integrated with other agencies, no deduction processes. NASSCORP prints Civil Service Agency list and manually visually against it on a periodic basis.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No steps taken to vet identity, therefore used more as a permit to drive a vehicle rather than proof of identity.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a (World Bank, 2014)
<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constitution</td>
<td>1986</td>
<td>Protects against ‘Arbitrary Interference with Privacy, Family, Home, or Correspondence’&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Freedom of Information Act&lt;sup&gt;b&lt;/sup&gt;</td>
<td>2010</td>
<td>Provides all persons the right of access to public information</td>
</tr>
<tr>
<td>National Identification Registry Act</td>
<td>2011</td>
<td>Provides for digital identification, and calls for the setup of a National Identification Registry (NIR) to be responsible for issuing a biometric-based identification card to each citizen and resident. The law recognizes that a reliable and effective system for identifying people in Liberia is essential for rule of law and for social planning, including the efficient delivery of services. The new law repeals PRC Decree #65, which was passed in 1981 and represented the first national effort to implement a national identification system in Liberia. The NIR Act of 2011 also calls to ensure that the collection and issuance of data about people are done in conformity with the freedom of information laws of Liberia and do not infringe upon the rights to privacy guaranteed by the country's constitution.</td>
</tr>
</tbody>
</table>

<sup>a</sup> (United States Department of State, 2011)  
<sup>b</sup> (Freedom of Information Act, 2010)

### Institutional Structures<sup>118</sup>

**Board of Registrars (BOR),** headed by the Minister of Internal Affairs, has been set up as a governing body and has convened multiple times to define the strategic and operational priorities of the NIR. The BOR consists of the following members:

- Minister of Internal Affairs (Chair of the Board)
- Director General of Liberia Institute of Statistics & Geo-Information Services (LISGIS)
- Minister of Health and Social Welfare
- Minister of Justice
- Director General of National Social Security & Welfare Corporation (NASS-CORP)

---

<sup>118</sup> (World Bank, 2014)
**National Identification Registry (NIR)** is planned to serve as an autonomous entity within the executive branch of the government, and would be empowered to operate as a legal entity with the full rights to transact. NIR’s functions are stipulated to be:

- Establish, maintain, administer, and implement the National Biometric Identification System of Liberia
- Design, implement and provision for the technology infrastructure and related processes
- Collect, organize, store, secure, and manage access to data, including biometric data
- Establish the adequacy of information provided by applicants for biometric identification cards per the law
- Issue a biometric citizen identification card to citizens and residents
- Issue a social security number (SSN), as part of the biometric citizen identification card, to serve as a unique identifier and the primary government-approved identity number

According to the NIR Act of 2011, the NIR is to be financed by legislative appropriations made through the national budget, without precluding the NIR from seeking and accepting assistance, donations, and/or grants from other person or institutions. Currently, no budget is allocated for the setup of NIR.

The Ministry of Health and Social Welfare (MOHSW) operates a civil register to record births and deaths in Liberia.

Since 2007, the Bureau of Passports and Visas at the Ministry of Foreign Affairs (MOFA), has been using biometrics to issue passports to citizens in Liberia. Since 2009, the Civil Service Agency (CSA) has been operating a biometric-based electronic register to improve human resource management within government.

**IDENTIFICATION PROCESSES**

**Birth registration**

Since 2011, the civil register has been partly decentralized to improve the efficacy of information collected at birth. Prior to 2011, birth registration had to be conducted at the office of MOHSW in Monrovia. Since people in rural areas had

---

119 (World Bank, 2014)
difficulty traveling to Monrovia, birth registration was low. Starting in 2011, the GOL has established 14 birth registration centers (as registrars) in different counties of Liberia and maintains a central registrar at the MOHSW office in Monrovia.

- At the time of birth (irrespective of whether the birth takes place in a community or at a county health clinic), a birth notification form is filled out in triplicates. Parents keep one copy of the birth notification form, and the other two copies are sent to the district registrar officer.
- The district registrar records the birth, transmits the information to the electronic database at MOHSW, and issues a birth certificate to the facility where the child was born.
- A parent can claim the birth certificate by presenting a copy of the birth notification form.

MOHSW has spent considerable effort to create awareness for the need of early birth registration. It has developed midwife birth facilities at the county health clinics, and is offering birth registration for free:

<table>
<thead>
<tr>
<th>Age</th>
<th>Cost of Registration</th>
<th>Location of Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 12 years</td>
<td>LRD 0</td>
<td>County Registrar or Central Registrar</td>
</tr>
<tr>
<td>Adults</td>
<td>LRD 500 (equivalent US $5.60)</td>
<td>Central Registrar</td>
</tr>
</tbody>
</table>

Source: Liberia MOHSW (2014)

**Passport**

- Ten fingerprints are collected using scanners at any of the 5 Ministry of Foreign Affairs (MOFA) enrolment stations in Liberia or in the 2 states outside of Liberia.
- Fingerprints are sent to an Automated Fingerprint Identification System (AFIS) within MOFA.
- At AFIS, the fingerprints are checked against an electronic database of people to whom MOFA has previously issued passports. If a match is found, the request for passport is seen as a duplicate and a possible fraudulent attempt. Otherwise, MOFA reviews issuing a passport, based on the validity of additional information provided. Deduplication occurs.
- Waiting time for the passport is 7 days.

---

120 (World Bank, 2014)
Future: National biometric ID Card (not implemented)

Residents will be entitled to obtain a biometric national identification card if they submit following information:

(a) a birth certificate; (b) fingerprints; (c) photograph; (d) proof of citizenship of parents; (e) date of birth; (f) place of birth; (g) gender; (h) color of skin, hair, and eyes; and (i) any other information deemed necessary to verify citizenship. Based on the information provided, a citizen would be issued a biometric citizen identification card bearing a SSN, and a resident would be issued a biometric resident identification card.

CURRENT CHALLENGES\textsuperscript{121}

- Multiplicity of systems: five functional digital identity programs are being operated under different government agencies in Liberia, with interoperability not facilitated as yet. A person can hold several identity artefacts
- Duplication of information in registries and the presence of false records (e.g. ghost civil service workers)
- No primary identification credential in place
- Voter re-registration must be completed for each election cycle without the ability to leverage a central foundational ID registry
- Legal framework around data protection, privacy and electronic data transmission is underdeveloped
- Currently no funding or business model planned or set up for the NIR
- Passport fraud attempts occur on a daily basis, yet the penalty is not enforced

\textsuperscript{121} (World Bank, 2014)
Maturity Assessment

Categorization: Greenfield

Registry Assessment

High poverty and inequality between rich and poor are hurdles for Djibouti in developing an integrated identification system. However, it has started a digital ID program in an effort to identify the poor, known as the Carte d’Identité Nationale, Numerique (Digital National Identity Card). Djibouti also started its “Social Registry” program in 2012, which has the ability to contribute to the development of a national registry in the future.

The Social Register program targets poor households in Djibouti. Its goal is to identify and register households considered to be poor or vulnerable and subsequently provide assistance to households in need. The registration process is twofold – first, individual people are registered in the Identity Registration System (IRS) and issued unique identification numbers, and secondly, individuals are grouped into households for the Social Register (SR). Individuals must be invited to join the program in order to visit community offices and enroll. Both biographic and biometric data is collected for the IRS. A Proxy Means Test (PMT) generates a household poverty score to be stored in SR database – households below a certain score receive assistance.

Hosting over 23,000 refugees, Djibouti faces an additional registration problem with the high number of refugees who reside in camps inside its borders. The UN refugee agency launched a program in 2009 to assist Djibouti register its refugee population and issue ID cards. The cards give refugees security and access to basic services. However, the UNHCR announced in 2015 that it will not be able to assist in joint registration of refugees unless sufficient resources are provided by Djibouti.

122 (Kayad, 2015)
123 (World Bank, 2015)
124 (UNHCR)
125 (UNHCR, 2009)
126 (UNHCR)
<table>
<thead>
<tr>
<th>Registry/ID</th>
<th>Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>Foundational</td>
<td>92% Births&lt;sup&gt;a&lt;/sup&gt; [total number] N/A deaths</td>
<td>N/A</td>
<td>N/A</td>
<td>Not integrated with other systems</td>
</tr>
<tr>
<td>Carte d'Identification Nationale</td>
<td>Foundational</td>
<td>N/A</td>
<td>Biometric data (10 prints and face for adults, only face for children), biographic data, invitation to program validated&lt;sup&gt;b&lt;/sup&gt;</td>
<td>Electronic record created, paper receipt with reference numbers from enrolment, Unique Identity Number (UIN) generated, Smart Card</td>
<td>Linked with Social Register. Electronically validated</td>
</tr>
<tr>
<td>Social Register (SR) for households</td>
<td>Functional</td>
<td>N/A</td>
<td>Socioeconomic and identity declarations. If they exist, UINs of household members</td>
<td>Proxy Means Test (PMT) generates household poverty score to be stored in SR database</td>
<td>Linked to IRS –individual UINs from the IRS are rolled up and assigned to each household. The data stored in the SR will eventually be integrated into a national ID program.&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td>Refugee Registration</td>
<td>Functional</td>
<td>N/A</td>
<td>N/A</td>
<td>Physical ID card&lt;sup&gt;e&lt;/sup&gt;</td>
<td>Not linked</td>
</tr>
<tr>
<td>Voting</td>
<td>Functional</td>
<td>27% [177,000]&lt;sup&gt;f&lt;/sup&gt;</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<sup>a</sup> (UNICEF, 2013)  
<sup>b</sup> (World Bank, 2015)  
<sup>c</sup> (World Bank, 2015)  
<sup>d</sup> (World Bank, 2015)  
<sup>e</sup> (UNHCR, 2009)  
<sup>f</sup> (IDEA, 2015)
LEGAL FRAMEWORK

Freedom House gave Djibouti a press status of “Not Free” in 2014. The legal and media environment is very restrictive and many laws that would support a national identification system are not in place.\textsuperscript{127}

Djibouti does not have any laws guaranteeing access to public information. It also does not have any data protection laws.\textsuperscript{128} The lack of a sufficient legal framework and legal protection will be a barrier that will need to be overcome with the implementation of a national ID system.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right of Access to Information</td>
<td>N/A</td>
<td>Does not exist in Djibouti (though it exists in 10 other countries in Africa), and has led to numerous conflicts and human rights violations.\textsuperscript{a}</td>
</tr>
<tr>
<td>Data Protection and Privacy</td>
<td>N/A</td>
<td>Djibouti has no data protection laws\textsuperscript{b}</td>
</tr>
<tr>
<td>Freedom of Communication Law</td>
<td>1992</td>
<td>Provides for “criminal penalties for media offenses, including libel and distributing false information” It has led to the sentencing and imprisonment of journalists and has led to a practice of self-censorship\textsuperscript{c}</td>
</tr>
</tbody>
</table>

\textsuperscript{a} (UN Universal Periodic Review)  
\textsuperscript{b} (Kayad, 2015)  
\textsuperscript{c} (Freedom House, 2014)

INSTITUTIONAL STRUCTURES

The SESN (Secrétariat d’État de la Solidarité Nationale) is in charge of social protection in Djibouti and therefore in charge of the Social Register program. The SESN has 8 local enrollment centers with 2 stations per location, and one SESN Central Facility that houses the database and information systems. However, the program may be moved under the Population Directorate of the Ministry of Interior in the future.\textsuperscript{129}

\textsuperscript{127} (Freedom House, 2014)  
\textsuperscript{128} (Kayad, 2015)  
\textsuperscript{129} (World Bank, 2015)
IDENTIFICATION PROCESSES

Identity Registration System

To enroll individuals in the Identity Registration System, people are invited to visit an enrollment station at a community office. Biometric and biographic data is collected and de-duplicated using an Automated Biometric Identification System (ABIS).

Social Register

For the Social Register program, households can be registered at community offices or from a house-to-house social survey via Open Data Kit on an Android tablet. A door-to-door campaign is conducted to find target households and individuals, the electronic survey is conducted, then the information is uploaded into the SR Management Information System (MIS). If any updates are necessary, the community office accesses the data portal and changes are recorded in the web application. ¹³⁰

The data is aggregated and each household’s poverty status is determined based on surveys and socio-economic data. Households are assigned a poverty score and assessed against other factors to determine eligibility for the program. To determine household scores, each person in the household is assigned a UID. Then, each UID is linked to the proper household through data manipulation and management modules. The system configuration, including the ABIS for the IRS and MIS for the SR are thought to be transferrable to a new national ID system in the future. ¹³¹

Refugee Registration

Djibouti has experienced significant movement across its borders in recent years. Djiboutian people move away from the unfavorable conditions such as drought and instability, while refugees from other countries, mainly Somalia, seek asylum in Djibouti. The influx of refugees poses a new registration problem. UNHCR is taking active measures in Djibouti to screen and register its refugees, even issuing identity cards to adults.¹³² Identification helps refugees to access basic services in refugee camps, including being able to identify themselves in front of police to resist arrest

¹³⁰ (World Bank, 2015)
¹³¹ (World Bank, 2015)
¹³² (UNHCR, 2010)
CURRENT CHALLENGES

Djibouti has made headway with the Social Register, but still faces a number of challenges in developing a national ID system:

- Djibouti’s large poor population is a major barrier to identification, as it currently costs $11 to get an ID\textsuperscript{134}
- Names in Djibouti are very similar, leading to authentication and de-duplication challenges\textsuperscript{135}
- For house-to-house enrollment, there is oftentimes no internet in rural areas and data must be collected offline, leading to possible data loss\textsuperscript{136}
- Currently the Identity Registration System is only open to a subset of the population – individuals must be invited to go to enrollment centers and register\textsuperscript{137}
- Enrollment could be more accessible – there exist only 8 enrollment centers across all of Djibouti
- Djibouti has a large nomad population which nullifies house-to-house registration\textsuperscript{138}
- The Djibouti government still faces an ongoing problem with registering refugees – the UNHCR is largely spearheading the registration of the refugee population\textsuperscript{139}
- Djibouti does not have the foundational laws in place to implement a national ID system
- Djibouti does not have a law to guarantee access to public information which leads to numerous conflicts with the media\textsuperscript{140}
- There are no data protection or privacy laws\textsuperscript{141}

\textsuperscript{133} (UNHCR, 2009)
\textsuperscript{134} (Kayad, 2015)
\textsuperscript{135} (Kayad, 2015)
\textsuperscript{136} (Kayad, 2015)
\textsuperscript{137} (World Bank, 2015)
\textsuperscript{138} (Kayad, 2015)
\textsuperscript{139} (UNHCR, 2010)
\textsuperscript{140} (UN Universal Periodic Review)
\textsuperscript{141} (UN Universal Periodic Review)
LAOS

MATURITY ASSESSMENT

Categorization: Greenfield

REGISTRY ASSESSMENT

Laos does not currently have accurate data on births, deaths, and vitals events because it does not possess a centralized electronic civil registration and vital statistics (CRVS) system, but announced at the Ministerial Conference on CRVS in 2013 that it will be taking urgent measures to register vital events. The Laos government is seeking assistance internally as well as development agencies like the World Bank to provide support in finalizing and executing on a strategic plan to implement a national civil registration system. The current registry assessment has been completed and a high-level strategic plan drafted – now Laos is looking for guidance to make the plan more detailed, effective, and actionable.

Other projects currently underway in Laos, such as the Lao PDR Health Governance and Nutrition Development Project, rely on a functioning birth registry and are therefore interested in the successful implementation of such a program. Additionally, The Family Management and Grass Roots Development Department of the MPS is in the midst of implementing an Electronic Identification Card (e-ID) program, which would also benefit from a functioning CRVS system. An ideal plan will effectively link the e-ID program with the new CRVS system.

Detailed aspects of the target CRVS system, such as what data will be captured or how the system will integrate with public and private services, have not yet been determined.142

142 (World Bank, 2015)
<table>
<thead>
<tr>
<th>Registry/ID Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System</td>
<td>75% of births registered(^a), but only 17% have birth certificates(^b) [4,857,000 registered, 1,101,000 certificates]</td>
<td>Basic birth details, cause of death</td>
<td>Paper Birth Certificate</td>
<td>Births and deaths recorded in ‘Family Book’ and in the MPS’s main record system; records are not integrated with other systems</td>
</tr>
<tr>
<td>National ID System</td>
<td>N/A (Future)</td>
<td>N/A</td>
<td>N/A</td>
<td>MPS is in the process of implementing an e-ID program to create national ID system</td>
</tr>
<tr>
<td>Passport</td>
<td>Very low, as most Laotians cannot afford to leave the country</td>
<td>Biographic data</td>
<td>Physical passport</td>
<td>Not integrated with other forms of identification.</td>
</tr>
<tr>
<td>Voting</td>
<td>88% of voting population(^c) [3,240,000]</td>
<td>N/A</td>
<td>N/A</td>
<td>Currently not linked with any other registries</td>
</tr>
</tbody>
</table>

\(^{a}\) (UNICEF, 2014)  
\(^{b}\) (World Bank, 2015)  
\(^{c}\) (IDEA)

**LEGAL FRAMEWORK\(^{143}\)**

It is still unknown if Laos has the necessary laws in place to implement a new civil registration system. The Laos Ministry of Justice has requested assistance from the World Bank in assessing whether its existing laws are adequate, by way of benchmarking Laos laws against other country’s data privacy laws.

Laos has three main laws pertaining to registration that are laid out in the table below. These laws establish citizen’s basic rights and requirements for registering vital events. The statistics law establishes standards for reporting such events.
Laos does not have any data protection or privacy laws in place, which is a potential inhibitor to implementing a highly integrated CRVS system.

If new laws are required, the Ministry responsible for enacting them has not yet been determined. The key activities of passing legislation and enforcing the subsequent laws falls under the jurisdiction of the Ministry of Justice (MOJ), Ministry of Home Affairs (MOHA) and Ministry of Public Security (MPS). If new laws and process are implemented, clear roles and responsibilities will have to be established for each of the stated Ministries to avoid duplication of work and ensure a smooth civil registration process.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family Law No 07/90/SPA</td>
<td>1990</td>
<td>The People's Supreme Assembly of Lao PDR passed this law on the subject of workers with family responsibilities. The law “provides equal rights for men and women under family law”(^a). Establishes stipulations of first name, last name, nationality as well as children’s rights. Other vital events such as marriage registration, divorce, adoption are also outlined.(^b)</td>
</tr>
<tr>
<td>Family Registration Law 03/SPA</td>
<td>1991</td>
<td>On the subject of regulating the registration of families, births, disappearances, deaths, marriage, divorces, adoptions, name changes, and other vital events. To register births and deaths, one must notify the village chief, who must then issue the proper certificate. All Laotian individuals have the right to a name and nationality under this law(^c)</td>
</tr>
<tr>
<td>Statistics Law No 03/NA</td>
<td>2010</td>
<td>Defines rules and regulations around handling statistical activities. Includes quality standards such as full coverage, accuracy, and consistency. All statistics must “contribute to the country’s development to achieve wealth, culture, well-being and equity”.(^d)</td>
</tr>
</tbody>
</table>

\(^a\) (International Labor Organization)
\(^b\) (Office of the Supreme People’s Prosecutor)
\(^c\) (Office of the Supreme People’s Prosecutor)
\(^d\) (Lao Statistics Law)
INSTITUTIONAL STRUCTURES

The Laos Ministry of Home Affairs (MOHA) is currently in charge of carrying out family registration centrally\textsuperscript{144}, while district heads are responsible for enforcing the law in individual districts. MOHA has been assigned the task of developing a civil registration system database in the near future. MOHA is currently in the process of writing a strategic plan outlining how the CRVS system will be implemented and specifying which digital architecture that will be necessary for successful execution, although the plan is very high-level right now.\textsuperscript{145}

Other governing bodies supporting the CRVS implementation are the Ministry of Health (MOH), Ministry of Justice (MOJ), Ministry of Public Security (MPS), Ministry of Planning and Investment, Ministry of Foreign Affairs, Vientiane Provincial Health Office, and Vientiane Provincial Hospital.\textsuperscript{146} MPS is responsible for issuing the family books and MOH is responsible for issuing birth notification.\textsuperscript{147} Other development agencies involved in the effort are WHO, UNICEF, Plan International and the Government of Korea.

The Ministry of Public Security registers births and deaths in the main record system and is also in charge of implementing Laos’ Electronic Identification card (e-ID).

In general, the roles and responsibilities of the ministries involved are not clearly delineated, which leads to duplicative efforts and coordination challenges. For example, MOHA was split off of the MPS in 2011 and work is often shared and not clearly separated. Determining which ministries are in charge of which activities will be necessary for a successful implementation and ongoing operation of integrated CRVS and e-ID systems.

IDENTIFICATION PROCESSES

Birth Registration\textsuperscript{148}

The Ministry of Public Security (MPS) is in charge of registering births in their district’s main record system. The registration process differs based on the child’s birth location. For institutional births, parents are given a notification form which

\textsuperscript{144} (UN Statistics)
\textsuperscript{145} (World Bank, 2015)
\textsuperscript{146} (World Bank, 2015)
\textsuperscript{147} (UNstats)
\textsuperscript{148} (World Bank, 2015)
they must then take to their Village Chief for recording in the ‘Village Family Book’. Parents will also record an institutional birth in their own ‘Family Book’. Both types of family books serve as legal instruments. For parents to obtain a birth certificate for a home birth, they must first visit a district MOHA office to obtain a birth certificate application. The application requires three witness’ signature and also must be sent to the Village Chief for recording in the ‘Village Family Book’ and for official certification. Once all of the signatures are obtained, the form is sent back to the MOHA office where the birth is registered in the main record system of the district and a birth certificate is issued. Birth information is captured in individual Family Books and data from various books is not aggregated in a central place.

**Death Registration**

The death registration process for institutional and non-institutional deaths is similar to the birth registration process outlined above. Deaths must be submitted to the Village Chief in order for a death certificate to be issued. Cause of death is a field on the death certificate, though the field is often inaccurate and non-standardized. Laos is currently implementing a system to record cause of death in institutions using standard language and coding, in an effort to increase coverage and registration of medically-certified deaths.

All in all, the registration process is not well understood and also fairly inaccessible to the population. Higher registration rates are associated with higher income, urban villages, and 80% or more of the Laotian population lives in poor, rural areas. Laos’ small population, underdeveloped modes of transportation, the inaccessibility of registration services, and lack of understanding of its necessity leads to very low registration rates, some of the lowest in Southeast Asia.

**CURRENT CHALLENGES**

Laos faces a large number of challenges in implementing comprehensive identification programs. Existing registries have low utilization, are inaccurate, or do not exist. In order to move forward with registering vital events, Laos will have to confront the current challenges it faces with the system. These challenges include the following:

- Laos does not have a clear plan for moving forward to implement a new CRVS system – the strategic plan drafted by MOHA is not comprehensive or sub-

149 (World Health Organization)
150 (International Labor Organization)
151 (UN Statistics)
stantial enough to begin executing

- The digital architecture and system requirements for a new CRVS database has not been determined
- Ministries are not clear on roles and responsibilities, with unclear ownership and occasional duplication of efforts. The lack of organization only be exasperated by the rollout of a new program\textsuperscript{152}
- The overall registration process is not well understood by the population\textsuperscript{153}
- Lack of clear procedures for birth registrations
- Vital event registration is not very accessible. Registration is often restrained to urban centers, while 80\% of Laos’ population lives in rural areas and modes of transportation / roads are not reliable.
- Death registration is low and has historically not been well documented\textsuperscript{154}. Cause of death is often inaccurate and non-standardized, which yields inexact mortality statistics and makes diseases and other health concerns hard to track
- It is unclear if Laos’ existing laws pertaining to registration and citizen’s access to information are adequate, or if they need to be amended in the context of a new electronic CRVS system
- No data protection laws are currently in place to protect citizen’s private data

\textsuperscript{152} (World Bank, 2015)
\textsuperscript{153} (UN Statistics)
\textsuperscript{154} (World Health Organization)
India has established a comprehensive identification system, with two foundational systems as its backbone: the National Population Register (NPR) and the National ID system (i.e., Aadhaar). It has linked the Aadhaar foundational registry with a variety of social and financial applications via the UID Architecture (shown in Figure 19: India’s UID Architecture). The data contained in the NPR is meant to be a registry of residents that includes biographic data, biometric data, and the UID Number once de-duplicated against the UID system. Meanwhile, the Unique ID (UID) Number (or 12-digit Aadhaar number) is the primary form of identification used to authenticate to services from food subsidies to rural employment schemes. The NPR is considering the issuance of a Resident Identity Card, a smart card containing the UID number for those over 18 years of age.
<table>
<thead>
<tr>
<th>Registry/ID Type</th>
<th>Usage</th>
<th>Data Captured</th>
<th>Output</th>
<th>Level of Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil Registration and Vital Statistics System (National Population Register)</td>
<td>Foundational</td>
<td>Name, relationship to head of household, parents names, spouse’s name, sex, DOB, marital status, place of birth, nationality, present address &amp; duration of stay, permanent address, occupation, education. Biometrics: photo, 10 fingerprints, 2 irises.</td>
<td>Resident Identity Card (currently only to some groups)</td>
<td>Connected to UID System – allows biographic/biometric data to be de-duplicated and individual is issued a Unique ID Number.</td>
</tr>
<tr>
<td>National ID System</td>
<td>Foundational</td>
<td>Name, DOB, gender, address, children: father/mother’s name and UID number, Introducer’s name and UID number (those lacking documents). Biometrics: 10 fingerprints, 2 irises.</td>
<td>Unique ID Number</td>
<td>Linked to Population Register using UID Number as reference. Primary number which facilitates secure authentication for distribution of public and private benefits/services.</td>
</tr>
<tr>
<td>ePassport</td>
<td>Functional</td>
<td>Biographic data, photograph, fingerprints</td>
<td>Biometric passport (physical)</td>
<td>Not currently linked to National ID System</td>
</tr>
<tr>
<td>Voting</td>
<td>Functional</td>
<td>Address proof, age proof, photo identity proof/document, filled/signed voter registration form.</td>
<td>Electoral Photo ID Card (EPIC)</td>
<td>Not currently linked to National ID System</td>
</tr>
<tr>
<td>a (UNICEF, 2013)</td>
<td>d (ePractice EU, 2015)</td>
<td>g (PressTrust of India)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b (UN Statistics Division, 2013)</td>
<td>e (e-Estonia, 2012)</td>
<td>h (IDEA, 2015)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The uptake of the foundational system in a matter of 5 years is substantial (69% coverage in UID, or 863M enrolled), making it the largest biometric system in the world. The level of integration with other public and private e-services is currently limited, and expected to increase as the UID platform is an open API allowing any agency to build an application to integrate with the identity system.

**LEGAL FRAMEWORK**

India’s data protection laws were recently established (2008) and are just the first step in establishing a robust legal framework for data privacy.

UIDAI is operating under an executive order issued on January 28, 2009 given the National Identification Authority of India (NIAI) has not yet passed. There has been a turf war between India’s UID and NPR programs due to the lack of clear jurisdiction for these initiatives.

<table>
<thead>
<tr>
<th>Legal/Policy Instrument</th>
<th>Year</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citizenship Act 1955 and the Citizenship (Registration of Citizens and issue of National Identity Cards) Rules, 2003</td>
<td>2003</td>
<td>The Act provides for the provisions that every usual resident in India to register in the National Population Register.</td>
</tr>
<tr>
<td>Registration of Births and Deaths Act</td>
<td>1969</td>
<td>The Act provides for the registry of every birth/stillbirth and death with the concerned state government within 21 days of its occurrence.</td>
</tr>
<tr>
<td>Rules under s43A (2008 Amendment), Information Technology Act 2000</td>
<td>2008</td>
<td>The Rules made under the s43A of the IT Act provide a data protection scheme that requires companies to have in place a comprehensive information security program, providing protection of sensitive personal data and information of individuals.</td>
</tr>
<tr>
<td>National Identification Authority of India Bill</td>
<td>2010</td>
<td>This Bill, which is still pending, seeks to establish the National Identification Authority of India (NIAI) to issue Aadhaar numbers to the residents of India.</td>
</tr>
</tbody>
</table>

_INSTITUTIONAL STRUCTURES_

**Unique Identification Authority of India (UIDAI)**

UIDAI is a Cabinet Committee that was constituted on October 22, 2009 to oversee the objectives of the UID program. Headed by the Prime Minister, it consists of
ministers from across the government to handle all functions relating to UIDAI including organization, planning, policies, funding, etc.

**Ministry of Home Affairs**

The Office of the Registrar General and Census Commissioner within the Ministry of Home Affairs is responsible for conducting the census every 10 years. This organization was also responsible for creating statistics on population statistics including Vital Statistics and Census. This is the same organization that also responsible for the registration of births and deaths.

**IDENTIFICATION PROCESSES**

**Birth Registration**

The child’s birth is registered with the concerned local authorities (and varies by state) within 21 days of its occurrence by filling out the form required by the Registrar. A birth certificate is then issue after verification with the actual records of the concerned hospital. If a birth is not registered within 21 days, a birth certificate is issued once police have verified the details.

**Update National Population Register**

Data is collected for the National Population Register in a two-phased approach):

**Phase 1: biographic collection:**

- via a Population Register employee that visits each household in the country and canvasses a questionnaire
- if citizen misses the initial visit, they are required to provide required information at designated NPR Centers

**Phase 2: biometric collection:**

- citizen goes to the local camps setup by Population Register employees to collect biometrics (fingerprints, face, irises)
- if citizen misses the camps, they are required to provide required information at designated NPR Centers

Once data is collected, the data is printed and displayed in the local area for

---

155 (Estonia, 2015)
review by the public at large and scrutinized by local officials. Local government officials deal with claims and objections by way of a grievance/redress mechanism. Once all claims have been dealt with and corrected, the local officials digitally sign the data which is then sent to the highly secure Central database for permanent storage. A mechanism to update data in the registry is not currently in place, but is being formulated. Resident Identity Cards are being issued to residents of coastal villages, and being considered for all residents over the age of 18.

UID Number

The resident goes to the local Registrar’s office to provide the following basic information (along with proof of identity and proof of address):

- Name
- DOB
- Gender
- Father’s/Husband’s/Guardian’s name and UID number (optional for adult residents)
- Mother’s/Wife’s/Guardian’s name and UID number (optional for adult residents)
- Introducer’s name and UID number (when resident lacks documentation)
- Address
- 10 fingerprints, photograph, and both iris scans

The Registrar sends the applicant’s data to the central ID repository for de-duplication. If the resident data is unique, a Unique ID (UID) Number will be generated and the number (printed on laminated paper) is mailed to the resident. Optionally, the resident can look up their UID Number using the enrollment number provided by the Registrar at the time of enrollment. This UID Number can then be used to assert identity and claim benefits/services at public and private institutions that have established themselves as authentication user agency.

CURRENT CHALLENGES

India has leapfrogged its previously weak identity infrastructure to a robust identity platform for authentication, but there are some challenges:

- The lack of a comprehensive legal framework continues to impact the UID

156 (Police and Border Guard Board, 2015)
program as legislation supporting UIDAI has not yet passed in Parliament, though enrollments continue. Governments should set national ID programs up in a way that works across all government agencies from a budgetary and legal authority standpoint. Also clarifying the role of enrollment agencies from that of authentication agencies, and having a legal framework for data sharing (to law enforcement or other organizations).

- There were conflicts between NPR and UID since both programs collect biometrics, but they are currently operating separately – NPR is considered relevant as a registry for national security, and UID for issuing a number that can be used to authenticate residents for benefits/services.

- The UID System enrolls children starting at the age of 5 (due to the instability of biometrics in children), and requires their biometrics to be updated every 5 years until the age of 18. Birth registrations are not captured in the UID System, but are vital events that must be logged properly in the National Population Register.

- Continued integration of India’s social programs to the UID system, including ePassports and the Voting system, will allow it to mature its identity ecosystem.
REFERENCES


Lepang, N. (2015, June 4). Interview with Botswana’s Director of Civil Registration.


Nyamulinda, P. (2015, June 3). Interview with Rwanda’s Director General of NIDA.


Population Register Act (May 31, 2000).


Supplementary Act A/SA on Personal Data Protection within ECOWAS (February 16, 2010).


UNstats. (n.d.). Retrieved from unstats.un.org/unsd/.../meetings/.../m01s03-03-LAO.pptx


