Toward More People-Centered Service Delivery: Opportunities for the National ID System in Lesotho
Table of Contents

Acronyms ............................................................................................................................ i

Acknowledgments ................................................................................................................ iii

Executive Summary ................................................................................................................ iv

1 Introduction .......................................................................................................................... 6

2 Lesotho’s National ID and Civil Registration System ....................................................... 8

3 Using the NID System for Identity Verification and Authentication .................................. 9

   3.1 Government of Lesotho Payroll .................................................................................. 10

   3.2 Old Age Pension Program ......................................................................................... 12

   3.3 Enhancing Customer Financial Due Diligence and Promoting Financial Inclusion .... 15

4 Additional NID Use Cases under Consideration .............................................................. 17

   4.1 Social Protection Programs ....................................................................................... 18

   4.2 Domestic Revenue Mobilization ............................................................................... 19

   4.3 Cross-border Services and Movement ...................................................................... 20

5 Harnessing the Potential of NIDs: Recommendations to Enhance Inclusion, Trust, and Linkages with Service Delivery ................................................................. 22

   5.1 Increasing Accessibility and Reaching the Last Mile ................................................... 23

   5.2 Updating the Legal and Policy Enabling Environment ............................................... 24

   5.3 Strengthening Business Processes for Identity Management ..................................... 25

   5.4 Strengthening Interoperability and Identity Verification and Authentication Services .... 26

6 Conclusion ............................................................................................................................ 28

7 References ........................................................................................................................... 30

8 ANNEX 1: Key Recommendations Arising from the 2019 Legal Enabling Environment Report .... 32

   Sharing ID Data ................................................................................................................ 32

   Use Cases/Legal Basis for Processing .............................................................................. 32

   Processing of Digital ID Data by Financial Institutions ................................................... 33

   Sensitive Personal Data .................................................................................................... 33

   Accuracy of Data ............................................................................................................... 33

   Cross-border Data Sharing .............................................................................................. 34

   Data Minimization ............................................................................................................ 34

   Accountability and Governance ....................................................................................... 34

   Cybersecurity and Cybercrime ......................................................................................... 34

   Data Flows ........................................................................................................................ 35

   .......
Non-discrimination and Inclusion ................................................................................................................. 35
Individual Privacy Rights ................................................................................................................................. 35

Boxes

Box 1: Digital IDs and the Digital Economy ................................................................................................. 19
Box 2: Toward Cross-border Interoperability in Africa ................................................................................. 21

Figures

Figure 1: NID as a Strategic Enabler for the NSDP II .................................................................................. 7
Figure 2: ID Interoperability in the Public Sector: Cost-Benefit Considerations ........................................ 15
Figure 3: ID Interoperability with the Financial Sector: Cost-Benefit Considerations .............................. 17
Figure 4: Pillars of the Digital Economy and Proposed Targets ................................................................. 20
# Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AfCFTA</td>
<td>African Continental Free Trade Area</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CBL</td>
<td>Central Bank of Lesotho</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>CFT</td>
<td>Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>CGP</td>
<td>Child Grant Payments</td>
</tr>
<tr>
<td>CR</td>
<td>Civil Registration</td>
</tr>
<tr>
<td>DA</td>
<td>District Administrator</td>
</tr>
<tr>
<td>DE4A</td>
<td>Digital Economy for Africa</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>EAC</td>
<td>East African Community</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Economic Community of West African States</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Electronic Identification, Authentication and Trust Services</td>
</tr>
<tr>
<td>ENBIC</td>
<td>ECOWAS National Biometric Identity Card</td>
</tr>
<tr>
<td>FIDO</td>
<td>Fast Identity Online</td>
</tr>
<tr>
<td>FNB</td>
<td>First National Bank</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>G2P</td>
<td>Government to Person</td>
</tr>
<tr>
<td>GDP</td>
<td>Gross Domestic Product</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GoL</td>
<td>Government of Lesotho</td>
</tr>
<tr>
<td>GSMA</td>
<td>Global System for Mobile Communications Association</td>
</tr>
<tr>
<td>HR</td>
<td>Human resources</td>
</tr>
<tr>
<td>HRMIS</td>
<td>Human Resource Information Management System</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technologies</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>ID4D</td>
<td>Identity for Development</td>
</tr>
<tr>
<td>IDN</td>
<td>ID Number</td>
</tr>
<tr>
<td>IFMIS</td>
<td>Integrated Financial Management Information System</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>KPA</td>
<td>Key Priority Area</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>LoA</td>
<td>Level of Assurance</td>
</tr>
<tr>
<td>LRA</td>
<td>Lesotho Revenue Authority</td>
</tr>
<tr>
<td>LSP</td>
<td>Lesotho Special Permit</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>MNOs</td>
<td>Mobile Network Operators</td>
</tr>
<tr>
<td>MoF</td>
<td>Ministry of Finance</td>
</tr>
<tr>
<td>MoHA</td>
<td>Ministry of Home Affairs</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>MOPS</td>
<td>Ministry of Public Service</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NICA</td>
<td>National Identity Cards Act</td>
</tr>
<tr>
<td>NICR</td>
<td>National Identity and Civil Registry</td>
</tr>
<tr>
<td>NID</td>
<td>National ID System</td>
</tr>
<tr>
<td>NIR</td>
<td>National Identity Register</td>
</tr>
<tr>
<td>NISSA</td>
<td>National Information System on Social Assistance</td>
</tr>
<tr>
<td>NSDP</td>
<td>National Strategic Development Plan</td>
</tr>
<tr>
<td>OAP</td>
<td>Old Age Pensions</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
</tr>
<tr>
<td>OVC</td>
<td>Orphans and Vulnerable Children</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PPP</td>
<td>Purchasing Power Parity</td>
</tr>
<tr>
<td>SADC</td>
<td>Southern African Development Community</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identification Module</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>UNSD</td>
<td>United Nations Statistics Division</td>
</tr>
<tr>
<td>VHW</td>
<td>Village Health Workers</td>
</tr>
<tr>
<td>VIP</td>
<td>Very Important Person</td>
</tr>
</tbody>
</table>
Acknowledgments

This note was developed by Rachel Ort (Public Sector Specialist, Task Team Leader), Kirstin Conti (Public Sector Specialist, Task Team Leader), Anna Metz (Program Analyst), and Valeria Mensah (Consultant), with inputs from and in collaboration with James Neumann (Senior Counsel), Jerome Buchler (Consultant), Victoria Monchuk (Senior Economist), Joachim Boko (Senior Social Protection Specialist), Michael Kidd (Consultant), Uzma Khalil (Senior Financial Sector Specialist), and Luda Bujoreanu (Senior Program Officer). The team wishes to thank the Lesotho Ministry of Home Affairs Department of National ID and Civil Registry (NICR) for its collaboration, engagement and inputs during the development of this note. We also wish to thank the Identification for Development (ID4D) Initiative for financing this work.
Executive Summary

During the past decade, Lesotho has made significant progress in implementing a national ID (NID) system and extending coverage to the country’s population. Managed by the Ministry of Home Affairs’ National Identity and Civil Registry (NICR) Department, Lesotho’s national ID covers an estimated 85 percent of the eligible population, that is, a little over 1 million people of a total population of 1.2 million. It is underpinned by modern identity management technologies. With close linkages between the NID and the civil registration (CR) system, Lesotho is on the path to providing its population with a trusted, unique, and verifiable identity from birth to death.

This note reviews the current and emerging use cases for the national ID system in the Kingdom of Lesotho. The NID system is currently being leveraged to improve the efficiency of the public sector payroll and Old Age Pensions (OAP) Program, and financial institutions and mobile network operators (MNOs) are piloting the use of the NID system to meet customer due diligence (CDD) requirements. Although still in the early stages, these initiatives demonstrate the significant potential of the NID system to generate fiscal savings, support digital service delivery, and expand financial inclusion. They also highlight a number of cross-cutting issues that must be addressed to ensure inclusion and long-term sustainability, promote trust and accountability, and fully realize the potential of the NID system as a platform for service delivery.

To improve the integrity of public sector human resource and payroll data, the Ministry of Public Service (MOPS) is utilizing the NID system to verify the existence, uniqueness, and biographical details of civil servants and civil pensioners on the payroll. Starting in June 2017, working with the NICR Department, the MOPS launched an effort to issue NIDs to civil servants and civil pensioners who did not already have one. In June 2018, the MOPS launched a biometric census of civil servants and civil pensioners. In order to be enumerated, individuals were required to present their national ID cards. As of July 2020, the MOPS is implementing a strategy to correct or remove anomalies identified during the census, including individuals who did not report for enumeration; human resource (HR) records associated with an invalid NID or deceased NID holder; and NID numbers associated with multiple HR records. In parallel, the Ministry of Public Service is collaborating with the NICR Department to reconfirm the existence, uniqueness and biographic data of all persons with HR records, including those staff onboarded after the census. Based on current progress, it is possible that the Government could save as much as $US5 million per year as a result of this cleaning exercise.

The NID system is also being used to verify the existence, uniqueness and eligibility of old age pension program beneficiaries. This has resulted in the stoppage of payments to 4,700 ineligible persons, representing a savings of up to US$2.8 million per year. Since 2017, the Ministry of Finance (MoF) Pensions Department has worked closely with the NICR Department to update the OAP beneficiary registry through demographic data-matching exercises. By January 2020, a ‘proof of life’ exercise had verified 63,000 pensioners using their NID. In addition, the enrollment of over 6,000 OAP beneficiaries without an NID was ongoing. An interface between the OAP Management Information System (MIS) and the NID system has been established to facilitate the timely removal of deceased pensioners from the payee list.

The e-Know Your Customer (KYC) pilot with the First National Bank (FNB), Vodacom Mpesa, and Econet highlights opportunities for leveraging the NID system for a more streamlined customer due diligence process. Real-time electronic identity verification could also provide significant cost savings for financial institutions and boost financial inclusion. The current identity verification processes to access financial services in Lesotho are cumbersome and offer limited assurance about customers’ identities. Financial
institutions note high transaction costs associated with regulatory compliance, and more than half of adults remain unbanked. The identity verification and authentication services offered by NICR to financial service providers could enable the latter to complete CDD processes and customer onboarding in a more rapid, efficient, and low-cost manner. Electronic identification and verification of customers may also help simplify the customer documentation requirements associated with opening a financial account.

**Additional use cases for the national ID system are already under discussion in Lesotho.** Improving linkages with the National Information System on Social Assistance (NISSA) may strengthen the integrity of beneficiary and payment management. Also, improving linkages with the tax administration could help to broaden the current tax base and promote better tax enforcement. In addition, cross-border interoperability between the NID system and select South African service providers could promote easier access to services for people on both sides of the border. The mutual recognition of IDs as travel documents could also contribute to trade, as well as the safe, orderly migration between Lesotho and South Africa — while also reducing the costs associated with cross-border travel.

**With a larger volume of data exchanged between the NID system and third parties, it will also be important to integrate privacy-by-design features into the NICR’s systems and business processes.** Additional safeguards need to be put in place to ensure that personal data collection, storage, and usage is secure, transparent, and limited to data that is absolutely necessary for carrying out the purpose for which the data is processed. For instance, as the NID number will increasingly be used as a common identifier across registries, tokenization could help limit risks to privacy. Measures that could also help to promote accountability include ensuring that all transactions involving identity data are logged in a tamper-proof manner, and providing individuals with more oversight and control over how their data is being used and shared.

**To maximize the benefits of identification for service delivery and development more broadly and to minimize risks, it will be important to systematically address cross-cutting challenges and remaining gaps.** Initial consultations point to certain priority areas and actions that will be critical to maintaining and building trust in the system, as well as to promoting its role as the foundation for effective service delivery, including:

- Addressing coverage gaps among vulnerable and hard-to-reach populations for the NID, and promoting timely and universal birth and death registration;
- Strengthening data capture, de-duplication, data updating, and exception-handling processes;
- Enhancing legal, policy, and technical safeguards to protect privacy and individual data;
- Establishing a comprehensive interoperability framework that defines the policies, processes, standards, as well as any fees for data sharing between the NICR and different entities; and
- Expanding identity verification and authentication options without compromising privacy or accessibility.

---

1 Tokenization substitutes a sensitive identifier (for example, a unique ID number) with a non-sensitive equivalent (that is, a “token”) that has no extrinsic or exploitable meaning or value. These tokens are used in place of identifiers to represent the user in a database or during transactions such as authentication. The mapping from the original data to a token uses methods— for example, randomization or a hashing algorithm—that render tokens infeasible to reverse without access to the tokenization system.
1 Introduction

This note documents the current and emerging use cases for the national ID (NID) system\(^2\) in the Kingdom of Lesotho. It demonstrates considerable potential and progress to date, and makes recommendations for moving toward a more inclusive, trusted and service delivery-oriented NID system. Global experience has shown that national ID systems can promote more efficient, transparent and people-centered service delivery in the public and private sectors, particularly when the system is designed with the appropriate enablers and safeguards in place to support improved development outcomes and mitigate risks. As countries move toward digital economies and governance, ID systems often serve as an essential digital platform, underpinning the digital payment infrastructure and transactions, as well as the provision of online and offline government services.

Foundational ID systems, such as a national ID system, can play a particularly important role in strengthening the efficiency and transparency of government. For example, a NID system can help to minimize leakages and opportunities for fraud in Government-to-Person (G2P) transfers, such as cash transfers, wages, and subsidies. It can also facilitate the expansion of digital payments, including through enabling more streamlined customer due diligence processes for opening financial accounts. High-assurance electronic identity verification and authentication mechanisms can promote easier bank account opening and enhance access to credit. An inclusive, trusted, and interoperable NID system can also contribute to strengthening human capital, one of the key priority areas of Lesotho’s National Strategic Development Plan (NSDP) II. Among other things, it can enable the effective identification of social protection program beneficiaries, facilitate better patient management in the health sector, and improve trust in key educational and professional qualifications and documents. In addition, trusted identity documents can facilitate safe and orderly migration, especially when such documents are recognized and verifiable across borders.

Recent experience with the COVID-19 pandemic also highlights the central role of ID systems in delivering services in response to a crisis. In countries with inclusive, trusted, and interoperable ID systems, authorities can identify those in need more easily and, importantly, can do so remotely. In addition, they can deliver emergency cash transfers more rapidly and securely, often through digital channels. When social distancing measures become necessary during a pandemic, governments can also use digital ID systems to shift their service delivery from physical offices to online options. Utilizing innovative, online identity verification and authentication solutions, countries can empower people to conduct most transactions online and work remotely, thereby reducing the need for physical movement — and reducing the risk of COVID-19 transmission. Ensuring continuous, remote access to services in key sectors during the current crisis and in the future will be critical to minimizing adverse impacts.

The Kingdom of Lesotho is a small, lower-middle income country that is facing several development challenges. Lesotho is a landlocked country with a population of 2 million, surrounded by South Africa. About 58 percent of the population live in rural communities, and an estimated 70 percent of households in rural communities depend on subsistence farming for their livelihoods. As of 2017, over one-quarter of the population lived below the international poverty line of US$ 1.90 (at purchasing power parity - PPP) a

\(^2\) In Lesotho, identity management is closely integrated with one system bringing together civil registration, (biometric) identification for persons age 16 and above, as well as passport data. All records are linked through a unique identifier. Throughout this note, the terms ‘national ID system’ or ‘NID System’ are used as a shorthand to describe this system and the population register that underpins it.
day. Half of the population lived below the national poverty line of 649 Maloti per month (about US$ 3.7 per day at PPP). Basotho migrant workers, living mainly in neighboring South Africa, are a vital contribution to livelihoods through their remittances. The Government of Lesotho (GoL) remains the main driver of economic activity, with public spending estimated at 60 percent of gross domestic product (GDP). This compares to the private sector, which accounts for just 14.6 percent of GDP.

Lesotho’s digital infrastructure has seen significant improvement over the past decade, but the adoption and use of technology are lagging. According to Global System for Mobile Communications (GSMA) data, 97 percent of the population was covered by a 3G (that is, third generation) network and 71.4 percent by a 4G network by 2018. However, internet use is low, with only an estimated 27.4 percent of the Basotho population using the internet regularly, according to International Telecommunication Union (ITU) statistics. Further, limited digital literacy hinders the adoption and use of digital products and services, restricting the growth potential for digital businesses. Overall mobile subscriptions in Lesotho stood at 106.6 per 100 inhabitants in 2017 (as compared to an average of 94 per 100 inhabitants in the Kingdom of eSwatini, 150 per 100 in Botswana, and 160 per 100 in South Africa). Despite progress in recent years, the level of financial inclusion remains relatively low, with 46 percent of the population in Lesotho above the age of 15 having an account with a financial institution (World Bank 2017a).

As discussed in Section 2, the NID system stands out as a trusted and well-functioning digital platform in Lesotho, with the potential to contribute to achieving several of the country’s national development objectives. Building on progress to date, Lesotho has an opportunity to leverage the country’s NID system to accelerate progress around multiple, key priority areas as articulated in the NSDP-II for 2019-2024 (Figure 1), which supports economic growth and improvement in individual welfare.

Figure 1: NID: Strategic Enabler for the NSDP II

Source: Author’s schematic, drawing on the Government of Lesotho National Strategic Development Plan.  
Note: ICT= information and communications technologies; KPA=key priority area

The remainder of this note is organized as follows. Section 2 provides an overview of the national ID system in Lesotho. Section 3 documents how the NID system is already being used to improve public
sector efficiency, streamline front-end services, and enhance financial inclusion. It reviews how the NID system is being leveraged for the payroll of the Government of Lesotho, the OAP, and electronic customer identification and verification in the financial sector. Section 3 further highlights additional use cases for the NID system already under discussion by stakeholders in Lesotho, such as social protection, tax administration, and cross-border verification services. Section 4 provides recommendations for the Government of Lesotho to build on progress to date and realize the potential of the NID System to promote more efficient, transparent and people-centered service delivery.

2 Lesotho’s National ID and Civil Registration System

The Government of Lesotho began implementation of its NID system in July 2013 under the aegis of the Department of National Identity and Civil Registry (NICR), within the Ministry of Home Affairs (MoHA). The NICR is responsible for a wide range of services and functions related to civil registration and identification, including the issuance of national IDs and passports, maintaining the population registry, and the registration of birth and deaths and the issuance of related certificates. The national identity register (NIR) is underpinned by a digital database and identity management system. Biometric data is collected to ensure that each person will only be enrolled once.

The administration of civil registration and identification is integrated under the NICR. The system brings together civil registration, identification, and passport data. Biometric data is collected for NID applicants, starting at the age of 16. Front-end processes for the civil registry and the NID system, as well as the back-end database, are closely linked. The birth certificate is required as part of the application for the NID, and the NID system draws on birth and death registration data to ensure that its records are consistent and up to date. The result is a population register that links children with their biometrically verified parents, and a unique lifetime ID number carried from birth to death. The unique ID number is also printed on the birth certificate, national ID card, passport and death certificate.

Lesotho’s national ID covers an estimated 85 percent of the eligible population (that is, a little over 1 million people of a total population of 1.2 million). Coverage gaps remain among people living in hard-to-reach rural areas and among marginalized and vulnerable groups who may be constrained in their mobility, be socially excluded, or lack the supporting documentation needed to obtain an ID. A 2017 nationally representative survey conducted by the World Bank found that 51 percent of Basotho without a NID found it “too difficult to apply” (World Bank 2019a). Lesotho nationals residing abroad are also believed to be among the population who have yet to enroll to obtain a national ID.

There are large gaps in the coverage and timeliness of civil registration. As of 2018, only 44.5 percent of children under the age of 5 have had their birth registered, and less than 60 percent of mothers or caretakers know how to register a birth. The Identity for Development (ID4D) Diagnostic Report (World Bank 2017b) notes that there is little demand for birth registration, as birth certificates and the associated unique ID numbers are not usually required for accessing services until a later age. Thus, birth certificates are seen as having limited value. Likewise, a comprehensive assessment of Lesotho’s civil registration and vital statistics system completed in 2019 indicates that the death registration rate is 38 percent.³

³ Government of Lesotho Ministry of Home Affairs data
There are 15 enrollment centers located across Maseru and each of Lesotho’s 10 districts that allow for birth registration and NID enrollment. All centers have internet connectivity and are linked to a central server in a dedicated data center. There are also about fifteen mobile registration units⁴, which are used to serve remote areas on a periodic basis. In order to minimize economic barriers in accessing the NID — and reinforce the role of identification as a national public good — the first ID card is provided free of charge. Nevertheless, the time and money required to reach registration centers presents a challenge for people in remote areas, as well as those with limited incomes and mobility.

The NID system leverages biometric technology to ensure the uniqueness of identities. Enrollment in the national ID system involves biometric data collection, whereby ten fingerprints and one portrait photo are captured. Enrollment can only be completed if no ID number has already been issued that is associated with the same biometrics. The biometric deduplication is exclusively based on fingerprints. The technology and algorithm used for fingerprint template generation and matching is believed to operate with a high level of accuracy. In case of a confirmed duplicate, the application for a new ID card is rejected. There is currently no manual adjudication process in place that would allow a human operator to examine inconclusive cases or to perform secondary checks. Introducing such a mechanism could help to strengthen the integrity and accuracy of the biometric deduplication process. A comprehensive assessment of operational, functional and system design is recommended to verify performance and alignment with international standards.

The NICR Department is seeking to provide automated identity verification and authentication services to government agencies (for example, pensions and payroll) and the private sector (for example, banks and mobile network operators). The software solution provider for the NICR system has developed an application programming interface (API) to facilitate the verification of the NID number, select demographic data, and fingerprints through an online web portal or via data exchange with digital platforms. Several public agencies, including the Ministry of Public Service (MOPS) and the Ministry of Finance (MoF), as well as financial institutions and the South African Department of Home Affairs have successfully tested connections to the NID system.

In parallel to testing the API, the Ministry of Home Affairs is looking to strengthen the legal and regulatory framework for data sharing and privacy. The Data Protection Act of 2011 is the prevailing law related to data privacy, and an amendment to the National Identity Act of 2011 is currently under development. An assessment of the legal and regulatory enabling environment was completed in 2019 with support from the World Bank. The assessment outlined recommendations for strengthening the existing legal framework. The Ministry has also developed a template Memorandum of Understanding (MOU) to be signed with agencies accessing identity data for verification purposes through the API.

3 Using the NID System for Identity Verification and Authentication

There is significant demand for digital identity verification and authentication from both the private and public sectors in Lesotho. Financial institutions are eager to leverage the NID system to fulfill Know-Your-Customer (KYC) requirements, and the MoF and the Central Bank of Lesotho (CBL) are exploring how the NID can help improve financial inclusion. For the public sector, the focus is on leveraging the NID system to streamline service delivery, improve the efficiency of public expenditures, and facilitate

---

⁴ The mobile registration units include a laptop and other equipment necessary to register an applicant. They are housed in a watertight suitcase for secure transport.
Government-to-Person (G2P) transfers (for example, salaries, civil pensions, old age pensions, and child grants). For the government’s fiscal year 2018/2019, the compensation for government employees and social protection programs constituted 41 percent and 13 percent of government expenditures, respectively. Thus, eliminating even modest leakages through improved identity verification and authentication could represent significant savings. It could also free up resources for additional investments in sectors vital to economic growth.

**Linkages with the NID system to facilitate identity verification and authentication for relying parties** have been piloted for several programs, with promising initial results. The three ongoing initiatives include the Government of Lesotho payroll, the OAP, and electronic identity verification for financial services. Although these initiatives are mostly in the early stages, they have already demonstrated the potential for significant savings, including reductions in transaction costs, as well as improvements in the end-user experience (see Figure 2). As of July 2020, the review of the payroll and OAP beneficiaries is still ongoing. As such, the savings from interoperability with the NID system presented in this section are only estimates and are subject to further validation. It is particularly difficult to estimate the lags in reporting or detecting deceased payees in the absence of a link with the NID system.

3.1 **Government of Lesotho Payroll**

The **Government of Lesotho currently spends about 16.8 percent of its GDP on public sector wages.** Among low-income countries, Lesotho’s wage bill as a share of GDP is one of the highest in the world. Yet, high expenditures on personnel have not translated into improvements in service delivery outcomes. One driver of the high wage bill is the absence of basic payroll controls and associated issues with the quality of human resource data. This leads to duplicate and fraudulent payments, and makes management of public sector staff more challenging.

To improve the integrity of human resource and payroll data, the **Ministry of Public Service launched a biometric census of civil servants and pensioners in June 2018.** The exercise covered all government services, with the exception of those in the Lesotho Defence Force (LDF) and the National Security Service (NSS), or roughly 93 percent of the fiscal year (FY) 2017/18 salary expenditures. The census leveraged the NID system to ensure all civil servants/pensioners are real, unique, living individuals. It also sought to verify relevant biographic data with the NICR (for example, birthdays). To prepare for the census, the Ministry of Public Service, working in collaboration with the Ministries of Finance, Education, Health and Home Affairs, launched a ‘rapid results initiative’ to record the NID numbers of all civil servants and civil pensioners on the payroll, as well as to issue NIDs to those who did not already have one. By January

---

5 A relying party is a service provider or other entity that depends on the NICR Department to verify the identity and/or authenticate an individual who is an existing or prospective user of its services or recipient of its transfers.

6 The scope of the census exercises was expanded to include Village Health Workers (VHW) in October 2018. This cadre of volunteer workers, some of whom receive pay from the government and development partners, was added to the census exercise at the request of the Ministry of Health. Given that there is no central registry for VHW, baseline data was compiled in consultation with District Health Teams and health centers. As in the main census exercise, the enumerators visited health centers throughout the country, and the VHW were required to present themselves with a NID (or passport) to be counted. A total of 8,694 were enumerated during the census. As the government moves to improve the management of this program, census records could be used as a baseline to improve deployment and payment, as well as to identify opportunities for performance management, capacity building, and other targeted incentive programs.

7 The estimate was calculated by subtracting the LDF and NSS share of salary payments from total compensation in the Kingdom of Lesotho FY20/21 Budget Estimates.
2018, the Ministry increased the number of filed payroll records with NID data from approximately 30 to 87 percent.

Using the April 2018 payroll data extracted from the Human Resource Information Management System (HRMIS) as a baseline, an enumeration firm visited all government duty stations in the country. Civil pensioners presented themselves for enumeration at their District Administrator’s (DA) Office. In order to be counted, civil servants and pensioners were required to present their National ID card, and they had their biometric data (fingerprints and photos) digitally captured. Individuals who missed enumeration at their duty station or DA Office were given another opportunity to present themselves at a central location in each district. In May 2019, the key findings were shared with line ministries, which were then given an opportunity to comment on anomalies identified during the exercise.

The biometric census of civil servants identified a number of anomalies. Nearly 12 percent of civil servants and pensioners did not report for enumeration during the census period. Yet, over 70 percent of these individuals still appeared on the payroll in August 2019. In addition, just over 2 percent of total records were associated with an invalid NID number. The NID numbers of 127 individuals enumerated during the census were associated with deceased records when checked against the NID system (<1 percent). In addition, 456 NID numbers were associated with two employed positions in the HRMIS after the census (<1 percent).  

The Ministry of Public Service is implementing a strategy to investigate and correct or remove anomalies. In December 2019, the Cabinet endorsed an action plan to address anomalies identified by the census. In January 2020, the Ministry of Public Service circulated the names of individuals not found during the census to Ministries and District Administrator Offices. These civil servants and pensioners were given a final opportunity to present themselves. The Ministry then initiated actions to suspend the salaries of those who could not be found by February 2020. To date, the government has found or suspended the pay for all individuals not found during the census. In parallel, the Ministry of Public Service is collaborating with the NICR Department to reconfirm the existence, uniqueness and biographic data of all HR records, including for staff onboarded after the census. This has resulted in the identification of further anomalies, including additional HR records associated with invalid or deceased NIDs.

While efforts to improve the integrity of HR/payroll data are still ongoing, an indication of the potential fiscal savings from the identification and correction of anomalies is feasible. Based on current progress, it is possible that the Government could save as much as US$470,00 per month (US$5.6 million per year, or 1 percent of total government expenditures). It is expected that some remaining exceptions will be corrected through investigation (for example, an employee or a pensioner later presents themselves in person by updating a record with a correct NID), and some through removal (for example, suspending payment to ‘ghost’ or deceased workers and pensioners). A more conservative estimate might anticipate that half of the remaining anomalies are resolved, and the other half are removed from the payroll, thereby resulting in a possible savings of closer to US$2.8 million a year.

---

8 Biometric authentication of identity through comparison of fingerprints between the biometric census and the NIR was possible for 94 percent of individuals enumerated during the census. The remaining 6 percent require further investigation.

9 As of July 31, 2020, the Ministry of Public Service reports that 2,073 individuals have yet to present themselves in person with a NID for enumeration, representing a value of approximately US$470,000 per month. Further savings from addressing invalid and duplicate NIDs are also expected.
The Ministry of Public Service is pursuing an interface between the HRMIS and the NID system to facilitate regular checks and keep the HR data accurate. In parallel to designing the biometric census of civil servants and pensioners, the Ministry of Public Service initiated efforts to establish a transactional interface between the HRMIS and the NID system. The technical specifications for an HRMIS API and a NIR API were developed and approved in 2017. The Ministry of Public Service financed the development of the NIR API through the World Bank-supported Public Sector Modernization Project (World Bank 2016). However, challenges with the HRMIS application stalled the development of the HRMIS API. After a business process review and a thorough assessment of the existing software solution, the Ministry of Public Service is currently undertaking the procurement and implementation of a new HRMIS software solution. The requirements for this system include an interface with the NIR, which is expected to be operational within the coming twelve months. Operationalizing the transactional interface holds the potential to sustain gains made through the one-time payroll clean-up, as well as simplify the enrollment processes for the civil service. The Ministry of Public Service has also issued a policy circular requiring the collection of the NID numbers for all newly hired public officers.

3.2 Old Age Pension Program

The OAP program is the largest social protection program in Lesotho, with expenditures of over 700 million Maloti (approximately US$40 million), which constitutes about 5 percent of the Government’s expenditures in FY 2018/19. The OAP provides cash grants to persons over the age of 70 who do not have access to any other form of pension. As of mid-2019, a total of 85,000 persons (3.7 percent of the population) were OAP recipients. With the relative economic and social importance of the OAP, ensuring the efficiency and integrity of the program are important objectives for the government.

The Ministry of Finance has taken significant steps toward cleaning the list of OAP beneficiaries. A demographic data-matching exercise was carried out between the OAP registry and the NID registry in September 2017, and again in March 2018. These matches found that almost two-thirds of OAP recipients had NID numbers. However, the exercise also uncovered a number of deceased and otherwise ineligible recipients. Building on this initial cleaning exercise, a web portal was established to allow the OAP (and other relying parties, such as the MOPS and financial institutions) to cross-check beneficiaries against the NID registry using demographic matching.

Overall, the initial cleaning and data-matching exercise, as well as the subsequent monthly checks, resulted in the stoppage of payments to 4,700 additional ineligible pensioners between July 2017 and April 2020 compared to the number of payments that would have otherwise ceased. Previously, the removal of the deceased beneficiaries had relied entirely on voluntary reporting by the deceased’s family members or the village chiefs — who had little incentive for doing so. Savings from the removal of the 4,700 ineligible pensioners during the last three years amounted to 4.5 million Maloti on a monthly basis11 (~US$230,000), which could translate into a savings of over 54 million Maloti (US$ 2.8 million) a year.

Between November 2019 and January 2020, a ‘proof of life’ verification exercise of pensioners was carried out to support the cleaning of the beneficiary roll and pave the way for closer linkages with the NID system. The verification exercise required pensioners to be physically present with their NIDs at the pay-point where they would usually receive their pensions. Through this exercise, 69,000 pensioners have

---

10 Demographic matching includes identifying likely matches by comparing names, dates of birth, gender, and other demographic characteristics recorded in two or more databases.

11 This assumes a 750 Maloti monthly payment.
been verified, of which 63,000 presented with their NIDs. A little over 6,000 pensioners remain to be enrolled.

**Pensioners without a NID will need to be provided with one as soon as possible to ensure that eligible individuals are not excluded from the program for lack of documentation.** Until May 2019, there had been no requirement for OAP beneficiaries to have NIDs for enrollment or receipt of payments. That month, a Regulation was issued by the Minister of Finance providing that “An eligible applicant shall provide an identity document as proof of birth.” (Government of Lesotho 2019b). The Pensions Department is interpreting that Regulation to require new OAP applicants to have a NID card as the sole acceptable proof of identity when collecting the OAP. In January 2020, the Ministry of Finance issued a Notice stipulating that effective as of April 1, 2020, a NID will be required for OAP enrollment and payments. The ‘proof of life’ exercise found that about 6,100 pensioners do not currently have a NID. The NICR has developed a plan to issue these beneficiaries with a NID, including the use of mobile registration. However, the enrollment was put on hold due to the restrictions imposed as a result of the COVID-19 pandemic.

**Interoperability and regular, automated data sharing between the OAP and the NID registry will be critical to keeping the OAP database up-to-date and ensuring fiscal efficiency.** The pool of OAP beneficiaries is naturally dynamic, owing to regular new entrants (by age) and exits (by mortality). This dynamism makes the seamless flow of information between the OAP registry and the population registry vital to ensuring the former’s integrity, as well as to maintaining fiscal efficiency.

**A new OAP Management Information System (MIS) is in the process of being implemented for pensions, which will rely on beneficiaries’ NID numbers to support liveness and uniqueness verification.** The new system is targeted for implementation in October 2020. It is designed to be interoperable with the NID system to perform regular, automated checks to ensure that OAP applicants and recipients are unique, real, living persons above the age of eligibility. The MIS will use the data collected during the ‘proof of life’ verification exercise of pensioners. In addition, the new OAP MIS can query the HRMIS to check whether a new applicant’s NID number is already associated with a beneficiary in the civil pension program (as a person is eligible to receive only one pension, either a civil pension or an old age pension). These improvements will help the OAP to maintain an up-to-date beneficiary list to serve as a basis for payments. Deceased and ineligible beneficiaries are to be removed in a timely manner.

**Incomplete death registration also poses a challenge for keeping the OAP (and civil pensioners) databases up to date.** Only 38 percent of deaths are estimated to be registered in Lesotho, which creates a challenge for the accuracy of the NID system and its ability to provide up-to-date information regarding deceased persons to the OAP and other relying parties. Even with seamless interoperability between the NID system and the OAP (and other systems), program integrity will be compromised if a large share of deaths continues to go unreported. Thus, addressing death registration gaps would play an important role in maintaining a clean payroll and minimizing leakages in the future.

**Improved interoperability between the OAP MIS and the NID system could also be used to promote the easier registration of beneficiaries.** With closer linkages between the OAP MIS and the NID system, it may also be possible to make the application process more seamless for beneficiaries. For instance, the NID system could provide the OAP with a list of soon-to-be 70-year-olds\(^\text{12}\) on a regular basis, thereby enabling

\(^\text{12}\) The age at which an individual is eligible to apply for OAP benefits is 70.
the OAP to actively reach out to eligible individuals and initiate the enrollment process. Similarly, it would simplify the implementation of any new policies to lower (or increase) the age of eligibility.

The efficiency of the OAP program could be further strengthened through higher assurance identity verification and authentication processes for payment delivery. OAP payments are currently made in cash (through post offices and other outlets), where beneficiaries or their proxies receive the cash payments. The NID system could be leveraged to strengthen the authentication of payment officers, beneficiaries, and proxies at points-of-payment. For instance, the NID system could be used to enable biometric authentication of beneficiaries and designated proxies to minimize the incidence of fraud and promote greater transparency and accountability. Solutions using one-time-passwords or the machine-readable features of the NID card could also be explored. Such measures could help improve the efficiency of the OAP’s operations, improve service delivery to the OAP’s beneficiaries, and generate fiscal savings from a reduction in fraudulent transactions, thereby helping to support the government’s fiscal consolidation effort.

The NID system could also support the transition from cash to digital payments. To enhance the delivery process, the electronic identity verification capabilities of the NID system could also be used to help beneficiaries establish mobile money or bank accounts with minimal paperwork and effort. OAP payments could then be delivered to digital accounts linked to the beneficiaries’ NID numbers. As such, changes are being considered. In this context, it will be important to ensure that pensioners will be able to spend their transfers without additional burden, for example, by ensuring that there is a sufficiently large network of cash-out-points and outlets accepting digital means of payment — as well as by ensuring that beneficiaries have access to and are able to interact with digital technologies.

---

13 Proxies are allowed to receive the pension payment on behalf of beneficiaries, but they must present their own ID along with that of the beneficiary as well as a letter stamped by the local chief.
3.3 Enhancing Customer Financial Due Diligence and Promoting Financial Inclusion

Meeting customer due diligence requirements\(^{14}\) is a challenge for many individuals in Lesotho. Customers of financial institutions are required to provide a national identification document or other government-issued proof of identity, as well as a proof of address. In some cases, a proof of income may be required as well. Tiered KYC requirements have been put in place for mobile money services. For Tier 1, self-registration (without the need for an official proof of identity) is allowed. For Tier 2, both a government-issued ID and a proof of address are required. Currently, the proof of identity requirements may be met by various existing IDs, including passports and the NID card. The proof-of-address requirement can be particularly difficult to meet due to the high mobility of persons within the country. Customers are often required to provide a letter from their chief, verifying their hometown.

Currently, identity verification processes for financial services in Lesotho are cumbersome and offer limited assurance about customer identities. Financial institutions, particularly banks, have noted the tediousness of enrolling and maintaining customers in the current context, including the extensive

---

\(^{14}\) Customer due diligence refers to a financial institution’s ability to identify the customers by using reliable independent source documents, data or information.
paperwork required and the frequency of lost paperwork, which increases transaction time and costs. The inability to verify the authenticity of the ID card presented — or that it truly belongs to the person presenting it — creates opportunities for fraud, undermining CDD objectives. Without trusted, unique identities, establishing reliable credit registries and expanding access to credit also becomes more difficult. In addition, cumbersome identity verification processes pose a barrier for individuals looking to open financial accounts and access financial services more broadly. According to the World Bank’s Global Findex Report (2017), 54 percent of adults in Lesotho remain unbanked, of which one-third cite the lack of necessary documentation as a reason for not having a financial account.

**More reliable identity verification mechanisms are seen by stakeholders as an avenue to improving both the efficiency and ease of compliance with regulatory requirements in the financial sector.** Identity verification and authentication services offered by the NID system to financial service providers could enable such providers to complete CDD requirements (particularly identity verification) more easily, thereby reducing the paperwork and administrative costs associated with regulatory compliance, increasing assurance, and enhancing operational efficiency (see Figure 3). Reducing the CDD costs in routine transactions would also allow the financial institutions to focus their anti-money laundering and combating the financing of terrorism (AML/CFT) resources on higher risk transactions. In addition, lower onboarding costs could reduce the overall cost of banking, which remains a significant barrier to access. Banks and telecommunications companies consulted during the mission were also of the view that the expected benefits would far outweigh their cost of linking with the NID (that is, through the development of interface and subscription fees).

**Greater availability and use of electronic identity verification mechanisms could also improve the ease of accessing financial services for customers.** The use of higher-assurance digital identity verification and authentication mechanisms, including the ability to verify data against the NID registry in real time, could also reduce the burden on customers in terms of the number of documents to be presented to open a financial account. In addition to more streamlined identity proofing, current proof of address requirements could also be simplified if this information could be directly and reliably verified against the NID registry.15

**The NICR Department, the FNB and select MNOs are piloting an electronic customer identification and verification solution to verify customers’ identities directly against the NID registry.** A MOU was signed between the FNB and the NICR Department to facilitate the first e-KYC pilot16. As part of this initiative, the FNB is provided with online access to the NID system and can verify a set of personal data (including the portrait photo) of its customers directly against the NID database (either through the use of an API or a dedicated website) using the ID number. Although the pilot has been successful in providing the FNB with a higher level of assurance about the identity of its clients, it has also highlighted the need to strengthen technical safeguards and business processes for enhanced data protection and customer privacy. For instance, under the pilot, identity verification requests did not require the authentication of the person whose data was being shared. As a result, it could not be assured that the requesting party had the consent of the customer. To address these potential vulnerabilities, it will be important introduce

---

15 To ensure that the address information held in the NID registry remains up-to-date, current processes and incentives for updating address details will also need to be reviewed. In addition, information not readily available in the NID registry and often attested by the chief, such as information about a person’s social network, will likely continue to remain relevant for banks, especially in the context of credit risk management and loan recovery.

16 The Central Bank of Lesotho (CBL) as a regulator of banks took part in this process. At the time of the mission, CBL had conducted an independent review of the NID system and provided clearance to the FNB to proceed.
additional data protection and privacy-enhancing features — discussed in Section 5 — before the large-scale launch of the electronic customer identification and verification services.

Maximizing the benefits of greater interoperability between the NID system and financial institutions would require changes in regulations and business processes. A review of current KYC guidelines could help ensure that the identity data that financial institutions are required to process — including as part of KYC and due diligence checks — would be limited to only what is absolutely necessary. Industry players also raised concerns about electronic customer identification and verification potentially leading to duplicative administrative processes, given that the existing requirements of the Central Bank regarding KYC still require the use of paper-based records.

Figure 3: ID Interoperability with the Financial Sector: Cost-Benefit Considerations

<table>
<thead>
<tr>
<th>Expected Costs</th>
<th>Expected Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direct Costs</strong></td>
<td><strong>Direct Benefits</strong></td>
</tr>
<tr>
<td>- Technical infrastructure.</td>
<td>- Enhanced KYC for regulatory compliance and risk management for financial institutions.</td>
</tr>
<tr>
<td>- Fixed and labor costs for the development and maintenance of APIs.</td>
<td>- Reduction of entry barriers will improve access to financial services by the population, and expand the clientele base for providers.</td>
</tr>
<tr>
<td>- Scanners and biometric verification devices/finger print scanners (where applicable).</td>
<td></td>
</tr>
<tr>
<td>- Annual maintenance fees to the NID.</td>
<td></td>
</tr>
<tr>
<td><strong>Indirect Costs</strong></td>
<td><strong>Indirect Benefits</strong></td>
</tr>
<tr>
<td>- Development of and compliance with trust framework for data sharing.</td>
<td>- Efficiency of operations by financial service providers due to lower transaction costs around KYC and risk management.</td>
</tr>
<tr>
<td></td>
<td>- Improved service delivery and convenience to clients due to efficiency gains.</td>
</tr>
<tr>
<td></td>
<td>- Increased financial inclusion.</td>
</tr>
</tbody>
</table>

Source: Authors’ schematic.
Note: API= Application Programming Interface; KYC= Know Your Customer; NID= National ID.

4 Additional NID Use Cases under Consideration

Additional opportunities to leverage the national ID system for efficiency, transparency and more citizen-centered service delivery are under discussion in Lesotho. These include utilizing the NID system to improve the efficiency of the NISSA and tax administration, as well as promoting the recognition of the NID across Lesotho’s borders as a travel document and as a proof of identity for service access. The analysis of additional use cases, such as improving accountability in the health sector or the administration of the tertiary education bursary program, could also be considered.
4.1 Social Protection Programs

Building on the experience of the pensions program, initial efforts are underway to expand the use of the NID and link digital identity verification mechanisms to other social protection programs. The NISSA, which operates under the aegis of the Ministry of Social Development, is a targeting platform for social assistance. It currently covers three main social protection programs: The Child Grant Payments (CGP), the Orphans and Vulnerable Children (OVC), and the Public Assistance Program. The CGP targets the poorest of the poor, providing quarterly payments for about 30,000 households, whereas the OVC pays the school fees for children identified under the same program. The Public Assistance Program offers cash grants to the poorest of the poor families (without children), providing 250 Maloti (US$ 15 equivalent) per month per person (paid quarterly) for about 12,600 beneficiaries. The NISSA also uses census data to target and identify the beneficiaries for the social protection programs.17

As linkages between the NID system and the NISSA are strengthened to minimize leakages and improve beneficiary identification, it will be important to ensure full NID coverage among NISSA beneficiaries. Currently, there is no requirement to have a NID number to access social protection. This helps to minimize the risk of exclusion for the already vulnerable population targeted under the programs.18 Notwithstanding, the NISSA projects that persons without NIDs currently enrolled in their programs are in the minority.19 At the same time, without a reliable means of verifying the identities of beneficiaries and relationships within households, the implementation of NISSA programs remains vulnerable to fraud. For instance, beneficiaries may overestimate the size of their household in order to receive a higher payment; alternatively, people may provide fraudulent information to receive another person’s grants. Although the incidence of such practices is believed to be relatively limited, leveraging data in the population registry could help to seal off such leakages, as well as ensure that assistance reaches the intended beneficiaries. At the same time, to ensure that vulnerable beneficiaries of NISSA’s programs without IDs are not excluded, it would be necessary for the NISSA, like the OAP, to work with the NICR Department to complete the process of obtaining NIDs for all adult beneficiaries, as well as birth certificates for all children in beneficiary households.

Interoperability between the NISSA and the NID system could create savings and strengthen the effectiveness of social protection. With improved digital linkages, the NISSA could: uniquely identify beneficiaries; verify the identity of applicants and authenticate beneficiaries with greater assurance at points of payment; and update the NISSA database with changes in household composition. This would help to enhance NISSA’s efficiency, minimize opportunities for fraud, and optimize expenditures. The NISSA has already engaged the services of a consulting firm to develop APIs for the institution, which should enable automated data exchange with the NID system. However, the work is still at a preliminary stage. The NISSA and the NICR Department have also initiated a dialogue regarding the verification of existing beneficiary data, and are working together to facilitate the enrollment of beneficiaries who do not yet have IDs.

---

17 NISSA uses the Community-Based Technique and Proxy Means Score as a targeting technique. In addition to the census-derived list, NISSA also has a case management system to manage on-going enrollments through an eligibility appeal process.
18 Some of the beneficiaries live in hard-to-reach areas and are among the last mile yet to be covered by NICR.
19 No exact figures were provided.
4.2 Domestic Revenue Mobilization

With a tax-to-GDP ratio of 41 percent, Lesotho is among the top performers in sub-Saharan Africa in terms of domestic revenue mobilization. Given that the sub-Saharan African average is 15.6 percent, Lesotho’s tax-to-GDP is significantly higher than many countries in Africa. It is also higher than in any of the Southern African Development Community (SADC) countries. Yet, given the country’s macroeconomic context — including subdued growth in its sub-region, significant development financing needs, and an even more uncertain policy environment with the COVID-19 crisis — it will be important to further strengthen domestic resource mobilization. In this context, the International Monetary Fund (IMF) highlights that there is room to broaden the tax base in Lesotho to provide additional revenues without undue burden on the private sector.

The Lesotho Revenue Authority (LRA) is already implementing reforms, a key part of which entails a re-engineering of taxpayer identification processes. In particular, the LRA plans to link NID numbers with Tax Identification Numbers as the institution gradually moves away from self-assessments to assessments based on digital, intelligence-based analysis for individual financial data. To this end, the LRA has recently developed APIs to interface with the country’s Integrated Financial Management Information System (IFMIS), although the connection is not yet fully operational. Interoperability with the NID system could also help to facilitate the identification of taxpayers across relevant databases. For instance, authorities in Argentina improved audit targeting and uncovered more instances of tax fraud, evasion, and arrears by linking tax databases together with other registers (including property and vehicles), thereby generating approximately US$44 million in additional revenues between 1999 and 2007 (World Bank 2018a). To explore the feasibility and terms of data exchange between their registries, further discussions between the LRA and NICR Department would be needed.

The NID system can also help strengthen business registration processes and support the formalization of cross-border traders. Improved identity verification processes leveraging the NID registry could be used to simplify the business registration process, as well as to support the work of LRA in its efforts to include informal businesses and the self-employed in the tax net. However, work on this topic is still in the early stages. Relatedly, the LRA has recently commenced an Exchange of Information Initiative with the South Africa Revenue Service dubbed “Your Export is My Import”. The NID could be used to credibly identify informal and self-employed exporters without business credentials under the program.

Box 1: Digital IDs and the Digital Economy

Digital ID systems — systems and processes that allow people to securely prove who they are online — are widely recognized as an important foundation of the digital economy (Figure 4). Many African countries, including Lesotho, are working toward leveraging digitalization; growing their Internet connectivity and access; increasing efficiency in service delivery; and creating new economic opportunities. As such, digital IDs are expected to play an important role. Given its remote nature, the digital economy requires that people be securely and reliably authenticated without in-person interactions in accessing internet-based services and transactions. Various digital platforms — including e-commerce marketplaces, service applications, and government portals — typically utilize alternative (and secondary) means to validate identities, such as email addresses or telephone numbers, guided by the level of assurance required. Yet, these credentials will often provide only a relatively low level of assurance, thereby limiting the type of services and transactions that their holders can access online. For example, they may not provide sufficient assurance to facilitate online access to financial services or government transactions, such as applications for social protection programs or processing tax filings. To respond to the growing demand for secure online identification, the current NID system could be leveraged for the issuance of trusted e-ID credentials, either by the government or by the private sector. This could help accelerate the transition to a digital economy and reduce the
costs and risks associated with in-person transactions (for example, reducing travel costs and time, long waits to be seen, COVID-19 transmission risks from crowds, and staffing costs).

Figure 4: Pillars of the Digital Economy and Proposed Targets

Source: World Bank Digital Economy for Africa (DE4A) Program and authors.

4.3 Cross-border Services and Movement

**Large numbers of people and goods cross the Lesotho-South Africa border on a daily or weekly basis.** As Lesotho is entirely surrounded by South Africa, there is high degree of mobility among citizens of both nations across the border for trade, work, education, as well as close cultural and family connections. As many as 400,000 Basotho are estimated to reside in South Africa (Truen and others 2016), and several thousand people cross the border on a daily or weekly basis for work or to go to school in South Africa. Similarly, some Basotho people reside in South Africa, but work in Lesotho.

**Closer collaboration between Lesotho and South Africa regarding cross-border identity verification and authentication could bring mutual benefits.** Given the constant flow of people and goods between the two countries, being able to verify identities across borders is important for the effective administration of public services in both countries, as well as for the creation of economic opportunities. There has already been a precedent for cross-border identity verification under the Lesotho Special Permit (LSP) program with South Africa. The LSP was introduced as an amnesty program for undocumented Basotho migrants in South Africa. To qualify, the persons had to be recorded in the Lesotho population register. The NICR Department developed APIs, which were then shared across the border with the South African Home Affairs Department. This made verification of Basotho nationals in South Africa by the South African Government possible under the LSP.

**Mutual recognition of national IDs as a travel document between and Lesotho and South Africa could help facilitate trade and the safe and orderly movement of people between the two nations.** At all borders, passports are currently required for travel, although a special dispensation is in place for a limited class of persons. These include students with study permits, diplomats, and very important persons (VIPs) whose passports are not stamped when they cross the border. However, the most frequent commuters
quickly fill their passports. Those who do not have passports may utilize unofficial travel routes, taking advantage of the porous borders, which poses risks to effective border management, as well as their own personal safety and well-being. The use of IDs as travel documents could make travel more secure and accessible for all, operating alongside national, regional or continental passports. In sub-Saharan Africa, the use of national IDs as travel documents has already been adopted among several countries, including Kenya, Rwanda and Uganda, as part of measures to implement the East African Community (EAC) Common Market Protocol agreement regarding the free movement of people.

Cross-border interoperability of ID systems and mutual recognition of national IDs could also support sub-regional, regional, and continental integration and economic opportunities (see Box 2). South Africa remains the most significant cross-border partner for Lesotho. However, there are additional opportunities under the SADC and the African Union for cross-border interoperability (and mutual recognition of IDs), if agreed by countries in a sub-regional or continental context. At the continental level, the African Continental Free Trade Area (AfCFTA) Agreement, which was also signed by Lesotho, is worth highlighting as it aims to boost intra-African trade. Expanding the number of agreements with African countries regarding the use of national IDs as travel documents could support mobility and trade, as well as the use of more formal channels. Currently, informal cross-border trade constitutes between 30 to 40 percent of intra-regional trade in the SADC region; greater formalization could significantly increase public revenues and promote inclusive economic growth. The mutual recognition of national IDs across borders could also help reduce vulnerability among individual informal traders, facilitate their use of financial services across borders, as well as the payment of taxes at the border (World Bank 2017c).

**Box 2: Toward Cross-border Interoperability in Africa**

There are two main approaches to the cross-border interoperability of ID systems to facilitate mutual recognition of IDs, namely standardization and harmonization. Standardization involves setting the minimum requirements that will enable ID systems to communicate with each other. Therefore, it focuses on the interoperability dimension, allowing countries to build or maintain their own foundational ID systems to reflect national priorities, contexts and aspirations. It also enables participating countries to move at their own speed. For example, the European Union’s electronic Identification, Authentication and Trust Services (eIDAS) (European Commission) enables a citizen or resident of one EU country to access online public services (and private services in some cases) in another EU country with a digital ID issued by the original EU country. This approach is based on standardization.

The harmonization of foundational or national ID systems into a single regional ID system or into the same system replicated across countries typically requires strict specifications that countries must implement. This may be more difficult to achieve in practice, as has been seen in the case of Economic Community of West African States (ECOWAS) National Biometric Identity Card (ENBIC). Standardization (as the eIDAS experience has shown) is thus often easier and less resource-intensive to implement in terms of achieving interoperability among countries in a region.

Based on World Bank research and operational experience, multiple architectures for cross-border interoperability could be utilized to facilitate mutual recognition on the African continent while also maintaining national sovereignty. These are based on the following underlying principles:

---

20 Outside of Africa, the Southern Common Market (MERCOSUR) of Latin America and the European Single Market have similar arrangements which allow citizens of member countries to utilize their national IDs as travel documents between member countries. Digital verification of the IDs and their holders is not always required/practiced. Sometimes a manual comparison of the photo of the ID card with the ID holder is sufficient.

21 As of May 2020, Lesotho had yet to deposit the Instrument of Ratification at the African Union Commission.
• Standards underlying mutual recognition: The process and data and legal and technical standards (for interoperability) are defined and agreed upon by member countries at the continental level for cross-border mutual recognition.

• Levels of Assurance: The level of assurance required for access to a service and the assurance level of the credentials/authentication mechanisms are defined and agreed upon by the participating countries.

• Flexibility: Each participating country may have one of more different forms of credentials/authentication mechanisms — which may be the same or different when compared to other states (for example, passwords, personal identification numbers (PINs), one-time passwords (OTPs), smart cards, fast identity online (FIDO) authenticators, mobile IDs, and biometrics).

• Principle of Variable Geometry: While a continental or sub-regional framework may be agreed by all countries, the principle of variable geometry means that implementation can proceed at different speeds.

Source: Authors.

5 Harnessing the Potential of NIDs: Recommendations to Enhance Inclusion, Trust, and Linkages with Service Delivery

With careful and targeted interventions, Lesotho can unlock the potential of its foundational national ID system. Current and emerging linkages between the NID system and programs and services in the public and private sectors indicate considerable potential, progress and interest in harnessing the NID system for more efficient, transparent and citizen-centered service delivery. These cases also reveal areas which can be strengthened to lay the groundwork for a more inclusive, trusted and service delivery-oriented NID system.

As service providers increasingly look to the NID system to verify identities, it is important to ensure that individuals are not prevented from accessing critical services due to a lack of identity documents. Thus, ensuring the accessibility of the NID system for all, including the most vulnerable segments of the population, will be critical. In parallel, it will be important to boost the completeness and timeliness of birth and death registration records to ensure access to identification from birth to death, as well as the accuracy of data held within the population registry.

With greater interoperability and data exchange come greater risks that will need to be carefully managed. The process of automated identity verification and authentication requires an interaction among different systems and data-sharing mechanisms. By virtue of capturing, storing and using individual data, digital ID systems present risks to privacy and the misuse of data. If not addressed properly, such vulnerabilities can erode trust in the NID system. To mitigate these risks, it is important to establish and/or update legal frameworks for data protection, privacy and cybersecurity, as well as to follow a privacy- and security-by-design approach for the management of the ID system.

Decision-making about which identity verification and authentication options will be deployed in various use cases should follow a risk-based approach. Stakeholders should consider the level of assurance needed for various transactions to mitigate fraud and other risks, as well as the potential for exclusion and privacy violations involved with requiring identification or authentication for various purposes. The NICR Department should strive to make a wide range of identity verification and authentication options available to correspond to the different risks (and levels of assurance) associated with a given service or transaction. For lower-assurance transactions, more informal or self-attested proofs of identity and other attributes may be sufficient. Protecting individual data and privacy through a
variety of measures, including appropriate laws, policies, business processes, and technologies, should be at the core of any services offered.

5.1 Increasing Accessibility and Reaching the Last Mile

As the GoL moves toward establishing closer linkages between the NID and other systems, it is important to increase efforts to reach people currently excluded from the NID system. This is necessary to ensure that the lack of a NID or other government-issued credential does not become a basis for exclusion as some services begin to make mandatory use of the NID to promote efficiency. To promote inclusion, service providers and even private-sector financial institutions can become partners for the NICR Department in reaching vulnerable populations — as is being done with the Ministry of Public Service and the OAP. Close collaboration with the NICR Department and service providers and the deployment of innovative and inclusive registration solutions can help ensure that clients or beneficiaries who do not yet have an NID are rapidly enrolled. Targeted end-user surveys, including qualitative research, can also help to identify additional barriers, needs, and concerns among the unregistered population. In addition, they can be used to inform interventions to provide universal access to NIDs.

Scaling up existing initiatives for mobile registration will be critical to expanding access to the NID among vulnerable and remote populations. Distance to registration centers and the associated cost of travel likely represent key barriers to obtaining a NID for those currently without one. Thus, being able to bring registration closer to the people through regular, periodic mobile registration drives — and by coupling mobile registration with key outreach efforts by other public service providers — could help to remove some of the greatest barriers to enrollment. The effectiveness of such an approach was well demonstrated by the payroll and old age pensions initiatives. It may also be necessary to put in place more flexible documentation requirements for registration. In this context, a 2017 survey also found that 54 percent of those without a NID cited a “lack of necessary documents” as a reason for not having one (World Bank 2017b).

It is imperative to ensure universal coverage of individuals and guarantee the accuracy of the NID system by increasing birth and death registration rates. The establishment of birth and death registration points in health facilities, including added incentives for timely registration, could bolster current death and birth registration rates. Close collaboration between the NICR Department with local governments and chiefs could also boost timely reporting. ‘Catch-up’ birth registration drives in schools as children enter primary education can also contribute to improving the completeness of records. Making birth registration a requirement — or enforcing the birth registration requirements for access to grants and other social protection programs — may also be effective in increasing registration rates. However, care should be taken to avoid the exclusion of vulnerable beneficiaries due to an inability to obtain the required documents.

Beyond NID enrollment, ID card renewal and data updating processes need to remain accessible to ensure that people’s records are kept up to date. As more and more service providers rely on the NID for up-to-date information, it will be important that ID holders are able and motivated to update personal details, such as their addresses or mobile phone numbers, in a timely manner. Currently, ID card renewals and data updates are time-consuming processes that include the biometric authentication of applicants. For updating of less sensitive details, the use of lower-assurance authentication methods could help to improve the user experience. It could also encourage more frequent updating of important dynamic data, such as addresses.
5.2 Updating the Legal and Policy Enabling Environment

A number of steps will need to be taken before Lesotho’s existing legal framework is ready to support domestic and international data sharing with the public and private sectors. A review of Lesotho’s legal enabling environment for data sharing was undertaken in 2019 with support from the World Bank’s ID4D Initiative. The review identified several gaps and inconsistencies within the existing legal and regulatory framework, and outlined recommendations for addressing them. A summary of some of the key findings from the report are highlighted below. Key recommendations are included in the Annex to this report.

Certain key provisions in the legislation dealing with the sharing of ID data by the Lesotho Government are overly restrictive. As a result, it may be challenging for the GoL to lawfully share the ID data for the purposes of administering salary or pension payments to public servants. In particular, the power of the GoL to share ID data with third parties may be unnecessarily limited under the National Identity Cards Act (NICA) of 2011. As such, it may require review and amendment to ensure that the permitted disclosures cover the categories of recipients and data-sharing purposes envisaged by the GoL.

The GoL will require a legal basis for processing ID data under the Data Protection Act (DPA) of 2011. One of these legal bases is user consent. If consent is relied upon as the basis for participation in digital identity verification and authentication processes, this could increase individual buy-in to the scheme. In this regard, it may assist in fostering trust and improving the individual’s perception of having sovereignty over their own data. To further protect individual privacy and promote fairness, consideration should be given as to whether the DPA 2011 should be amended to provide that, where the processing of personal data is based on user consent, users may withdraw consent to processing at any time. In response, data controllers must cease processing that data when consent is withdrawn. For some purposes, consent may not be the most appropriate legal basis, depending on the envisaged use for the NIR (for example, consent will not be appropriate where the envisaged use case is fraud detection, including where payment of salaries using NIR data is carried out with the purpose of reducing ghost beneficiaries). If the GoL chooses not to rely on consent and opts to make participation in identity verification and/or authentication processes mandatory, this may be effective in increasing the volume of participants in the scheme. The appropriate legal basis under the DPA 2011 will also depend on the approach the GoL wishes to take.

Provisions related to the processing of sensitive personal data may need to be revised. In the process of establishing the interoperability between the NIR and service providers and the provision of identity verification and authentication services, the GoL may also be processing sensitive personal data (such as data relating to children). Processing sensitive personal data is generally prohibited under the current legal framework, unless an exemption under the DPA 2011 applies. However, the existing exemptions may be too narrowly drafted to allow the government to process these types of data lawfully for the envisaged purposes.

Certain provisions are drafted heavily in favor of the relevant data controller, potentially to the detriment of individual privacy rights. This may lead to a risk of a lack of trust in the national ID system and its use in service delivery, which in turn may negatively affect participation. In particular, financial institutions have sweeping powers to process extensive amounts of personal data for the purposes of carrying out due diligence on their customers. Individuals have rights of access and the ability to request

---

22 This section summarizes the findings from the Legal and Policy Enabling Environment for Digital ID in Lesotho, carried out by the ID4D initiative. Key issues and recommendations are drawn from the report’s executive summary. For a more detailed review, please see the full report.
corrections of inaccurate data. However, data controllers may refuse such requests. The DPA of 2011 does not delineate the kinds of circumstances under which the data controller may refuse to comply with data subject access requests. This may give rise to issues involving perceptions of unfairness and an imbalance between the rights of data controllers and the rights of individuals.

The existing data protection governance regime may need to be bolstered to improve accountability and transparency. The current arrangements regarding the removal of members of the Data Protection Commission (which enforces the DPA of 2011) could potentially give rise to allegations of partiality because the Prime Minister may remove a member without cause and at his/her discretion. The Data Protection Commission may also choose to abandon enforcement actions if it considers that such actions are “unnecessary or inappropriate”. This power could potentially be exploited. Thus, the relevant provisions under the DPA of 2011 dealing with the establishment and powers of the Data Protection Commission may need to be revisited.

Additional protections should be put in place to govern the sharing of personal data. Developing sector-specific template agreements (or MOUs) for use when sharing ID data with other government agencies or the private sector (for example, financial services) could be considered to ensure that the transfer is subject to appropriate contractual protections. It may also be beneficial for the Data Protection Commission to consider consulting on proposals for publishing a data-sharing code of conduct, which sets out best practices for sharing data, including ID data.

The establishment of an appropriate legal and regulatory framework regarding cybersecurity would provide additional safeguards. The government is in the process of enacting cybercrime legislation which sets out various computer-related offenses. However, it is not clear if there is also a separate regime governing cybersecurity, which is key to ensuring adequate protection of digital ID systems from a cybersecurity perspective.

To prevent exclusion, it may be beneficial to revisit provisions regarding prescribed ID enrollment fees. Exercising the right of access, as well as obtaining national ID cards and passports, is subject to a prescribed fee. This raises issues of potential discrimination and the risk that poorer Basotho may be prevented from exercising their rights effectively — or, indeed, from participating in the digital ID scheme altogether.

5.3 Strengthening Business Processes for Identity Management

Continued work toward strengthening the robustness of the NID system will be necessary. Efficient, accountable data management, underpinned by clear business processes, is essential for the trustworthiness of any identification database and credentials used for authentication. Safeguards against exclusion, tampering, identity fraud, and other errors occurring throughout the identity lifecycle are important for ensuring the sustainability of an ID system over the long term. A November 2019 World Bank technical assistance mission identified areas where improvements are needed to future-proof the NID, including improvements around data quality and the business processes for handling exceptions and inconclusive cases, as follows:

- A comprehensive assessment of operational, functional and system design for the National ID - Civil Registry platform is recommended to verify performance and alignment with international standards.
• **Improving the quality of the photos collected would support more accurate authentication of ID holders for service delivery.** Unlike fingerprints, there is currently no automated quality control routine for the portrait photo. Integrating a quality assurance Software Development Kit (SDK) (against criteria set out in the International Civil Aviation Organization [ICAO] 9303 standard) into the front-end software will enhance the quality of the holder’s portrait photo printed onto the ID card. It would also render the manual (that is, with the naked eye) comparison of the NID card with the person presenting it easier. In addition, it would enable the option for authentication (1:1 matching) against the facial image on record.

• **The standardization and centralization of exception-handling processes could help minimize opportunities for discrimination — and promote greater transparency in NID enrollment.** Currently, critical exceptions are processed and resolved at the district level. These are done at the discretion of the local manager(s), without a clear oversight or monitoring mechanism. This arrangement could increase the risk of fraud and discrimination. Processes for exception handling during enrollment need to be clearly laid out (for example, in operation manuals). Establishing a central exception-handling desk to monitor and handle suspended and rejected applications could help to ensure that exceptions are processed in a uniform and objective manner, thereby strengthening the integrity of the enrollment process. Registration agents and management should also receive training to ensure that guidelines are correctly applied in practice.

• **Introducing manual adjudication would strengthen the accuracy of the biometric de-duplication process while also ensuring inclusion.** No automated biometric matching system is 100 percent accurate. Thus, the ability to perform secondary checks and resolve inconclusive cases using manual adjudication or verification by a human operator is important in ensuring the accuracy and integrity of the process and the ID system. For a typical ID system, manual adjudication would be triggered for 0.5 to 3 percent of the new registrations, depending on multiple parameters. Introducing manual adjudication for Lesotho’s NID system could enable the tightening of biometric matching thresholds to minimize the probability of the system accepting false negatives (that is, not rejecting some applicants already enrolled in the system).

5.4 **Strengthening Interoperability and Identity Verification and Authentication Services**

Identification and authentication services should be flexible, scalable and meet the needs and concerns of individuals (end-users) and relying parties (for example, public agencies and private companies). Existing initiatives to link the NID system to service delivery suggest a robust business case for establishing a more systematic interoperability framework and for investing in technical infrastructure. This will enable seamless, secure data sharing between the NID system and domestic and cross-border service and payment providers.

As systems exchange more data, it will be critical for the NICR Department to adopt a privacy-by-design approach to its operations. Maintaining user privacy is a fundamental concern for ID systems. In addition to aligning legal and regulatory frameworks with international data protection and privacy principles, privacy-enhancing technologies and security measures should be built into every aspect of the ID system—that is, privacy assurance must become an organizational norm. The following measures can be considered by the GoL to reinforce information security in the context of interoperability:
• **Minimize data being collected and stored:** The current NID database includes a number of sectoral fields, such as information about assets owned by the individual (immovable properties, livestock, and so on). Storing foundational identity data with sectoral data represents an additional risk in terms of privacy. Therefore, the removal of the collection, processing, and storage of purely sectoral data from NID and CR systems, whenever possible, is recommended. This would also significantly reduce processing times at the district level.

• **Minimize data shared:** Instead of sharing entire records or profiles of individuals, identity verification and authentication requests should instead return a Yes/No answer only. Additionally, a good practice in terms of consent collection consists of conditioning the sharing of personal data on the successful authentication of the corresponding subject (person and/or mobile phone authentication). Indeed, an effective way to ensure consent and minimize the opportunities for identity fraud is to verify that the subject was physically present at the time of the transaction.

• **Review API security:** The application-level security of the generic interface API currently relies on a white list of public Internet Protocol (IP) addresses and a pass phrase. Nevertheless, IP addresses can be spoofed\(^{23}\), and static secrets can leak. Given the critical nature of the data being communicated, it is advisable to: use end-to-end encryption for data in transit; authenticate API client systems using digital certificates; and introduce additional safeguards, such as making re-authentication mandatory in case of overuse. A comprehensive data security assessment is recommended, and it should be carried out by a reputable IT security auditing firm.

• **Strengthen client authentication and individual accountability:** Relying on IP addresses for accountability could further encourage malicious agents to indulge in fraudulent activities. Currently, the same public IP address can be used by multiple operators (for example, 10 different clerks at the same branch). Logins and passwords can often be shared between employees. In those circumstances, accountability for misuse or unauthorized access cannot be easily determined. Various options can be considered to strengthen individual accountability and access control, including leveraging biometric logins and/or providing each operator with an individual, personal (nominative) physical token required for operating the requesting system(s).

• **Improve people’s oversight and control over their data:** A central tenet of the security and privacy by design principles is that individuals have the right to access and correct their data, as well as monitor how it is being used by governments and third parties — and to hold these actors accountable for any misuse. Creating a platform or portal where individuals can log-in and view their personal information and records of who has accessed their data, when, and why can strengthen accountability and personal oversight. It is also important to ensure that there are appropriate grievance redress mechanisms in place for individuals to raise their concerns and receive a timely response, whether about the accessibility, security, or the efficiency of the system.

• **Introduce ID number tokenization:** The national ID number is unique, permanent (irrevocable) and easily accessible to all, as it is printed on birth certificates and ID cards. As such, it could be

\(^{23}\) By spoofed, we refer to a practice of creating an Internet Protocol (IP) package with a false source IP address for the purposes of impersonating another computer system.
used by malicious actors to subject individuals to surveillance and profiling, thereby increasing the risk of identity theft. Therefore, a good practice is to limit the disclosure of this root unique identifier by substituting it for an ID number token. A token would be a unique identifier generated by the central back-end ID system and linked to a national ID number. The tokens can be user-generated (through a web portal or a mobile application) or system-generated. Contrary to a root ID number, a token can be revoked/replaced.

- **Replace the ID number printed on the ID card with a token ID number:** An increasing number of countries have started to replace the irrevocable, root unique identifiers printed on identity documents with tokens (for example, The Netherlands and Nigeria). This measure mitigates the risk of misuse of identity data. If needed, the root ID number could still be stored in the Machine-Readable Zone of the ID card (that is, the 2D barcode printed at the back of the card).

A range of new authentication, verification, and data-sharing services could be offered to better cater to the needs of relying parties while also preserving the privacy of users. The NICR should strive to make multiple, different authentication options (for example, fingerprint authentication + OTP over SMS) available to relying parties wishing to have an even higher level of assurance when authenticating their users. It is also important to consider that many relying parties need not access personal data collected and stored by the NID system. Using the information contained on the ID card, including its Machine-Readable Zone and 2D barcode, may already constitute a sufficient level of identity assurance for certain services and transactions. A good practice consists of engaging with existing and future relying parties to better understand their needs in terms of authentication, verification and access to personal data managed by the NICR Department, while also managing expectations.

Identity verification and authentication services can be a source of revenue, but it is important to ensure affordable access and manage unintended negative consequences. Before implementing any fees, it will be important to undertake extensive stakeholder consultations to understand potential impacts. A key concern will be to ensure that fees are not set at a level whereby costs will be passed on to the consumer in such a way as to hamper financial inclusion or access to basic services. Ensuring transparency in the fee structure and accessibility to identity verification and authentication services for relying parties in a non-discriminatory manner would also be crucial.

6 Conclusion

Lesotho has put in place a strong foundational National ID, which is already being leveraged to support more efficient, citizen-centered service delivery. As reflected in this note, with further careful and targeted interventions, the ID system will be able to provide secure, inclusive identity verification and authentication services for a wide range of public and private sector applications. It also has the potential to facilitate more effective cross-border service provision and a boost in mobility. Collaborative initiatives already underway between the NICR, the Ministry of Finance, the Ministry of Public Service, and financial institutions demonstrate the potential benefits to be realized and feasibility in the Lesotho context.

To maximize the benefits of the NID system and fully harness its transformational potential, this note identified critical areas to strengthen. As service providers increasingly look to the NID system to verify identities, it is important to ensure that individuals are not prevented from accessing critical services for lack of identity documents. This requires careful attention to reaching the last mile. Further, with greater
interoperability and data exchange come increased risks related to data protection and privacy. These risks can be carefully managed by updating legal frameworks for data protection, privacy and cybersecurity, as well as by incorporating privacy- and security-by-design in ID systems. Finally, continued attention to bolstering technical capabilities and business processes can promote trust and help ensure the long-term sustainability of the foundational National ID.
7 References


8 ANNEX 1: Key Recommendations Arising from the 2019 Legal Enabling Environment Report

Sharing ID Data

a) Sections 6(2) and 7(1) appear to deal with data sharing of information recorded in the National Identity Register; however, the relationship between these sections is unclear, particularly whether the grounds for sharing in section 7(1) are in addition to those set out in section 6(2). Consideration should also be given as to whether the relationship between sections 6(2) and 7(1) of the National Identity Cards Act (NICA) should be clarified pursuant to an amendment to the NICA.

b) To the extent required, consideration should be given as to whether section 6(2) of the NICA should be amended to ensure that the permitted disclosures cover all the categories of recipients and data-sharing purposes are envisaged by the Lesotho Government — in particular, where data is being transferred between government departments and public bodies.

Use Cases/Legal Basis for Processing

a) If participation in the digital ID scheme is based on consent, this may increase individual perception of sovereignty over their ID data. To further protect individual privacy and promote fairness, consideration should be given as to whether the Data Protection Act (DPA) of 2011 should be amended to provide that, where the processing of personal data is based on user consent, users may withdraw consent to processing at any time. Furthermore, data controllers must cease processing that data when such consent is withdrawn.

b) Consent may not be the most appropriate legal basis, depending on the relevant use case for the ID data. In that instance, another legal basis under the DPA of 2011 will need to apply. Certain legal bases for processing set out in the DPA 2011 may not be drafted widely enough to allow the government to process ID data for the envisaged purposes. Accordingly, consideration should be given to whether:

i. The legal basis set out in section 15(2)(e) of the DPA 2011 (which allows for the processing of personal data by public bodies in the performance of their “public law duty”) is wide enough to cover the envisaged purposes for processing ID data, including for the payment of pensions to eligible individuals; and

ii. Section 15(2)(f) of the DPA of 2011 is very broadly drafted, as it allows for the processing of personal data in the legitimate interests of the data controller and the third-party recipient of the data. As such, it may need to be reviewed and amended to assist with recalibrating the balance of interests between the data controller and the data subject. Consideration should also be given as to whether data controllers should be required to carry out a balancing test to ensure that the rights of individuals are not being prejudiced when utilizing this legal basis. In addition, consideration should be given as to whether it is appropriate for public bodies to be able to rely on this legal basis.
Processing of Digital ID Data by Financial Institutions

a) Consideration should be given to the types of digital ID data that financial institutions would be required to process to carry out Know Your Customer (KYC) and due diligence checks. This needs to be reviewed to ensure that data being processed under the KYC guidelines is relevant and not excessive.

b) Section 8 of the KYC guidelines should be reviewed and possibly amended by removing reference to ‘any other matter that a bank may find fit to consider’. This may assist with ensuring the bank only collects the personal data it needs to carry out due diligence and other relevant checks.

c) Consideration should be given as to whether section 12(3) of the KYC guidelines should be reviewed and possibly amended to ensure that individuals will continue to be ‘politically exposed persons’ and therefore classified as ‘high risk’ customers for a period longer than twelve months after leaving office.

Sensitive Personal Data

a) The general exemptions to the prohibition on processing sensitive personal data set out in section 36 of the DPA of 2011 are relatively narrow. Therefore, the Ministry of Home Affairs (MoHA) should consider the following:

i. Amending section 36 of the DPA of 2011 so that it provides for an exemption, which will apply to the government’s processing of sensitive digital ID data; and amending the definition of “sensitive personal data” in the DPA of 2011 so that it does not include data relating to children. This may be an overly broad inclusion, as it goes above and beyond the approach taken in the General Data Protection Regulation (GDPR), which does not classify these types of data as “sensitive” (or “special category” data as it is known under the GDPR); and

ii. The GDPR also includes “biometric” and “genetic” data in the definition of “special category” data, which the MoHA should consider including in the definition of “sensitive personal information” in the DPA of 2011. Indeed, these types of data will have special significance in the context of administering a digital ID scheme, particularly where that scheme has biometric authentication functionality.

b) Under section 37 of the DPA of 2011, the Data Protection Commission may make an authorization allowing for the processing of personal data under certain circumstances. The Data Protection Commission should consider whether this is appropriate for the purposes of making salary and pension payments, as well as for the use of ID data by financial institutions.

Accuracy of Data

In some instances, the relevant sources from which the government may collect ID data do not appear to be updated in real-time, which may lead to issues in terms of data accuracy. Consideration should be given to implementing a technical solution to allow real-time updates between the various sources, including the National Identity Register.
**Cross-border Data Sharing**

a) To enable more effective data sharing with South Africa, consideration should be given to the relationship between the DPA of 2011 and the South African Development Community (SADC) Model Law on Data Protection, specifically whether it would be appropriate to align Lesotho’s laws on data transfers with those of the SADC Model Law on Data Protection since both Lesotho and South Africa are members of the SADC (although it should be noted that the SADC Model Law on Data Protection takes a different approach to international best practice under the GDPR).

b) In order to seek to ensure that any transfers outside of Lesotho and the SADC are subject to an adequate level of protection, consideration should be given to whether the GoL (or the Data Protection Commission, whichever is more appropriate) should consult on and develop a set of standard data protection clauses, which would establish the minimum required safeguards to be implemented by the recipient entity for transfers of data.

**Data Minimization**

The GoL should consider the minimum information required to process digital ID authentication services, and to ensure that it does not collect more personal data than necessary to carry out that purpose.

**Accountability and Governance**

a) Under section 9(a) of the DPA of 2011, the Prime Minister has the power to remove members of the Data Protection Commission without reason. To ensure the independence of the Data Protection Commission, consideration should be given as to whether this power is appropriate, and whether the involuntary removal of members should only be permitted with good cause, such as the dereliction of duty.

b) Section 41(2) of the DPA of 2011 provides that the Data Protection Commission may drop enforcement action where it is of the view that that enforcement action is “unnecessary or inappropriate”. However, this may need to be reconsidered. Since this provision is so widely drafted, it may be open to the risk of misuse. If the Data Protection Commission decides not to take any action in relation to an enforcement notice, section 41(1) of the DPA of 2011 sets out various specific reasons on which it may rely. Section 41(1) of the DPA of 2011 should also be reviewed to ensure that it establishes adequate, fair and balanced reasons for abandoning enforcement action.

c) It may also be beneficial for the Data Protection Commission to consider consulting on proposals for publishing a data sharing code of conduct, which establishes a best practice for sharing data, including ID data.

**Cybersecurity and Cybercrime**

a) The MoHA should consider implementing a separate, detailed regime to deal with cybersecurity matters, if it has not done so already. This is a key part of ensuring the security of the digital ID system.

b) Consideration should be given as to whether digital ID systems should be categorized as “critical infrastructure” in order to be included in the protection of section 9(3) in relation to offenses against critical infrastructure.
c) Consideration should be given as to whether the concept of “critical infrastructure” may also need to be reflected in any legislation pertaining to cybersecurity. This would help to ensure that critical infrastructure is afforded additional protection in terms of requiring that special cybersecurity measures be implemented for that type of infrastructure.

d) Consideration should be given as to whether sections 12(3) and 15 of the Lesotho Cybercrime Bill regarding identity-related offense should be reviewed to ensure that the drafting and penalties are sufficiently robust to operate effectively and act as a deterrent.

Data Flows

In seeking to ensure that ID data being shared between government agencies or with private entities is subject to an adequate standard of protection, the MoHA should consider the following:

a) Developing sector-specific template agreements (or MOUs), which private entities and other government agencies are required to enter into when data is shared with a government agency or a private entity. It should be noted that the MoHA is in the process of implementing this recommendation. As of August 2019, the World Bank provided an initial draft of the proposed MOU with the First National Bank of Lesotho (the “FNB Agreement”); and

b) Publishing the template agreements (or MOUs) in the Gazette and online, along with a list of signatories. This would help to foster a culture of transparency around the sharing of ID data.

Non-discrimination and Inclusion

In considering the most appropriate way to fund the digital ID scheme, consideration should be given to the effect that the proposed funding would have in terms of individual participation and inclusion. For example, one model would be to require the private sector to pay reasonable fees for verification/authentication. However, individuals and the public sector would not be charged. The NICA Amendment envisages that information from the National Identity Register will be provided by the Director to a third party at a prescribed fee.

Individual Privacy Rights

Sections 26 and 27 of the DPA 2011 outline the rights of individuals to request access to their data, including correction of their data. These sections also provide that data controllers may refuse to comply with such requests; however, the DPA of 2011 does not detail the circumstances under which the data controller may refuse to comply with these requests. This may give rise to issues in terms of a perception of unfairness and an imbalance between the rights of data controllers and the rights of individuals. The MoHA should consider whether these sections should delineate certain limited circumstances in which data controllers can refuse to comply with data subject access requests, as well as requests for correction of information. The MoHA should also consider whether data subjects should be provided with additional rights, such as the right to data portability, the right of objection and the right to withdraw consent to processing in order to improve an individual’s perception of sovereignty over their data (paragraph Error! Reference source not found. of Part B onwards).