ecdpm

Funded by
the European Union

DISCUSSION PAPER No. 360

Digital ID systems in Africa: Challenges, risks and opportunities

By Melody Musoni, Ennatu Domingo and Elvis Ogah

December 2023

In this paper, we look at the state of play of digital ID implementation across Africa with a focus on South Africa, Kenya, Nigeria, Benin and Namibia. We assess the opportunities and challenges of implementing e-ID systems and analyse the policy implications for African governments as well as for the EU to support its partners' roll-out of user-centric, sustainable and interoperable digital ID systems and frameworks.

Africa is experiencing rapid growth in the development of digital infrastructure. In particular, the development of digital ID systems is high on the policy agenda for the African Union (AU) and its member states as it plays an important role in enabling and improving governments' service delivery, access to digital services, inclusive economic growth and participating in the African Continental Free Trade Area (AfCFTA). African countries, through the AU, have agreed they need to develop interoperable digital ID to facilitate the seamless movement of people, goods and services continentally. Apart from continental efforts, different Regional Economic Communities (RECs) are also piloting regional interoperable digital ID.

Despite this progress, achieving universal coverage remains a key challenge with nearly 500 million people still lacking a legal identification in Sub-Saharan Africa. Furthermore, African governments have been developing biometric databases and digital ID systems mostly before establishing robust data governance frameworks such as data protection and cybersecurity laws. These challenges – which put vulnerable groups such as ethnic minorities and women at risk of exclusion – have hindered the implementation of safe, inclusive and sustainable digital identification systems.

Table of Contents

List of Boxes

List of Figures

List of Tables

Acknowledgements

The authors would like to thank the experts and policymakers who shared their insights with us throughout the research process. This project was funded by the European Union. We would like to thank Pauline Veron and Jamie Slater for supporting us with research on Benin, interviewing policymakers and contributing to the writing of the Benin country study. We also want to thank Chloe Teevan and Pauline Veron for their comments and feedback on this paper. We would also like to thank Annette Powell for her editorial assistance. All views are those of the authors alone and do not represent the views of ECDPM. The authors take responsibility for any factual errors. For any feedback or suggestions regarding future work, please contact mmu@ecdpm.org and edo@ecdpm.org.

Acronyms

ABIS	Automated Biometric Information System
AfDB	African Development Bank
ANIP	Agence Nationale D'Identification Des Personnes
APDP	Beninese Personal Data Protection Authority
AU	African Union
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (Ministry of Economic Cooperation and Development)
CRI	Civil Registration and Identification
CRVS	Civil Registration and Vital Statistics
CSOs	Civil Society Organisations
DCDT	Department of Communications and Digital Technologies
DHA	Department of Home Affairs
DITE	Digital Identity, Digital Trade and Digital Economy
DPCO	Data Protection Compliance Organisation
DPGs	Digital Public Goods
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DPSA	Department of Public Services Administration
DSM	Digital Single Market
DTS	Digital Transformation Strategy
EAC	East African Community
EC	European Commission
ECOWAS	Economic Community of West African States
EIB	European Investment Bank
eIDAS	Electronic identification and trust services
EIF	European Interoperability Framework
eNATIS	Electronic National Traffic Information System
EU	European Union
GDPR	General Data Protection Regulation
GIZ	Gesellschaft für Internationale Zusammenarbeit
GMPC	General Multi-Purpose Cards
GMSA	Global System for Mobile Communications Association
ICAO	International Civil Aviation Organisation
ID	Identity

ID4D	Identification for Development
IDGC	Initiative for Digital Government and Cybersecurity
IDPs	Internally Displaced Persons
IOM	International Organization for Migration
ITU	International Telecommunication Union
KDPA	Kenyan Data Protection Act
MHAI	Ministry of Home Affairs, Immigration, Safety and Security
MOSIP	Modular Open-Source Identity Platform
MRZ	Machine Readable Zone
NADPA	Network of African Data Protection Regulators
NAMFISA	Namibia Financial Institutions Supervisory Authority
NDP	National Development Plan
NDPC	Nigeria Data Protection Commission
NIDB	National Identity Database
NIIMS	National integrated Identity Management System
NIMC	National Identity Management Commission
NIMS	National Identity Management System
NIN	National Identification Number
NIS	National Identity System
NPR	National Population Register
PAPSS	Pan-African Payment and Settlement System
POPIA	Protection of Personal Information Act
PPPs	Public-private-partnerships
RECs	Regional Economic Communities
RNPP	National Registry of Physical Persons
RPA	Registration of Persons Act
SAA	Smart Africa Alliance
SADC	Southern African Development Community
SASSA	South African Social Security Agency
SATA	Smart Africa Trust Alliance
SDGs	Sustainable Development Goals
SEPA	Single Euro Payments Area
SITA	State Information Technology Agency
SSA	Sub-Saharan Africa
STC	Specialised Technical Committee
QR	Quick Response
UIN	Unique Identification Number
UNDP	United Nations Development Programme
UNECA	United Nations Economic Commission for Africa
UNFPA	United Nations Population Fund
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations International Children's Emergency Fund
UPI	Unique Personal Identification
USAID	United States Agency for International Development
WHO	World Health Organisation
WURI	West Africa Unique Identification for Regional Integration

Box 1: Glossary of Key terms

Biometric data:	A biological or behavioural attribute of an individual that can be used for biometric recognition. Examples include fingerprints, face, iris, keystrokes, and signature.
Civil registration:	The continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events (birth, death, marriage, divorce, adoption, etc.) pertaining to the population.
Credential:	A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Examples include ID books, ID cards, Smart ID cards, certificates, unique numbers, etc.
Digital identity:	A set of electronically captured and stored attributes and/or credentials that uniquely identify a person, enabling the distinction of one individual from another.
Digital identification system:	An identification system that uses digital technology through the identity lifecycle, including for data capture, validation, storage and transfer, credential management and identity verification and authentication.
Electronic signature:	An electronic authentication technique that carries the legal weight of and substitutes for a handwritten signature.
Fourth Industrial Revolution:	The digital revolution which is characterised by the fusion of technologies cross-cutting physical, digital and biological spheres.
Foundational identification system:	An identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services.
Functional identification system:	An identification system created to manage identification, authentication and authorisation for a particular service or transaction. Examples include social programmes, voting, tax administration and financial services.
Identity:	A set of attributes that uniquely describe a person within a given context.
Identity attributes:	A characteristic inherent in or ascribed to someone or something such as name, age, sex, place of birth, biometrics, identity number, etc.
Identity ecosystem:	A set of identification systems (databases, credentials, laws, processes, protocols) and their interconnections within a jurisdiction, geographic area, or particular sector.
Identity lifecycle:	The process of registering, issuing, and managing personal identities, including collecting identity data, validation through identity proofing and deduplication, issuing credentials, verification and authentication for transactions and updating and revoking identities and credentials.
Interoperability:	The ability of different functional units to communicate, execute programmes or transfer data in a manner that requires the user to have little knowledge of those functional units.
Unique Identification Number:	It is a number that uniquely identifies a person - i.e., each person only has one UIN and no two people share the same UIN.
Source:	World Bank ID4D Practitioner's Guide 2019

Executive Summary

Africa is experiencing a rapid growth in the development of intermediate digital infrastructure, including digital identification systems, digital payment systems and wider e-governance systems. The development of digital identification systems is high on the policy agenda for the African Union (AU) and its member states. Digital identity or e-ID allows people to identify themselves when transacting, ensures that services are accessed and delivered to the right person, enables and improves governments' service delivery, ensures access to digital services, and has the potential to support inclusive economic growth and participation in the African Continental Free Trade Area (AfCFTA). There are more than 35 African countries in the process of developing and improving their foundational legal identification and national ID systems to address the identification gap. Currently, 500 million people in Sub-Saharan Africa (SSA) do not have any form of foundational legal identification. The rollout of digital ID systems which rely on foundational legal identification is likely to increase this identification gap. Furthermore, low levels of internet coverage, high cost of internet access, and low levels of digital literacy can also prevent minority groups, refugees, internally displaced persons, women, persons with disabilities, elderly people and poor people from accessing digital ID technologies.

The operationalisation of the AfCFTA, with its aim to increase cross-border trade and develop a single digital market in Africa, is motivating African countries to mobilise in developing continental interoperable digital systems. The AU's new framework on digital ID interoperability aims to guide member states in designing interoperable cross-border digital ID systems (AU Digital ID Interoperability Framework). There are several regional initiatives focusing on the interoperability of digital ID systems. The Smart Africa Alliance spearheaded a digital ID project that led to the development of a Blueprint on Digital ID which provides a governance structure and framework of principles, procedures and technical standards to build trusted digital ID systems. Other regional programmes promoting the interoperability and mutual recognition of foundational ID for cross border movement of people include the West Africa Unique Identification for Regional Integration (WURI) programme and the National Corridor Integration Project in the East African Community. These projects are still in their nascent stages, so it is not yet certain if they will be successful. However, signs already suggest possible compatibility concerns due to the application and use of different technical standards and software across the continent.

There is also a tendency across Africa to prioritise the development of biometric databases and digital ID systems instead of first updating identity laws and establishing robust data governance frameworks such as data protection and cybersecurity laws. Yet such laws are essential as they provide guidelines on how digital ID should be processed, the security measures that must be in place to protect and secure digital ID, allowing holders of digital ID to exercise certain rights over how their data is processed, and mandating data regulators to enforce compliance. There are more than 30 African countries that have regulations on civil registration that put emphasis on identity Acts (including Eswatini, Lesotho, Mauritius, Tanzania, Somalia, Rwanda, and Ghana). Kenya and Ethiopia seem to be the only countries that have drafted a policy document specific for their digital ID systems; the 'Huduma Bill' and the 'Digital ID Proclamation' respectively (see Table 1 for more information). The majority of identity laws in Africa do not respond to the challenges brought by the use of technology, although the development of digital ID systems relies on these regulatory frameworks. Though there have been improvements in the protection of personal data through the promulgation of national laws and ratification of the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), Africa's digital ID ecosystem is still likely to face challenges due to limitations on implementation and enforcement of data protection laws. Of the 36 countries with data protection laws, some have set up data protection regulators to oversee and monitor compliance and attend to grievances from data subjects, while others have yet to set up these enforcement bodies. In this sense, digital ID systems are being enrolled in the absence of a regulatory watchdog to ensure that all processing activities align with data protection principles.

African governments are receiving support from different actors to develop their digital ID systems. The support ranges from financial to technical assistance at national, regional and international levels. The main actors working across Sub-Saharan Africa include international institutions, private foundations and private sector actors. These include the World Bank, United Nations High Commissioner for Refugees (UNHCR), United Nations Development Programme (UNDP), United Nations International Children's Emergency Fund (UNICEF), International Organisation for Migration (IOM), African Development Bank (AfDB), European Investment Bank (EIB), European Union (EU), United States Agency for International Development (USAID), Bill and Melinda Gates Foundation, Omidyar Network, Global System for Mobile Communications Association (GMSA), Idemia, Thales and Gemalto (recently acquired by Thales). Digital ID projects are mainly framed as important for economic development, and in some instances, governments fail to link the benefits of digital ID with human rights and address some fundamental questions about the purpose of such systems. As a result, there has been pushback from several civil society organisations (CSOs) that have raised serious concerns that developmental actors and donors are funding digital ID programmes which offer very minimal, ill-defined and poorly documented benefits to the majority of people while only a group of companies and security-minded governments benefit.

In this study, we looked at five case studies - South Africa, Kenya, Nigeria, Namibia, and Benin - to identify the opportunities and challenges of implementing e-ID systems in different country contexts. The selection criteria include countries deploying different technological solutions to support the rollout of digital ID (for example, MOSIP, X-Road), population size, role in leading and participating in regional digital ID frameworks (SATA, WURI, et cetera), as well as impact of the e-ID system on human rights. **South Africa's** identity coverage is near universal and the country has made great strides in modernising its identification systems and introducing the Smart ID card. The Department of Home Affairs has integrated its systems with other departments and some private firms, and there are ongoing efforts to introduce a new digital ID system. It is also one of the few African countries revamping its identification laws to create a regulatory basis for digital management systems and has a data protection law which is fully operational. The challenges with the procurement of services related to its biometric database provide insights to other governments on the importance of clear and transparent processes when procuring software. **Kenya** is a global leader in the development of mobile money and increasing rates of financial inclusion, but the country does not have a comprehensive digital identification system yet. Kenya's digital ID journey provides key lessons for other African countries as it points to the importance of data protection and public consultations before governments launch digital ID projects. In 2021, the court ordered the government to suspend the issuance of Huduma ID cards pending the Data Protection Impact Assessment (DPIA) in line with Section 31 of the Kenyan Data Protection Act (KDPA). The new Kenyan Government is planning to replace the 'Huduma Namba' with a Unique Personal Identifier (UPI) which will register births and deaths and serve as a digital ID to access government services (including the Kenya Revenue Authority, the National Social Security Fund, or the National Hospital Insurance Fund) through the e-citizen digital platform.

After a decade of trial and error, **Nigeria** is making efforts to issue a National Identification Number (NIN), but a more sustainable approach is needed to prevent the ID programme from becoming an ongoing financial drain on the country's coffers. The sharing of identity-related data is particularly hampered by the existence of silo identity databases that are maintained by about 13 government agencies and other critical organisations in Nigeria. The development of a digital ID system in **Namibia** is still in its embryonic stages but is growing at a relatively fast pace due to demonstrated political commitment by involved stakeholders. With the support of Estonia, Namibia implemented its interoperability solution dubbed 'NAM-X' which made it possible to develop e-services and for its public sector institutions to exchange data securely. In 2021, the President of Namibia launched a 'New Look' ID card which is a form of secure digital ID card to be used to access services. Our last case study looks at **Benin**, which is one of Africa's front-runners on regulation, that adopted a data protection law in 2009 and is leading the Smart Africa Blueprint on Digital Identity, as well as leading the implementation of the World Bank-funded WURI project.

The experiences of these five countries in developing national digital ID systems show that many countries are struggling to ensure transparency, strong oversight, certainty over data protection regulation and its enforcement, effective participation of CSOs in the design and implementation of such systems and finally, setting up financing models for more operationally and financially sustainable ID systems.

In the last section of our paper, we provide policy recommendations for African policymakers, and the European Union and its member states. We argue that African governments need to develop strong regulatory and operational frameworks as well as robust data protection mechanisms by revising and updating their identity laws to accommodate the registration, issuance and management of digital IDs. The AU could establish a Specialised Technical Committee on Digital ID (STC-Digital ID) which can provide minimum standards on technical, operational and legal requirements in support of the AU Interoperability Framework. Since the research uncovered the reluctance of people to adopt and use digital ID, we recommend that governments need to improve public trust in government services by adopting and promoting transparency, privacy and data protection. This can be achieved through digital ID pilot programmes demonstrating how digital ID empowers individuals and enhances their access to services, and by actively promoting meaningful public participation through public consultation/collaboration with all key stakeholders including CSOs. As a global standards setter and one of Africa's international partners with strong experience in developing DPGs in the context of its own quest towards interoperable public services across its digital single market, the EU can be a key partner for African governments and the AU. The EU can do this by sharing its experiences in developing regulatory standards for its interoperable digital ID systems and reforming the electronic identification and trust services (eIDAS) digital ID wallet with its African partners. The EU can improve its understanding of the different contexts in which e-ID systems are being developed across Africa and work with African actors to develop context-based solutions through supporting pilot projects or sandboxes which can be scaled up as use cases. Additionally, the EU can continue to support African countries to develop data protection frameworks in line with their national laws and continental frameworks. Finally, while promoting a comprehensive approach to digital ID in partner countries, it is essential to ensure the sustainability of digital ID systems. This can be achieved through supporting digital skills programmes aimed at empowering African government officials, businesses, CSOs, as well as citizens.

1. Introduction

Having a form of legal identification is a basic human right enshrined in the United Nations Declaration of Human Rights (Article 6) and the International Covenant on Civil and Political Rights (Article 16) (UN n.d.-a; OHCHR n.d.). There is an urgency for governments to make sure that everyone has a legal identification as a way of promoting inclusive and sustainable development (Sustainable Development Goal 16.9). Identity allows people to participate in the economy, access various services, improve their well-being, and participate in political processes. Individuals are required to identify themselves and provide supporting evidence of who they are in the form of an identity document (a national identity, birth certificate, voter card, passport, or driving licence). Furthermore, as we progress in the Fourth Industrial Revolution,[1] most transactions and services are being offered via digital platforms. A traditional identity document may not always be fit for purpose for many of these digital transactions, and instead, a digital proof of identity may be required. A digital form of identification or digital ID ensures that services are accessed and delivered to the right person (Atick 2016). The rapid digital transition to online public and private services has resulted in growing demand for efficient and user-centric digital ID systems so that people can identify themselves when transacting.

Unfortunately, about 500 million people still live without any form of foundational legal identification in SSA (WB 2019a). One of the cited reasons for this is the lack of comprehensive Civil Registration and Vital Statistics (CRVS) systems. Since most digital ID systems are based on foundational legal identity, the challenges in obtaining foundational legal identity are replicated in digital ID systems, resulting in marginalised groups[2] being further excluded and severely disadvantaged in the adoption of digital ID. The slow adoption of digital ID systems in Africa is attributed to several challenges linked to the level of digital transformation across the continent, the absence of enabling policy and legal environment, lack of policy coherence, policy interoperability and digital skills gaps. These challenges are clearly articulated in the AU Digital Transformation Strategy and have the potential to amplify the identity exclusion gap and inhibit the faster adoption of digital ID.

This paper analyses the development and adoption of government-issued digital identity systems across Africa, arguing that ultimately each country must carefully calibrate the design and implementation of its digital ID system to match its specific context and to meet the many challenges that such systems present, particularly in African contexts. In the first section, the paper looks at the overall status of digital ID adoption in Africa, tracking the stages of implementation of digital ID, and looking at some of the challenges that African countries face in adopting digital ID systems, including making systems inclusive, ensuring the correct legal and policy environment, interoperability and the role of third-party actors, including donors and private sector actors. In the second section, the paper uses five case studies to identify the internal and external factors that are motivating the adoption of digital ID in African countries, the varying interests of different stakeholders and how these are shaping the development of interoperable foundational ID systems in Africa. It focuses on five case studies – Benin, Kenya, Namibia, Nigeria, and South Africa – and gives a detailed analysis of the development and state of digital ID in these countries. Finally, it highlights actionable recommendations for African and European policymakers citing the opportunities for further AU-EU cooperation and partnerships in this area.

To conduct this research, we relied on qualitative research methods. Through desk research, we examined the legislative instruments and policy documents shaping identity and digital ID frameworks. We complemented this by conducting several interviews with representatives from government, civil society, academia, the private sector, and data regulators from both Africa and Europe.

[1] Klaus Schwab defines the Fourth Industrial Revolution as the digital revolution characterised by the fusion of technologies cross-cutting physical, digital and biological spheres (Schwab 2016).

[2] These groups include women, children, migrants, poor people, disabled and the elderly.

2. Digital ID Systems in Sub-Saharan Africa: State of play

Across SSA, governments are embracing the development of digital ID systems with the aim of achieving universal ID coverage and legal identity for all by 2030 in line with Agenda 2063: The Africa We Want and the UN Sustainable Development Goals (SDGs) (AUC 2015). The development of robust digital ID systems is high on the policy agenda for the AU and its member states due to the important role that digital ID plays in accelerating digital transformation in general and in particular in expanding the data economy and service delivery. Compared to a decade ago, Africa is experiencing a steady growth in digital ID infrastructure (GSMA 2022). According to the AU, nearly 85% of African countries have national ID systems underpinned by an electronic database and more than 70% of African countries collect biometric data to ensure the uniqueness of identities (AU Interoperability Framework; see Table 1). Indeed, African governments are making efforts to make sure that every citizen has a digital ID to access e-government services, participate in e-commerce, access digital financial solutions, travel to other countries and fully participate in the digital economy. Although the main reasons to develop digital ID systems are to meet developmental and policy goals and to enhance administrative efficiency in providing e-government services, governments also implement these systems to reduce identity fraud committed by individuals and businesses,[3] to improve national security and to achieve political advantage during electoral processes (Razzano 2021a; AUC 2015).

African governments and digital actors' efforts at providing digital ID to African citizens take different forms. For example, countries like Angola, Lesotho, Mauritius, and Kenya among others are modernising their foundational identification systems to make them fit for purpose. While these countries have been rapid in developing their digital ID systems, Angola still needs to digitalise its civil registry and link the e-ID with social services, while Lesotho, Mauritius, and Kenya's digital ID systems have raised issues around security and privacy rights and therefore are still being developed. Other countries such as Madagascar, Ethiopia, Zambia, or Mozambique are in the piloting process. The remaining few countries including Eswatini, Zimbabwe, Tanzania, or Togo are still considering implementing national digital ID systems (see Table 1). Regardless of what stage they are at, the majority of African countries are in the process of improving the legal environment for the regulation of digital ID systems including strengthening data protection laws. At a regional level, the Economic Community of West African States (ECOWAS) is piloting a regional interoperable digital ID to facilitate the seamless movement of people, goods and services in the region, and continentally, the AU is developing a continental Digital ID Interoperability Framework.

In recent years, African governments have been increasingly attracting investments in digital infrastructure including digital ID systems by promoting the ICT sector as a key pillar of their national development strategies. However, it was the COVID-19 pandemic that accelerated the development and modernisation of African digital ID systems, because it underscored the importance of digital identification to improve government service delivery (see Table 1). Governments with strong data processing and a national identification system were able to rapidly identify communities in need of social protection schemes, helping to lessen the economic and health impact on individuals' lives. For instance, Togo was able to target social payments using a newly built digital cash payments system, NOVISSI, and integrate an AI-targeting approach (Chowdhury et al. 2022), while South Africa's Social Security Agency (SASSA) struggled to process new benefit claims because it was difficult to cross-check the eligibility of applicants across other databases like the unemployment insurance fund (Razzano 2020). However, despite the potential of digital ID systems to support better rollout of government services and catalyse economic growth, poorly designed digital identification systems can generate a number of risks which have a special impact on vulnerable and already disadvantaged groups.

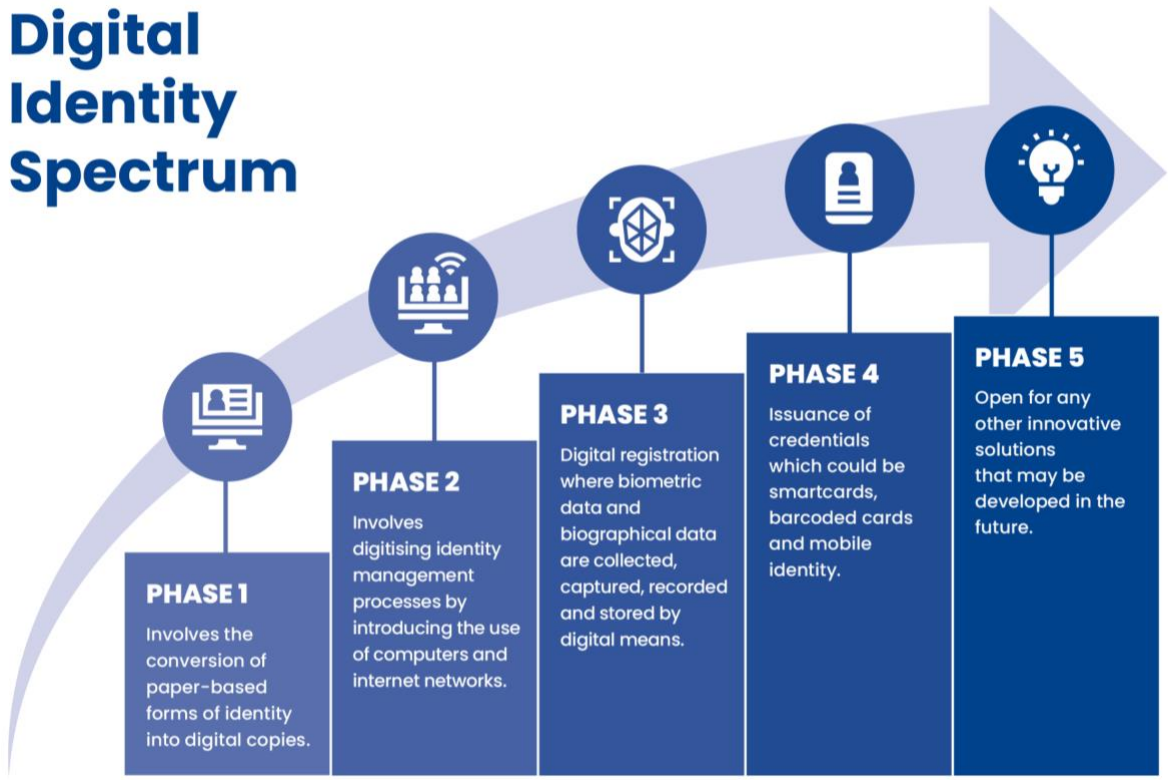
[3] The Nigerian government was able to identify and remove 62,000 ghost workers by using digital ID (Hutchinson et al. 2019). The government of Zimbabwe was able to remove 10,000 ghost workers by deploying a biometric verification system for civil servants (Burt 2020).

2.1. Stages of implementation of digital ID systems

The approach to digital ID adopted by African governments, as well as the private sector, is influencing the types of policy interventions being adopted. Digital ID can be issued by governments (like a UIN on a Smart-ID card) or it can be issued by the private sector (for example, banks and insurance companies) or it is a form of identity that is built based on one's digital footprint or the digital personae that an individual portrays about themselves through social media (Sullivan 2011). These broad definitions create a '*Digital Identity Spectrum*' within the digital ID ecosystem.

The first stage of this Digital Identity Spectrum involves the conversion of paper-based forms of identity into digital copies. The second stage is digitising identity management processes by introducing the use of computers and internet networks. The third stage is digital registration where biometric data and biographical data are collected, captured, recorded and stored by digital means. The fourth stage is the issuance of credentials which could be smartcards, barcoded cards and mobile identity. The fifth stage is open to any other innovative solutions that may be developed in the future. Because of the different stages or phases of the Digital Identity Spectrum, we found that stakeholders' understanding of digital ID was influenced by the stage at which their country was on the spectrum. This may be challenging for African policymakers tasked with developing minimum standards and requirements for cohesive approaches to digital ID as countries have different priorities and needs depending on where they stand along the Digital Identity Spectrum.

Figure 1: Digital Identity Spectrum



Source: ECDPM

Countries that have reached stage 4 of the Digital Identity Spectrum and issuing digital ID credentials also show differences in the types of digital ID credentials they issue and the transactional capabilities of their digital ID. Digital ID attributes are determined by the type of identity system (foundational or functional) in a country (GSM2016) as well as the stage of technology uptake in the public sector. Some countries issue digital ID credentials in the form of smartcards while others issue a digital ID number which can be used for transactions. Ethiopia issues a unique Fayda Digital ID Number and a person has the option to get a physical copy of the Fayda Digital ID printed in the form of a card or keep a mobile token (Government of Ethiopia n.d.).

Countries undergoing the early stages of digital transformation of their public sector have negligible e-government services and restrict the use of digital IDs for identification purposes (Atick 2016). Other countries are linking their digital ID with service delivery, making it possible for individuals to access public and private e-services. In Nigeria, one can use a digital ID card as a payment solution, while South Africa's Smart ID Card currently has no transactional capabilities. Countries implementing functional digital ID systems and designing digital ID with transactional capabilities attract private sector stakeholders who see opportunities to develop solutions and products which rely on digital ID such as mobile wallets, tokens and applications which can be used by individuals to access services.

The Digital Identity Spectrum also influences policy decisions across different government departments. Because the registration of citizens for digital ID is not decentralised, some government departments are still in the early stages of the spectrum while others have been using digital ID credentials for a while (this is the case for Angola, Kenya, Comoros, Eswatini, and Lesotho, see Table 1 for more information). Similarly, the private sector is also technologically advanced and their understanding of digital ID is more on solutions relating to digital credentialing, authentication and verification.

The Digital Identity Spectrum is a reflection of the uneven digital transformation across Africa, and in particular, of e-governance levels. While African governments are advancing towards wide implementation of digital identification systems, without a clear leadership that can stir the political and technical exchange between different digital actors, the process is likely to remain a patchwork with important technological and legal gaps. On the other hand, countries that are already at the fourth stage of the Digital Identity Spectrum should create partnerships with less advanced countries to share lessons learned, for example how to improve issues around inclusivity and promote regulation of digital technologies while allowing technological innovation in the digital ID ecosystem. The implementation of digital ID systems and support to other countries in this area might also encourage governments to link their development and geopolitical objectives.

2.2. Inclusiveness: The challenges of universal coverage

Research shows that digital identification can accelerate inclusive development when it is intentionally designed to be more inclusive, user-friendly, and protective of people's rights and data through the development of new standards, models and tools to exercise personal oversight and control over how data is used (WB 2021a). While many African governments are already recording remarkable strides toward establishing robust ID systems to support meeting the development goals under the Agenda 2063, there are different challenges to achieving universal coverage.

First, internet use in Africa has grown rapidly thanks to the increase in investment for digital infrastructure by the private sector and international donors, but the continent has yet to realise its full digital potential. According to 2022 figures, there are over 570 million internet users in Africa, with Nigeria having the highest share of users, followed by Egypt and South Africa (Statista 2023a). While improved cellular infrastructure and rising mobile device penetration have increased internet access throughout Africa in recent years, the internet penetration rate still

stands at approximately 43%, well below the global average of 64% (Statista 2023b). This means that setting up ID registration centres in rural areas – where only 23% of people use the internet – is a big challenge (ITU n.d.; Statista 2023c; Jaiyeola 2022). This sort of digital divide limits the options for connecting central identification offices usually located in urban centres and registration units in rural areas, thereby forcing people in rural areas to travel long distances to get registered. Furthermore, many countries, such as Botswana, Cameroon, Liberia, and Sierra Leone experience slow, expensive and poor internet connections, while electricity is expensive in other countries, such as Nigeria and Namibia, and power cuts and load shedding are prevalent in countries such as South Africa and Zimbabwe. To address the digital divide, the AU and member states, in partnership with the private sector and international partners, have developed different continental and national interventions and strategies aimed at addressing the investment gap in hard and soft digital infrastructure.

Second, women face more difficulty accessing identification credentials than men. According to the World Bank, over 45% of women lack foundational ID in low-income countries. In Nigeria for example, out of 101 million registered persons as of the first quarter of 2023, only 44% are women and girls (Desai et al. 2018; Egole 2023). Similarly, in Burkina Faso, a survey collecting data from 400 villages indicated that 71-91% of women do not own or have not renewed their national identity cards (Tanager 2023). In Malawi, on the other hand, 53% of the registered adults are female (Malik 2020). Nevertheless, despite high proportions of female registration, women are less likely than men to adopt and use identity. Constraining factors have been identified to include but not limited to illiteracy, transportation cost, gender, and social norms (GSMA 2019; Jarrahi 2021). In Benin, Cameroon, Congo, Mauritius, Namibia, and Egypt, married women cannot apply for national ID cards, unless they are granted permission from their spouses (SIHMA 2023). Because digital ID systems form the cornerstone for service delivery, if marginalised groups and women do not have access to identification documents they cannot participate in society and reap the benefits of the technological innovation in their societies.

Third, refugees and Internally Displaced Persons (IDPs) in Africa find it difficult to get identification, including digital ID. Cameroon, Senegal, Mali, and Rwanda, are just a handful of countries that have managed to issue a limited number of refugee IDs (Aljazeera 2022). A group of NGOs previously sued the government of Uganda, claiming that vulnerable groups were refused potentially life-saving assistance owing to inadequacies in the country's biometric ID system. The court was asked by these NGOs to rule that sole dependence on the national identification system to access social safety net programmes and health care services is not only discriminatory and exclusionary but also breaches citizens' human rights. This impasse has led to a groundswell of voices now advocating for the government to enforce alternate forms of identification and to put policies in place to deal with the difficulties encountered in the country’s digital ID roll-out (Aparo 2023). In 2017, UN refugee agency officials disclosed that there are 1.8 million IDPs in Nigeria. The UNHCR commenced the registration and issuance of e-ID cards to 100,000 IDPs in Nigeria in collaboration with the National Identity Management Commission (NIMC) (NAN 2017). Six years after the pilot phase, not much has changed.

Finally, nearly half a billion African citizens do not have a foundational form of identity, which puts them at risk of being excluded from vital services (Theodorou 2022). In many African countries, registration regulation requires people to present some form of supporting document before they can be registered for digital identification. For example, the Nigerian Government has a list of 18 supporting documents from which an applicant must present at least one before registration is carried out, but many still show up at the registration centre without possessing any of these documents, not even a birth certificate. There are approximately 96 million unregistered children in Africa, with Zambia (12%), Chad (16%), and Tanzania (16%) recording the lowest birth registration rate on the continent (UNICEF 2020; WB 2017a). The low registration levels across Africa and in particular in SSA, indicate the level of risk of exclusion that many people face as registration to digital identification is linked with access to government services.

A broad look at African countries' experience in developing digital ID systems shows that early adopters of digital ID systems are still struggling with issues around inclusion and universal coverage due to scoring low in the mentioned categories. In this sense, Kenya and Niger offer very drastic examples in which governments have aimed to adopt new digital ID systems (more advanced systems) to address issues around exclusion and costs respectively. While challenges around the digital divide can be addressed through increasing investment in digital infrastructure to improve access and affordability of digital tools, challenges linked to social norms as well as identity are political issues that need time and dedicated debates to find pragmatic solutions. Civil society organisations worldwide have raised concerns about the rapid roll-out of digital ID systems and its impact on human rights. In September 2022, more than 70 activists, academics and CSOs wrote open letters to the World Bank's ID4D initiative, which is the main international actor encouraging and funding the rapid roll-out of digital ID systems globally, raising their concerns about the initiative's impact on human rights, exclusion, exploitation and surveillance, and called for digital ID providers to review the digital ID systems in regards to improve their transparency and strengthen engagement with civil society in the design and implementation of such systems (Access Now 2022; CHRGJ 2022).

2.3. Creating a legal and policy environment for e-ID systems

The data-centric nature of digital ID and its privacy and security risks, point to the need to have robust data governance frameworks, especially data protection laws. Data protection laws add a layer of trust and security in digital ID ecosystems. These laws provide guidelines on how personal data should be governed, as well as how data is collected, stored, and used, the security measures that must be in place to protect and secure personal data, allowing holders of digital ID to exercise certain rights over how their data is processed, and mandating data regulators to enforce compliance. However, there is a tendency across Africa to prioritise the development of biometric databases and digital ID systems instead of first establishing robust data governance frameworks such as data protection and cybersecurity laws. Though paper and ink-based identity systems collect biometric data, electronic systems differ significantly. They encompass a broader range of data types from one thumbprint to ten fingerprints and palm prints, from a paper-based photo to facial biometrics, iris scans and voice biometrics. Digital ID systems also utilise artificial intelligence technologies like facial and voice recognition, and use of data analytics to extract value from databases. The collection and storage of high volumes of data in the context of poor data protection legislation as well as cybersecurity and cybercrime strategies in several African countries renders citizens' personal data at risk of exploitation, surveillance, as well as fraud.

There is a trend among telecommunications operators to collect biometric data of users registering SIM cards, with some legally mandated to capture biometric data (in countries like Tanzania, Nigeria, and Zambia), while others capture data for their own legitimate interests like user security and fraud prevention (TCRA 2020; NIMC 2021; Endjala 2023; Privacy International 2019). Biometric collection by both the public and private sector is alarming due to the privacy and security concerns of misuse of biometric data, particularly the use of facial recognition technology (in countries like Uganda, Tanzania, and Zimbabwe - see Table 1) to track and target government critics, especially during election seasons (Paradigm Initiative 2022).

A significant number of regulatory frameworks on foundational ID and identity management systems across Sub-Saharan Africa were promulgated and implemented before the beginning of the digital revolution, which meant that many did not respond to the challenges brought by digital technologies and are thereby outdated. As part of a broad trend to upgrade their identity management and civil registration systems using modern technologies, some countries are thus focused on modernising their identity systems based on laws that interpret identity from social and political perspectives. However, this approach is likely to exacerbate inequalities under a new digital ID system (for example, Zambia and Zimbabwe - see Table 1 for the complete list of identity laws across SSA). While some countries are amending specific provisions of existing identity laws (Botswana, and Madagascar) others are

committed to a complete overhaul of identity laws (Malawi, Lesotho, Namibia, and South Africa). The regulatory changes in identity laws are mainly focused on putting in place the right framework for the creation of an electronic system for the collection and storage of biometric data, and ensuring that identity frameworks are trusted, secure and inclusive. This is achieved by also introducing data protection and cybersecurity laws.

The African Union Convention on Cyber Security and Personal Data Protection (**Malabo Convention**) came into force in June 2023, 30 days after Mauritania submitted the 15th ratification instrument and 9 years after its adoption by the African Union Assembly (AU 2014). Its four broad themes (electronic commerce, data protection, cybersecurity, and cybercrime) address different aspects of digital ID, making it an important legal instrument for the successful adoption of digital ID across the continent. It also sets out obligations for data controllers, and the rights of data subjects, and encourages member states to develop national data protection laws and promote the free flow of personal data. The Malabo Convention boosts trust in digital ID by encouraging member states to develop policies, strategies and frameworks on the protection of critical cyber infrastructure[4] (like foundational digital ID databases), and criminalising conduct which affects the confidentiality, integrity and availability of information, communication technology systems, the data they process and the underlying network infrastructure (see Section 3). However, the continental convention is not sufficient to warrant an effective data protection regime in Africa. Though the convention is operational in the countries which ratified it, these countries need to implement the convention at a national level.[5] Concerns have also been raised on the convention being too broad, inconsistent, vague, outdated and omitting some important fundamental definitions like 'pseudonymisation' and there have been calls to supplement these gaps (Ndemo et al. 2023; ALT Advisory 2022).

At present, 36 African countries have data protection laws, and 3 are working on their draft legislation, which leaves identity management systems in the remaining 15 countries vulnerable to unclear, opaque and possibly unlawful processing activities (Domingo and Tadesse Shiferaw 2022). Of the 36 countries that have data protection laws, some have set up data protection regulators to oversee and monitor compliance and attend to grievances from data subjects, while some have yet to set up these enforcement bodies. Some have also pointed out that the major hurdle for African countries is the implementation of these data protection laws. Organisations such as the Network of African Data Protection Regulators (NADPA) can play a crucial role in the implementation process by developing regulatory guidelines on specific processing activities, such as the use of facial recognition in digital ID systems (Musoni 2023).

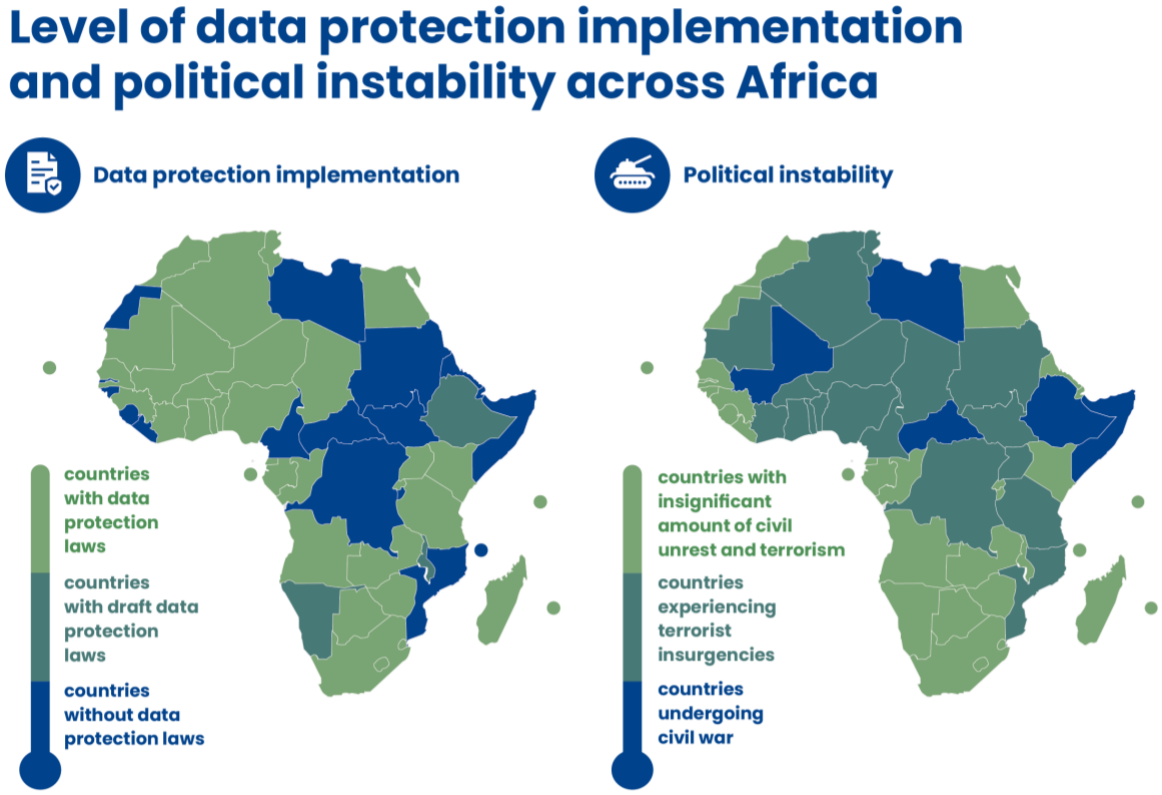
Beyond encouraging the remaining 15 African countries[6] to develop and adopt data protection laws, regional and continental policymakers should look into the underlying factors inhibiting the quicker adoption of such laws. These include disinterest by governments to develop laws which restrict their control over citizens, lack of resources (financial, human and technical) and multi-crisis (natural disasters, floods, civil unrest, war, and economic instability) that the remaining countries are facing (Kakaire 2022; Gagliardone and Stremlau 2022). The contribution of political instability to the slow adoption of data protection laws should also be considered, as African countries which have faced political instability and terrorism have delayed the adoption of data protection laws.

[4] Critical cyber infrastructure is defined as the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace.

[5] At present, Namibia and Mozambique do not have national data protection laws, while Cape Verde's 2001 law is still not operational (Data Protection Africa n.d.).

[6] At the time of writing, Namibia, Ethiopia and Malawi had drafted data protection bills. But Mozambique, Comoros, Somalia, South Sudan, Sudan, Central African Republic, Cameroon, Libya, Liberia, Sierra Leone, Guinea-Bissau, The Gambia, Western Sahara, Burundi, and Eritrea have no data protection frameworks in place.

Figure 2: Level of data protection implementation and political instability across Africa[7]



Source: ECDPM

There is a correlation between peace, security and development of data protection laws. On the data protection heat map, countries highlighted in blue presently do not have data protection laws. On the political instability heatmap, countries highlighted in blue and dark green are going through different forms of political instability. A comparison of the two heat maps shows an overlap between countries which have been experiencing war, political instability and terrorism and countries without data protection laws. This can be one explanation why it is taking longer for these countries to develop their own data protection frameworks.

While there may be a relationship between political instability and the slower development of data protection laws, it is essential to approach such connections cautiously. Political instability and conflicts might indeed hinder the development and implementation of legal frameworks, including data protection laws. Countries undergoing conflict may prioritise immediate security and stability over long-term regulatory frameworks. However, while there might be an overlap in the heat maps, the correlation doesn't necessarily imply causation as the reasons for delayed data protection frameworks in these regions could be multifaceted. For instance, instability might divert attention and resources away from legislative development. Moreover, the process of establishing data protection laws involves complexities beyond immediate stability concerns, such as technological infrastructure, capacity building, and public awareness. While the correlation is interesting, a deeper analysis would be needed to definitively establish the causative relationship between political instability and lack of data protection laws.

Regional Economic Communities in particular can play a more active role in encouraging their member states to adopt national data protection laws and be guided by respective regional data protection instruments (for example,

[7] To develop the infographic, the authors consulted the data from the Data Protection Africa initiative by ALT Advisory.

the SADC Model law on Data Protection). For instance, the EAC has a non-binding data privacy framework and while the region faces challenges when implementing regional regulations at national level, it has urged its member states to upgrade their national policies on data protection and privacy to facilitate the integration of digital markets and the creation of a Single Digital Market for East Africa (Domingo et al. 2023). Although there is an increase in uptake of e-commerce laws in recent years, laws which recognise digital signatures are also sparse across the African continent. The current legal landscape in Africa shows that there is still a long way for digital ID to be comprehensively protected across the continent's free trade area and Digital Single Market (DSM).

Holding e-ID institutions accountable

Existing legal frameworks in African countries provide operational mandates and assign specific responsibilities to institutions responsible for identity and identity management. These institutions either operate as autonomous and independent agencies governed by a board representing different stakeholders (for example, in Ghana and Nigeria) or they are an agency or directorate operating within an existing ministry or department (for example, Botswana, Namibia, and Rwanda). The challenge with identity documents is that they are highly politicised because of the link to certain rights such as voting, resulting in ID institutions potentially being used as political tools to advance certain political interests (WB 2019b).

In the absence of clear rules on the governance of data, the digital ID system can be politicised and incumbent governments can make unilateral decisions over who can have access to the data, what they can do with it and who they can share it with. This is why it is imperative to have independent regulators exercising oversight. Unfortunately, the majority of identity laws in Africa do not make provision for an independent oversight body to monitor ID institutions. As the number of African countries developing and implementing data protection laws increases, people have the confidence that data regulators can be the avenues for clear oversight over digital ID systems. The question in many African countries remains as to whether these data regulators or commissioners enjoy genuine independence when carrying out their legal mandate. Factors such as the allocation of financial resources, political influence, the composition of such authorities, and how the members are appointed can potentially influence the level of independence and impartiality of the regulators (Paradigm Initiative 2021).

The danger of biased regulators is that they may not be able to enforce compliance by ID institutions or any other powerful or influential stakeholders involved in the provision of ID management services. Some data regulators have set a good precedent on compliance (for example, Kenya's Data Protection Commissioner going after big tech harvesting biometric data) and made tough and significant decisions (such as South Africa's Information Regulator going after big pharma and the department that it is housed under) (Musoni 2023; CA 2023; Information Regulator [South Africa] 2023). These success stories can be an inspiration to motivate regulators across the continent to remain impartial and for other countries to establish independent data authorities in line with the Malabo Convention.

Table 1: State of digital ID implementation in Africa

Country	e-ID regulation	Governing authority	Data protection	Digital ID system	Type of ID platform	International Partners
Implementation of e-ID systems in the SADC						
Angola	Civil registration Code (1967)	The National Directorate for Identification, Registries and Notaries	Personal Data Protection (2011)	Issues e-ID	HID Global and DGM partnership	EXIM Bank, ANY Security Printing (Hungary), The UAE

Botswana	The National Registration Act (1986).	The Department of Civil and National Registration	Data Protection Act (2018)	Started project on e-ID cards for travelling	X-road	EU, Veridos (Germany) Morpho South Africa
Comoros	Law on Civil Status (1984)			Very early stage		World Bank, IFC, UNDP, AUDA-NEPAD
Eswatini	Identification Order (1998)	Ministry of Home Affairs	Data Protection Act Computer Crime and Cybercrime Act (2022)			Central Bank, World Bank
Lesotho	National Identity Cards Act (2011)	The Department of National Identity and Civil Registry - Ministry of Home Affairs	Data Protection Act (2012)	Advanced-working on interoperability		World Bank, GovStack
Madagascar	The Malagasy Nationality Code	The Ministry of the Interior	Protection of Personal Data Act (promulgated in 2014)	Modernising	MOSIP	World Bank, Indian and Lithuanian companies, UNICEF GIZ
Malawi	National Registration Act (2010)	The National Registration Bureau	Draft Data Protection Bill (2021)	Started ID project in 2017		UNDP, UK Aid, Irish Aid, USAID, the EU, Norway
Mauritius	National Identity Act (1985)	Civil Status division - Prime Minister's Office	Data Protection Act (2017)	Modernising - Launch of ID system in 2013		
Mozambique	The Civil Registration Code (2004)	The Ministry of Justice and Ministry of Home Affairs		Early stages		World Bank, Simprints (UK), BioRugged (South Africa), Muhlbauer (Germany)
Seychelles	Civil Status Act and the Civil Code	The Immigration and Civil Status Department	Draft Data Protection Bill 2023	Early stages		World Bank, Swiss company A French company
Zambia	The National Registration Act (1964)	The Chief Registrar	Data Protection Act (2021)	Early stages - project on e-ID started in 2022		World Bank

Zimbabwe	The National Registration Act (1976)	The Registrar-General of National Registration	Data Protection Act (2021)			Mulk International (UAE), CloudWalk Technology (China)
Implementation of e-ID systems in the East Africa region						
Tanzania	The Registration and identification of Persons Act (1986)	The National Identification Authority (NIDA)	Personal Data Protection Act (2022)	Planning stage		Too early to know
Ethiopia	The Digital ID Proclamation (2022)	The National Identification Programme (NIDP)	Personal Data Protection Proclamation - not approved yet	Advanced phase- scaling up project	MOSIP	World Bank, UNECA
Somalia	Identification and Public Registration (2023)	The National Identification and Registration Authority	Public Data Protection Act (2023)	Launched national ID system in 2023		GovStack, Government of Pakistan (Pakistan's National Database and Registration Authority)
Rwanda	Law on Registration of the Population and Issuance of the National Identity Card (2008)	The National ID Agency	Data Protection Law (2021)	Planning stage of Rwandan Single Digital ID system (SDID)		World Bank, AfDB, GovStack
Uganda	Registration of Persons Act (2015)	National Identification and Registration Authority	Data Protection and Privacy Act (2019)	ID programme launched in 2014		Joint Stock Global Security (Russia) (10-year contract)
Sudan	The Civil Registration Act (2011)	The General Directorate for Civil Registration and the General Directorate for Passports and Migration		Introduction of Smart ID card in 2017		
South Sudan	Nationality Act (2011)	Department of Civil, Nationality, Passport and Immigration				UNHCR, IOM, WFP

Eritrea	Eritrean Citizenship Proclamation	Department of Immigration and Nationality		Electronic ID card announced in 2015		
Djibouti						GovStack (discussion)
DRC		The National Identification and Population Office	Digital Code	Re-launched the biometric ID card project in 2023	MOSIP	World Bank, Indemia (France), Thales and Veridos (Germany) competing
Burundi		Ministry of Interior		Tried to develop an e-ID system		
Implementation of e-ID systems in the ECOWAS						
Burkina Faso		The National Identification Office		Rolling out ID project since 2001	MOSIP	World Bank
Cabo Verde		National Civil Identification and Authentication System		ID card implemented in 2014		Caixa Mágica Software. Imprensa Nacional – Casa da Moeda
Côte d'Ivoire		The National Identification Office				Word Bank USAID
Gambia		The Gambia Biometric Identification System		Biometric ID card introduced in 2009		
Ghana	Identification Authority Acts	The National Identification Authority	Data Protection Act	Implementing the Ghana Card Digital ID	Identity Management Systems II Ltd)	
Guinea	Decree 254 of September 1995 and 1998	Guinea election commission and its Ministry of Territorial Administration and Decentralization			MOSIP	
Guinea-Bissau	Nationality Regulation Law (2011)	SEMLEX Ministry of Justice		ID programme was introduced in 2013		UNICEF EU UNHCR Plan International

Liberia	National Identification Registry Act (2011)	Liberian National Identification Registry		ID system is operational since 2011		Word Bank
Mali	NINA Law (2006)	The Ministry of Territorial Administration and Decentralization	Law on the Protection of Personal Data (2013)	Implementing the Mali ID card		
Niger	Decree 64-193/MI (1964)	The Ministry of Interior, Public Safety and Decentralization	Law on the Protection of Personal Data (2017)	Reverted back to paper cards due to cost	MOSIP	
Senegal		The Ministry of Interior and public security	Loi sur la Protection des Données à Caractère Personnel (2008)	An e-ID project was launched in 2022.		UNDP, EU, GovStack
Sierra Leone	The National Civil Registration Act (2016)	The National Civil Registration Authority		Launched a registration system in 2017	MOSIP	UNDP Price Waterhouse Coopers (PwC)
Togo	Decree No. 2003 – 268/PR (2003)	The Directorate General of National Documentation of Togo		The new biometric identification programme is not yet live	MOSIP	The International Institute of Information Technology Bangalore, India

Source: ECDPM

2.4. Interoperability of digital ID systems

Across Africa, there is widespread agreement that digital ID systems should be interoperable to enable the building of 'a secured Digital Single Market in Africa by 2030 where free movement of persons, services and capital is ensured and individuals and businesses can seamlessly access and engage in online activities in line with Africa's Continental Free Trade Area (AfCFTA)'. The operationalisation of the AfCFTA is a motivating factor for improving the interoperability of digital identity systems in Africa. The AU is leading the work on promoting interoperability. The AU Interoperability Framework for Digital ID, once implemented, has the potential to set clear standards and rules on digital ID, making it easier for all African citizens to securely access the public and private services they need, when they need them and independently of their location. The AU has spearheaded the development of a continent-wide digital ID by proposing the development of common requirements, minimum standards and governance mechanisms which can shape digital ID frameworks (AU Interoperability Framework on Digital ID 2022).[8] The

[8] The framework is currently not publicly accessible. A copy of the document was shared with the researchers by the African Union.

objectives of the Digital ID Framework are to allow African citizens to verify their legal identity offline and online to access public and private sector services, empower all African citizens with control over their personal data and strengthen trust and interoperability among foundational identification systems of AU member states. Under this framework, member states have control over how they design their national digital ID systems, but they also enable the recognition of proof of identity across the continent (WB 2021b). This work will be supported by national and regional data protection provisions which promote cross-border data flows as well as the AU Data Policy Framework, which guides African countries in developing open data standards which promote data sharing and ensure that data ecosystems are built on trusted, interoperable digital infrastructure.

However, this demonstrated level of political commitment might be hampered by the traditional challenges of policy implementation at the national level. It is not clear when and how the proposed policy interventions outlined in the Digital ID Framework will be developed and deployed. For Africa to develop an interoperable digital ID system useful for the DSM, standards should be developed and adopted at a continental level. Standards establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices regarding the capture, storage, transmission, and use of legal identity data, as well as the format and features of legal identity credentials and authentication protocols (WB2017b; AU Digital ID Interoperability Framework). This work requires urgent attention and the AU should build up on the Digital ID Framework to develop the relevant technical standards together with specifications.

The Smart Africa Alliance (SAA) initiative, which brings together 39 African heads of state and governments committed to accelerating economic development through ICTs, can be instrumental in developing a harmonised approach to digital ID among like-minded countries. The Smart Africa Blueprint on Digital ID provides a governance structure and framework of principles, procedures and technical standards to build trusted digital ID systems (Smart Africa 2020). The Smart Africa Digital ID Blueprint, which elaboration was led by Benin, proposed the development of the Smart Africa Trust Alliance (SATA) to guide the implementation of the blueprint. What is interesting about SATA is a private-public-partnership that aims to create a framework for developing interoperable digital ID systems within the jurisdiction of Smart Africa Alliance members with a view of creating trust between different governments and ultimately increasing trade. Ghana, Zimbabwe, Gabon, Rwanda, Tunisia, and Guinea signed the SATA during the Transform Africa Summit in early 2023. SATA aims to bring leadership and address the trust barriers hindering the interoperability of digital ID systems, but more awareness campaigns will be needed to explain the added value of SATA in the context of emerging overlapping initiatives including the World Bank's WURI for West African countries, as well as clarifying how the alliance fit within the continental digital interoperability framework.

The United Nations Economic Commission for Africa (UNECA) and its partners[9] also launched the Digital Identity, Digital Trade and Digital Economy (DITE) initiative to promote the adoption of digital ID in Africa (Seck 2023). This initiative established the Center of Excellence on Digital Identity, Trade and Economy[10] to provide technical advice to countries on their digital ID and digital economy while supporting the implementation of minimum standards for digital ID systems to safeguard inclusion, trust, interoperability, and harmonisation of both civil registration and digital ID systems (UNECA n.d.).

Different RECs are also making efforts to make digital ID useful for migration purposes across their respective regions (ECOWAS WURI programme and EAC National Corridor Integration Project promote the recognition of foundational ID as travel documents across the respective regions). The WURI programme, which is funded by the World Bank and implemented by the ECOWAS Secretariat, Benin, Burkina Faso, Niger, Togo, Côte D'Ivoire, and Guinea aims to

[9] Rockefeller Foundation, Omidyar Network, and World Bank.

[10] At the time of writing of this paper, there was not a lot of publicly accessible information on some of the activities being carried out by this centre.

strengthen ECOWAS and its member states' service delivery, as well as connect their national systems. In particular, it allows service providers in West Africa to verify the unique identity of their users while they in turn can authenticate themselves via a QR code (WB 2023a). Countries are also entering into bilateral agreements on cross-border travel (for example, Namibia and Botswana have opened their borders to allow citizens from both countries to travel using their national IDs instead of passports) (Dube 2023). In countries like Lesotho, the development of e-passports and modernisation of border control and immigration systems is a pressing priority due to the dependencies on cross-border trade.

The success of these initiatives can be exemplary in demonstrating the important role played by digital ID policy frameworks. However, Africa faces the challenge of simultaneous mushrooming of digital ID initiatives which might create inconsistencies in how digital ID systems are developed across Africa. For instance, the AU Digital ID Framework focuses on foundational ID to develop digital ID, while the Smart Africa Digital ID Blueprint cautions that basing the creation of digital ID exclusively on foundational ID solutions could exclude millions of Africans (AU 2022; Smart Africa 2020). The unintended consequence is that African countries may adopt different digital ID standards depending on the entity providing them with technical support – the AU, SAA, UNECA, or the WB. If differences in technical standards are not carefully managed, they may have an impact on how digital ID systems across Africa integrate.

Besides low levels of regulatory harmonisation, the lack of vendor and technology neutrality is a big challenge hindering the implementation of interoperable digital ID systems. In fact, according to the 2018 ID4Africa survey, vendor lock-in was the primary cause of dissatisfaction with technology vendors among African identity authorities (Burt 2018). Open standards – which the International Telecommunication Union (ITU) defines as standards that are available for the public and are developed, approved and maintained through collaborative and consensus-driven processes – could solve vendor lock-in. Its use could allow African countries to access a large set of technologies as well as increase interoperability of technologies and the exchange of data from different services (AU Data Policy Framework). This is because when government agencies design software solutions based on open standards, it is easier to facilitate interoperability and integration with solutions developed by other agencies that are also built in compliance with those standards, and by doing so they enable a whole of government approach to delivering services. This means that when governments design digital ID systems based on open standards at both national and regional levels, they can support intergovernmental and regional cooperation in delivering cross-border travel and digital government services as they mutually recognise each other's ID. Adopting open standards and norms allows governments to access a larger set of technology options, they also facilitate interoperability and data exchange between different services. However, there needs to be more investment to make software a public good that can ensure scalability and flexible use.

The GovStack initiative, together with a growing international focus on developing DPGs, could play a role in filling this gap. GovStack aims to minimise vendor lock-in and product lock-in, as it takes a whole government approach based on developing specifications around interoperable, generic and reusable building blocks. The specifications for each building block can then be used independently to serve the needs of GovStack partners, for example, to develop procurement guidelines. It also offers a network of practitioners, which is essential to facilitate innovation and exchange in the e-governance ecosystem. GovStack is in discussion with Kenya, Djibouti, Somalia, Rwanda, and Egypt to support sandboxes and capacity building related to their e-government services.

There are a number of open-source solutions currently available that can be used or adapted by African governments to develop e-government services, including digital ID. Estonia's X-Road is another e-government interoperability framework being rolled out in countries including Namibia and Benin. X-Road is a free and open-source data exchange layer providing standardised methods for transferring information between the data systems of private

and public sector organisations (X-Road n.d.). Within X-Road, each citizen, but also each government agency and company, has a unique ID, allowing them to exchange, access and control their data (Nortal 2022). This interoperability layer provides the groundwork upon which advanced digital ID systems can be built, integrating a wide range of functions due to the ability to securely access a wide range of public and private services. The Modular Open-Source Identity Platform (MOSIP), developed by India with the support of the Bill and Melinda Gates Foundation, Norad and the Pratiksha Trust, is an open-source software that allows governments to conceive, develop and implement foundational ID systems. MOSIP is a modular open-source and open standards foundational digital identity platform, which aims to allow countries to build an ID system without locking themselves into a single system integrator and to adapt the modular architecture to respond to their local needs (Burt 2019). MOSIP has gained traction in Africa because it allows low- and middle-income countries leeway to customise it to their own context (UNDP 2023a). African countries, including Morocco, Sierra Leone, Togo, Guinea, Ethiopia, Niger, Madagascar, and Burkina Faso are already partnering with MOSIP and running pilots (MOSIP n.d.; Hersey 2023).

2.5. The role of donor agencies, international organisations and private sector in roll-out of digital ID systems in Africa

Governments across SSA work closely with the private sector, donor agencies and governments, global foundations, regional development banks and development partners in the development of digital ID ecosystems. The main actors working across SSA are the World Bank, UNHCR, UNDP, UNICEF, IOM, African Development Bank (AfDB), the European Investment Bank (EIB), the European Union, USAID, the Bill and Melinda Gates Foundation, Omidyar Network, Global System for Mobile Communications Association (GMSA), Idemia, Thales and Gemalto (see Table 1 for further examples of international partnerships in Sub-Saharan countries). The World Bank Identity for Development (ID4D) initiative has the highest contributions from various donors and development partners and foundations.

International donors provide both technical and financial support for African governments that do not have the requisite expertise and necessary financial resources to unilaterally embark on such projects or to sustain the digital ID systems in the long run. Depending on the type of approach they choose to take, African governments are working with different international actors. However, by breaking the components of e-governance down into building blocks and setting basic specifications for these building blocks, the GovStack approach aims to avoid vendor lock-in and therefore should allow governments to work effectively with different donors on different components of e-governance. However, there is a potential challenge of different donors with different agendas pushing African countries in different directions and causing unnecessary duplication of efforts.

For European actors, the approach is to focus on developing a secure interoperability layer for the exchange of data first and building digital ID on that. For example, the new Initiative for Digital Government and Cybersecurity (IDGC), funded by the EU and Germany's BMZ, aims to support digital governance and cybersecurity in Kenya, Djibouti and Somalia under the Horn of Africa Initiative. The Estonian e-Governance Academy, in partnership with the private sector, has helped Benin develop the Unified eXchange Platform. Similarly, Cybernetica and e-Governance Academy adopted Estonia's X-road in developing Namibia's e-government interoperability framework (more on these examples in the next section). Some international donors, including the EU, have very clear minimum requirements on the types of digital ID projects they can fund and those they are not willing to fund (Omidyar Network 2017).[11] For example, the EU's reluctance to fund digital ID roll-out in Kenya and Ethiopia in the past has been linked to strong

[11] Omidyar Network has been funding a lot of digital ID projects in Africa. They also make it clear that they do not support digital ID systems which are designed for surveillance purposes, systems which are designed for discriminatory purposes, systems in states with no robust privacy legal frameworks and systems that are not aligned with the Principles for Sustainable Development.

civil society advocacy about the extent of data collection and the implications for ethnic and minority groups.[12] Similarly, the EIB and the Agence Française de Développement (AFD) are co-financing Nigeria's digital ID system, together with the World Bank, but the EIB loan was delayed due to the lack of a data protection law and authority (EIB 2018; AFD n.d.; WB 2023b). Moving forward, a new EU-funded regional action on e-governance in SSA to be launched in 2024, will work closely with the AU and RECs to support the development of interoperable e-governance in Africa, including digital ID.

The World Bank has been the most active international donor in the area of digital ID via its ID4D initiative, which focuses on the rollout of foundational ID systems and is active in a number of African countries. The World Bank states that embarking on a digital ID project is capital intensive, with costs ranging from $3-$6 to enrol and register a person and $1.15-$5 per ID card to authenticate and verify including communication, operational and maintenance costs (Atick 2016). In 2018, the World Bank estimated that Africa would need $6 billion to meet its digital identification and civil registration needs (WB 2018a). Of course, the costs for complete digital ID systems can be difficult to estimate as each country's costs are shaped by the ID design choice (choice of biometrics, enrolment timelines, biometric fields, and enrolment kits, et cetera) and unique country characteristics (population, wage levels, infrastructure, and digital literacy levels, et cetera) (WB 2018b).

The active participation in the digital ID ecosystem by developmental actors and donors has been questioned by critical CSOs and academics, expressing concerns regarding the potential negative impact of digital ID systems on human rights. Some view these ID programmes as motivated by economic interests with very minimal, ill-defined and poorly documented benefits to the majority of people, while others condemn the programmes for adopting foreign or international best practices with no relevance to African contexts (CHRGJ 2022; van der Spuy et al. 2021). There is a window of opportunity for Team Europe to use its strategic position as a key actor in building e-governance and digital ID systems to promote democratic values, high standards, good governance, and transparency. This also requires Europe to prioritise supporting digital ID projects in countries that demonstrate strong performance on human rights, as indicated by the Freedom House barometer (with Namibia, South Africa, and Ghana having very high scores) (Freedom House n.d.). This approach aligns with Team Europe's commitment to fostering robust and rights-respecting digital ID initiatives. With the majority of African countries in the early phases of the Digital Identity Spectrum, there are several opportunities for partnerships between Europe and Africa, especially public-private-partnerships (PPPs) on the long-term sustainability of these digital ID systems. There are interesting examples that African countries can draw from, both across the continent and also in Europe. Our interviewees suggested that beyond creating partnerships with international donors to set up the infrastructure for their digital ID systems, African governments need to involve the private sector to ensure the management and financial sustainability of their systems. In addition to partnering with the private sector, governments can also charge a small fee to citizens that can go to the maintenance of the system. For example, European countries like Estonia and Spain, where digital ID is compulsory, charge small fees for the first-time issuance of digital ID, renovation, or other reasons such as loss. This is an approach that is also being taken by Tanzania, where citizens pay $0.22 USD for any query or authentication and legal residents and refugees pay $1.00 USD while the same service is free in Kenya (WB 2019b). However, business models involving fees for identification services should be approached cautiously to avoid exclusion.

The digitisation of ID systems has opened avenues for new business models and it is crucial to explore innovative pathways and collaborate with the private sector to derive value from data generated by digital ID systems. South Africa's proposed consideration of a business model involving charging fees for interfacing with the National Identity System, as outlined in the Draft Official Identity Management Policy (2020), is a potential model worth exploring further. This means that while governments own the main source of identity for citizens, they can share the cost of maintaining the database with the private sector. However, this means that when entering into agreements with

[12] Comments from an interviewee.

international partners, African governments need to make sure that local vendors and experts are part of the agreement and that there is a transfer of capacity and digital skills. Even within Europe, there are different approaches to digital ID toolkits, including the cost of ID cards, whether mandatory or not, as well as the economic model, which means that governments need to take this very pragmatically, striking a balance between sustainable operation and citizens' right to access to identification services at feasible fees.

Private sector actors provide various services such as supplying hardware, software and support for the development of digital ID systems, providing authentication services and supplying identity solutions. They are mainly motivated by the potential for profits, new markets and access to data which drives the demand for digital ID solutions which in turn reduces the operating costs and improves efficiency (WB 2019a). Access to data generated from increased digital transactions and digital ID systems is a goldmine for the private sector as they can repurpose such data to develop other service offerings. The major players providing digital ID services and solutions across Africa are identity services providers, financial institutions, telecommunications companies and fintech companies representing both domestic and international firms. Some companies have been awarded contracts to develop foundational ID cards, some are working on e-passports (Seychelles, Zimbabwe, and Lesotho), some are working with several government departments to develop functional digital IDs (such as Botswana and Zambia), while others are actively providing identity verification and authentication services and digital ID wallet solutions. Active participation of the private sector in identity management functions has raised concerns about the encroachment of private interests (Howson and Partridge 2022) as the private sector can hold government data ransom (Mabuza 2018)[13] and push for profits instead of human-centric development.

Private companies from Europe have partnered with different African governments. Veridos of Germany supported the government of Botswana in modernising its border management systems by introducing biometric technology and designing and issuing e-passports. InGroupe of France supported Seychelles in producing its new biometric passport. There have been reports that European embassies have been instrumental in helping EU-based companies win contracts for biometrics in countries like Kenya and Uganda (CHRGJ 2022).

3. A deeper look at 5 African countries' journeys to roll out digital ID systems

The rapid roll-out of digital ID systems in African countries is yet to generate results, as there are very few countries that have developed inclusive, sustainable and interoperable national digital ID systems. There are, however, countries that stand out in Africa due to their unique experience in developing a national digital ID system. Understanding the progress made by these countries in rolling out their own systems or facing challenges is key to setting up interoperable digital ID systems that can help the countries scale up their economies.

We look in depth at 5 countries' progress in developing digital ID systems at the national level, these are South Africa, Kenya, Nigeria, Benin, and Namibia. These countries are all democracies with different population sizes as well as political motivations, yet they play distinct roles in the digital ID ecosystem and their experiences can help draw important lessons for their peers. South Africa is a front-runner in the provision of e-government services in the continent offering one of the most advanced digital ID systems, Kenya is transitioning from its failed Huduma Namba ID cards to a new UPI due to issues of exclusion of ethnic minorities and lack of transparency. Benin is leading Smart Africa's digital ID Blueprint and is also a member of the World Bank-funded WURI project, yet contrary to the

[13] A private company was awarded a contract to develop and maintain the Electronic National Traffic Information System (eNATIS) for the Department of transport. Due to contractual disputes, the company did not want to release the system to the government department.

other, its system relies on Estonia's X-Road open-source platform. Finally, Namibia is lagging behind in terms of developing an e-ID system but is already ahead of others in the interoperability of government services. By looking at these case studies, we aim to highlight the opportunities and challenges that governments face as they attempt to implement e-ID systems in their respective contexts and assess what the policy implications are for international partners.

3.1. South Africa case study: A smart ID with limited transactional capabilities

Figure 3: Overview of the Digital ID system in South Africa

Source: ECDPM

The development of foundational digital ID in South Africa is part of the government's 2030 vision to digitise the public sector and develop a dynamic and connected information society and vibrant inclusive knowledge economy (Government of South Africa 2012). In 2012, the Department of Home Affairs (DHA) launched its modernisation programme, which integrated and digitised identity management systems. [14] The modernisation programme positioned the DHA as a strategic department for the country's economic growth and national security. One of the advancements of the DHA's digital management is the ongoing building of the National Identity System (NIS), an

[14] The DHA Smart Identification Card System was found to be a successful programme which transformed government service delivery through technology (National e-Government Strategy and Roadmap 2017).

interoperable system supported by the multi-modal Automated Biometric Information System (ABIS), to capture and store fingerprints, palmprints, facial recognition, iris scans, face images, and children's footprints. Once completed, the NIS will be interoperable with other government systems to provide a 'single view of a citizen' (National e-Government Strategy). To make it easier for digital ID systems to be interoperable across government entities, the Department of Public Services Administration (DPSA) has developed technical standards on interoperability applicable to all government departments (Government of South Africa 2006; Government of South Africa 2007a; Government of South Africa 2007b). Unfortunately, the development of the ABIS and the launching of the new digital ID system has been delayed due to a corruption scandal and court battle that followed (Mungadze 2021).

South Africa is one of the few African countries which is revamping its identification laws to create a regulatory basis for the digital ID management system. The Draft Official Identity Management Policy (Government of South Africa 2020) is a comprehensive document setting out South Africa's strategic direction on digital ID and the development of digital ID systems. The Draft ID Policy discusses the challenges that the current identity landscape faces, from the exclusion of certain groups of people, lack of interoperable systems operated by the DHA, the role of the DHA in addressing identity-related crime and national security interests, the economic benefits which can be derived from data generated from the digital ID system, etc. From the interviews we conducted, there were indications of limited or poor stakeholder participation and consultation on the Draft ID Policy. This was attributed to the Draft ID Policy being published amid the COVID-19 lockdown when interested stakeholders were adjusting to working remotely and paying little attention to policy developments. It is not clear when the Draft ID Policy will be finalised, or whether a second round of public consultations will be held.

The proposed National Identification and Registration Bill 2022 (Government of South Africa 2023), once passed into law, will replace the Identification Act of 1997 (Government of South Africa 1997). The objectives of the ID Bill are to establish a single, inclusive and integrated national identification system for South Africa applicable to citizens, residents and foreigners. The ID Bill requires the Director General of the DHA to compile and maintain a population register and a database and proposes to amend the ID numbering system to be inclusive of non-binary persons. The ID Bill also requires any data-sharing activities by the DHA with third parties like insurance companies, banks, and government departments, to align with South Africa's law on the Protection of Personal Information Act 2013 (POPIA).

In addition to the modernisation of the identification system, South Africa introduced the Smart ID card in 2012 which replaced the green barcoded ID book. The Smart ID card is designed with security technology to reduce forgery while enhancing trust in the system. However, the use of the Smart ID Card is not very popular. First, some citizens who possess the green barcoded ID book are not willing or can't afford to pay the administrative fee to switch to the Smart ID card. This reluctance is also exacerbated by the lack of transactional capabilities of the Smart ID card when compared to the social security card. [15] Closely linked to this, CSOs also fail to see the tangible benefits of excessive collection of biometric data of individuals and argue that digital ID systems only benefit the private sector and government. [16] Third, some DHA offices, especially in rural areas, are not equipped with systems to capture biometrics (Research ICT Africa 2022) and in some areas, there are no participating banks issuing Smart ID cards on behalf of the DHA in close proximity.

The DHA is the institution responsible for issuing IDs and maintaining the population register in South Africa. However, there is no legislation that identifies and affirms the DHA as the sole provider of official identity

[15] SASSA card issued by the South African Social Security Agency (SASSA). The SASSA card enables beneficiaries of social service grants to withdraw money from the South African Post Office, ATMs and certain retail outlets.

[16] Interviews with civil society organisations.

management services, which limits the ability of the DHA to challenge other entities which may be providing identity verification services (Government of South Africa 2019; Government of South Africa 2020). Due to the lack of a legal mandate appointing the DHA as a sole provider of identity verification services, other departments have been working on their own digital ID projects (for instance, both the DPSA and the State Information Technology Agency [SITA] are developing their own strategies on digital ID).[17] A siloed and fragmented approach to digital ID strategies may result in difficulties using digital ID across different platforms and systems from both the public and private sectors. As an ID institution, the DHA has been failing to secure its database and its poor track record on data security remains alarming. In 2017, ID numbers and other personal data of 30 million South Africans were exposed in a data breach (IOL 2017) and the following year, there was another security compromise which resulted in ID numbers and phone numbers of DHA website users being exposed (McKane 2018).

The data protection law, POPIA, requires public and private bodies to protect people's privacy and personal data. The identity management systems of the DHA, both the old and new systems, together with all the DHA activities must comply with POPIA and such compliance extends to the management of DHA service providers. The current DHA practice allows it to share data with public and private actors (especially banks). There are no documented and transparent guidelines that regulate sharing of identity data between the DHA and relying parties, leading to an unregulated exchange of personal information between parties (ID Policy). From the language of the Draft ID Policy, there is a level of assurance that the DHA understands the importance of people's privacy and the protection of personal data in line with POPIA. What remains to be seen is whether DHA processes comply with POPIA and how effective the data protection authority, the Information Regulator, is to enforce compliance. It is not clear whether the Information Regulator has been closely monitoring the current legislative and policy changes to the identity management ecosystem of South Africa. POPIA requires the Information Regulator to examine any proposed laws and policies which may affect the protection of personal information and report to the Minister the results of that examination. The extent of the Information Regulator's involvement in examining the Draft ID Policy and ID Bill is not clear and there is no publicly available information from the Information Regulator clearly setting out its position on the Draft ID Policy and the ID Bill.[18]

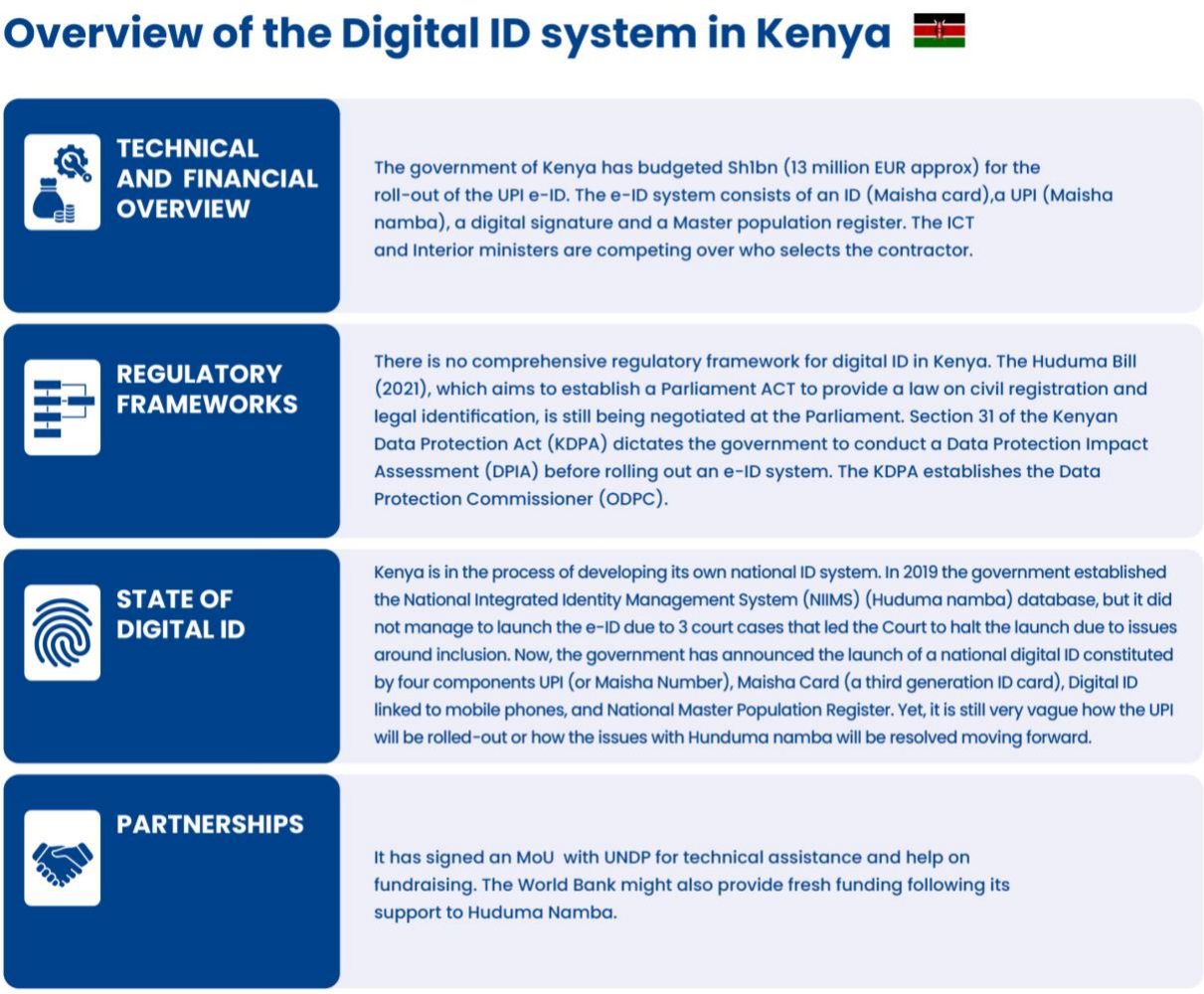
For South Africa to advance on its digital ID journey, there are some areas which require immediate attention. First, political intervention is urgently needed to address the fallout of the corruption scandal over the ABIS project and the final completion and launching of the new biometric system. Second, the ID Bill can be improved by making provision for the issuance of a unique number to any person registered on the NIS and for this unique number to be used as a digital ID to access services. Current national ID numbers in South Africa are not unique as the number is linked to or founded on a person's sex, date of birth or place of birth and citizenship status. Third, the Information Regulator, in line with its legal mandate, should play an active role in assessing the processing activities (like data sharing) carried out at the DHA. Fourth, instead of working in silos, the DHA, DPSA, SITA and Department of Communications and Digital Technologies (DCDT) should work together to develop a uniform strategy on digital ID and public key infrastructure as envisioned by the National Cybersecurity Policy Framework. Finally, South Africa needs to ensure that the new identification system is financially and operationally sustainable by creating opportunities to generate revenue streams and investments. Current revenue streams such as tariffs for civic and immigration services, self-financing, and charges for verification of identity and status should be supplemented by charging premium services and fees for interfaces with the NIS (Draft IP Policy) as well as developing other innovative solutions to provide the private sector with access to non-personal NIS data.

[17] Interviews with SITA and DPSA indicated that the discussions on digital ID strategy were held in the absence of DHA as a crucial stakeholder.

[18] The interviewed representatives of the Information Regulator indicated that they were not aware of the Draft ID Policy and ID Bill and whether formal submissions from the Information Regulator were submitted.

3.2. Kenya case study: From 'Huduma Namba' to the UPI

Figure 4: Overview of the Digital ID system in Kenya



Source: ECDPM

Kenya is recognised as a global leader in the development of mobile money and increasing rates of financial inclusion. It is leading the Smart Africa Digital Economy Blueprint and its rapid digital development has motivated it to lead global digital processes such as the adoption of e-government as well as digital economy. However, despite the endogenous innovations that have positioned the country among the key digital players on the continent, the country does not have a comprehensive digital identification system yet. Over the past few years, different policies and regulations have been developed with specific duties for the government to issue digital IDs. For instance, the National ICT Policy 2019 states that the government should provide a digital identity (universal personal identifier) for every citizen so they can use and access services safely and within the law (Government of Kenya 2019a).[19] Most recently, the Kenyan National Digital Master Plan 2022-2032, which has digital government services, products, and data management as one of the four pillars of the strategy, states that one of the flagship programmes is the creation of a Smart ID card to provide a personal unique identifier (Government of Kenya 2022).

[19] Which aligns with Article 12 of the Constitution entitling every citizen to rights, privileges and benefits such as having a Kenyan passport and any document of registration or identification issued by the state.

Kenya's digital ID journey provides key lessons for other African countries as it points to the importance of data protection and public consultations before governments launch digital ID projects. In 2019, the Registration of Persons Act (RPA) was amended to establish the National Integrated Identity Management System (NIIMS) database, which would serve as a foundational ID system providing one single source of identification for Kenyans. The setting up of the NIIMS database and the amendment of the Registration of Persons Act led to the government making it compulsory for everyone to register their biometric data including DNA in digital form and GPS of their home addresses in the database (Government of Kenya 2019b). Upon the free registration on the NIIMS database, a person would receive a unique identity number called Huduma Namba ("service number" in Swahili). Following the launch of the Huduma Namba project, there was a long and protracted legal battle between the government and CSOs, who opposed the government prioritising security over data privacy. In one court case of January 2020 (Government of Kenya 2020),[20] The High Court found that the collection of DNA and GPS for the NIIMS database was unjustified and ordered the government to adopt an appropriate and comprehensive regulatory framework for the implementation of NIIMS. In another court case of October 2021 (Government of Kenya 2021), The High Court found that the KDPA applied retrospectively as it is a law which gives effect to the constitutional right to privacy. Section 31 of the KDPA makes it a requirement for the government to conduct a DPIA when rolling out identity and digital ID programmes (King'ori 2022). It provides that "where a processing operation is likely to result in a high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out a DPIA" (King'ori 2022). The court ordered the government to suspend the issuance of Huduma ID cards pending the carrying out of DPIAs.

In December 2021, the Kenyan National Assembly introduced the Huduma Bill to the Parliament, after the previous Huduma Bills (2019 and 2020) failed to address issues around inclusivity (Yousif 2022). But this bill, which offers an opportunity to shape the law that governs the Kenyan registration system, is still being negotiated at the Parliament. Furthermore, members of the ICT ministry and wider commentators claim that the Huduma Namba faced public backlash because the Government failed to communicate clearly the value of the digital ID card to its citizens, and failed to involve CSOs in the process of design and implementation of the system (Abuya 2023; Citizen TV Kenya 2023). Additionally, lack of transparency from the government as well as mistrust in the digital ID system led to the low level of registration. As of December 2022, the Government had issued only 7.3 million Huduma Namba cards (Otieno 2023), while more than half of the registered Kenyans did not pick up their Huduma card (Abuya 2023). The Government made it mandatory to acquire a primary identification document such as a national ID card or birth certificate to register for the digital ID system, but ethnic groups such as Nubians, Somalis, Boranas, Maasais, Indians, and Arabs have, since the colonial period, struggled to secure legal documents to prove their identity, and therefore are at risk of exclusion from accessing government services.

The new Kenyan Government has announced that it will replace the 'Huduma Namba' cards with a UPI number Maisha Card, as an attempt to distance itself from the failures of the Huduma Namba. The communication of the new UPI has been rather unclear with the postponement of the launch of the initiative in late September, as well as in terms of defining the difference between the two systems. Nevertheless, the new UPI aims to build on the Huduma Namba system. Furthermore, the approach to the new UPI is facing challenges of fragmentation as it is not clear who – between the Ministry of Interior (which issued the Huduma card) and the National Registration Bureau (responsible for the new UPI) – will govern the new digital ID as well as the database (interview). Even though the Government has not put out a strategy for the UPI, it has already started to pilot it in some hospitals and schools. Contrary to the Huduma Namba, which only targeted people above 18 years, the UPI will register births and deaths and serve as a digital ID to access Government services (including the Kenya Revenue Authority, or the National Social Security Fund and the National Hospital Insurance Fund) (Kenya News Agency 2023) through the e-citizen digital platform (Angira 2023). It is therefore a foundational ID system which will be a centralised database

[20] Nubian Rights Forum and 2 others v Attorney General and 6 others; Child Welfare Society and 9 others (Interested Parties).

connected to functional ID systems. All the government agencies will also be connected to the UPI to authenticate the foundational data, thereby creating a National Master Population Register that will harmonise and consolidate all government databases (Burt 2023). The National Bureau and the Ministry of Interior have the most sophisticated national databases which can be interoperable with other databases such as the Revenue Authority's database once they have cleaned the data (interviewer).

The proposed roll-out of UPI has, however, raised concerns around the lack of transparency on the legal basis of UPI, lack of effective, nationwide public participation in the system and uncertainty about data protection (Access Now 2023). It is not clear whether human rights impact assessments will be conducted and made available for the public to review. One of the key lessons from the Huduma Namba rollout is that when digital ID systems are not designed following principles of inclusion, data minimisation, and respect for digital rights, the implementation of such systems creates further inequalities for minority and historically marginalised communities, including the Nubian, Borana, Swahili, and Somali communities as well as double registered persons (for example, Kenyans whose biometrics are in the refugee database) who already struggle with systemic discrimination in obtaining registration and nationality documents. One way of addressing barriers to access to digital ID is to eliminate the vetting process, which has been deemed as a discriminatory practice. Furthermore, it is key for the government to provide an answer to statelessness in the country before linking services with the registration for the UPI.

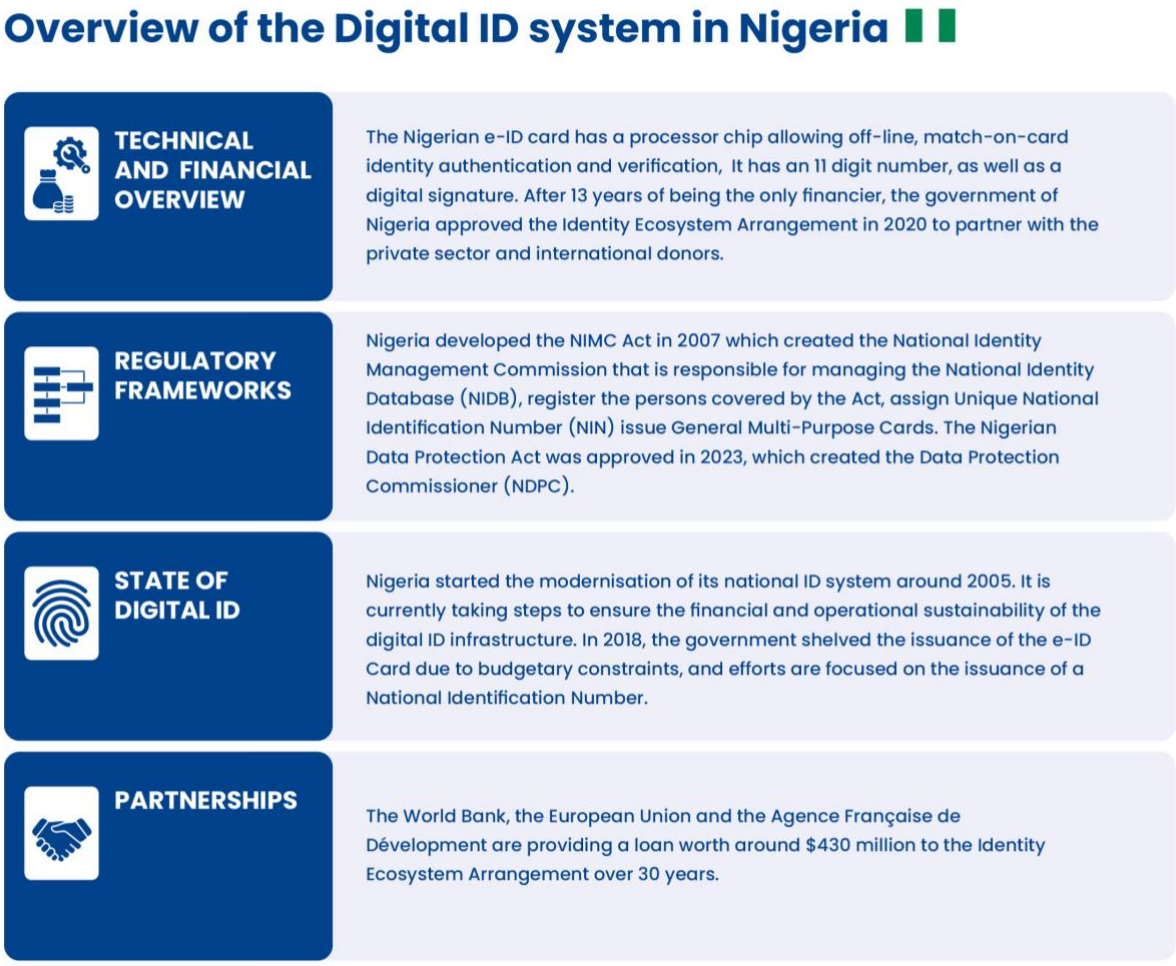
The Government of Kenya has communicated its vision of developing the UPI but there are still many questions unanswered. Despite the fact that Huduma Namba contributed to the development of personal data protection laws, there is not yet a regulation governing the Kenyan e-ID system.

The new administration has arguably fewer resources to develop the UPI and announced plans to cut the budget (Hersey 2023) for the issuance of Huduma Namba cards down by 85% ($5.3 million to $832,000) as it prepares for the launch of the new UPI. Estimates indicate that it might cost around 20 billion Ksh (much of it will be used to set up the platform and in the communication strategy). The government has budgeted 1 billion Ksh ($6.83 million) for the roll-out of the new ID system. Although international organisations such as the World Bank and UNDP might respectively contribute with new fresh money, help with fundraising, design and monitoring of the UPI roll-out, the Kenyan Government should think of financing models which can make the UPI more financially and operationally sustainable (UNDP 2023b). Over the past year, the Government has been sending Kenyan delegations to Pakistan, Estonia, Belgium, and other countries with success stories of digital ID implementation to create partnerships for the roll-out of the Masha ID system.

Kenya's journey to develop its own national ID systems shows some of the key challenges that many African countries face in creating unique, inclusive and sustainable ID systems. First, the Government's failure to run a risk assessment on the Huduma Namba led to the further exclusion of communities. Designing digital ID systems and regulation that mandates the exclusion of minority groups, women, and people in rural communities is essential for ID systems to succeed in their objective of transforming the economy and well-being of citizens. Second, Kenya implemented the e-ID system without a strong regulatory framework in place, thereby falling short of ensuring transparency, accountability of e-ID systems, legitimacy of collecting data, as well as giving assurance to citizens that their data will be protected and used for their and the country's benefit. Third, the failure to communicate the e-ID system and its benefits for the country and its citizens created an atmosphere of mistrust. Finally, implementing an e-ID system without addressing underlying political issues around identity and belonging in the country. Kenya's experience also indicates that being part of global networks for the roll-out of digital ID systems is very important, perhaps more so for large and multi-ethnic countries with clear geographic and gender digital divides. These networks can serve as platforms for exchanging knowledge between countries with similar characteristics and challenges as well as countries with key expertise in rolling out e-ID systems.

3.3. Nigeria case study: Accelerating National Identification Number Issuance through Digital ID ecosystem

Figure 5: Overview of the Digital ID system in Nigeria



Source: ECDPM

The modernisation of Nigeria's identification system took a more purposeful turn in 2005 when the federal government constituted a committee to, among other things, report on appropriate steps to take for the harmonisation of disparate identification schemes in the country (NIMC 2017a). This action was particularly motivated by the country's poor consumer credit market and the lack of a reliable system of identification that would specifically help law enforcement authorities in the fulfilment of their duties (NIMC 2010). Following the Government's adoption of the Report of the Committee, the NIMC Act (NIMC 2007) was passed in May 2007 to accelerate the development of an Identity Sector. The Act created the National Identity Management Commission, the country's apex ID institution charged with the mandate to establish, own, operate, maintain and manage the National Identity Database (NIDB) in Nigeria, register persons covered by the Act, assign a unique NIN and issue General Multi-Purpose Cards (GMPC) to those who are citizens of Nigeria as well as others legally residing within the country. The proliferation of identity card systems, many of which are analogue and lack the means to be verified and checked in real-time, has been a notable aspect of the historical development of the identity sector in Nigeria. With the new Act, the Nigerian Government saw the need to move away from the issuance of 'ordinary ID cards' and decided to roll out a peculiar GMPC, otherwise known as the National e-ID Card. The Nigerian e-ID Card comes

with a processor chip that enables off-line, match-on-card identity authentication and verification. It is issued to Nigerians registered under the National Identity Management System (NIMS) and legal residents who have attained the age of 16 years and above (Nigeria e-ID Card). In 2018, citing budgetary constraints, the Nigerian Government shelved the issuance of the cards, having issued roughly 10% of the 50 million targeted to be issued at the first instance; instead, efforts are now geared towards the issuance of a NIN (Onwuaso 2018).

The NIN is composed of 11 random, non-intelligent numbers that are given to a person following successful enrollment. In the case of Nigeria, enrollment entails the recording of a person's demographic information as well as the capture of ten fingerprints, a head-to-shoulder photo, and a digital signature. These are all used to cross-check the data already present in the National Identity Database to ensure that the same information has not already been entered (the National Identity Management Commission). It is the unique identifier used to link all entries in the database concerning a certain person, as well as to establish or verify identity. All Nigerian nationals and residents who are in the country legally must register for the NIN starting at birth (NIMC 2017b). As of the second quarter of 2023, 101 million eligible individuals, representing 45% of the country's population of 223 million people based on UNPF data, had registered and obtained NIN under the Nigerian ID Program (NIN Enrolment Dashboard). The main reasons motivating Nigerians to register for the NIN are the need to open and operate a bank account, to obtain a Nigerian passport and to buy and register a SIM Card.

A harmonisation and integration evaluation study was commissioned by the NIMC in 2008, and the results showed that most, if not all, government entities lack the technical and network readiness needed for seamless data exchange. The sharing of identity-related data is particularly hampered by the existence of silo identity databases that are maintained by about 13 government agencies and other critical organisations in Nigeria. These databases use comparable procedures to acquire identification data but are not linked to one another (NIMC n.d.). This scenario drove the NIMC to establish standardised practices in several operating fields. For instance, the demographic, biometric, and verification processes were standardised between 2010 and 2013 (NIMC 2011a and Nigeria Demographic Data Standard). To achieve interoperability and optimise the benefits of the NIMS, standards and guidelines were developed towards the creation of an interoperable system with sufficient interactive windows to facilitate the use of available databases by government agencies without hindrance. Through the NIN which is the single version of the truth, and the NIDB which serves as the centralised ID gateway system, NIMC now performs seamless interchange operations with functional identity databases and other systems that adhere to uniform interchange standards (NIMC 2017c). Using an explicit and formal information model and standard coded terminology, NIMC can now interoperate with other systems that use known interoperability standards. Based on the design, the NIMC system has the latitude to update, customise, inactivate, or destroy access privilege.

Nigeria's past experience in building an ID system was based largely on vendor-dominated arrangements, culminating in the 2001 ID card turnkey contract that failed within 5 years, leading to a vendor lock-in impasse. But in the current ID Program, which is a paradigm shift from just ID card issuance for identity management, the Nigerian Government recognised the dearth of expertise and/or experience and took the necessary precautionary steps to forestall a repeat of similar experiences (NIMC 2011b). Modular arrangements are now preferred, meaning the NIMC now has three key front-end vendors and different vendors for the deployment and maintenance of the back-end systems. The idea is that, if a particular procured technology is not working as it should, or the service level agreements are not being met, NIMC has the liberty to trigger the exit clause built into the vendor's contract. The exit clause states that they have to hand over everything to the Commission (interview).

June 2023 marked a watershed moment as the Nigerian Data Protection Act was signed into law and became fully enforceable. The Act safeguards the rights of data subjects by requiring that personal information be handled fairly, legally and responsibly. It also encourages data processing methods in Nigeria that preserve the security of personal

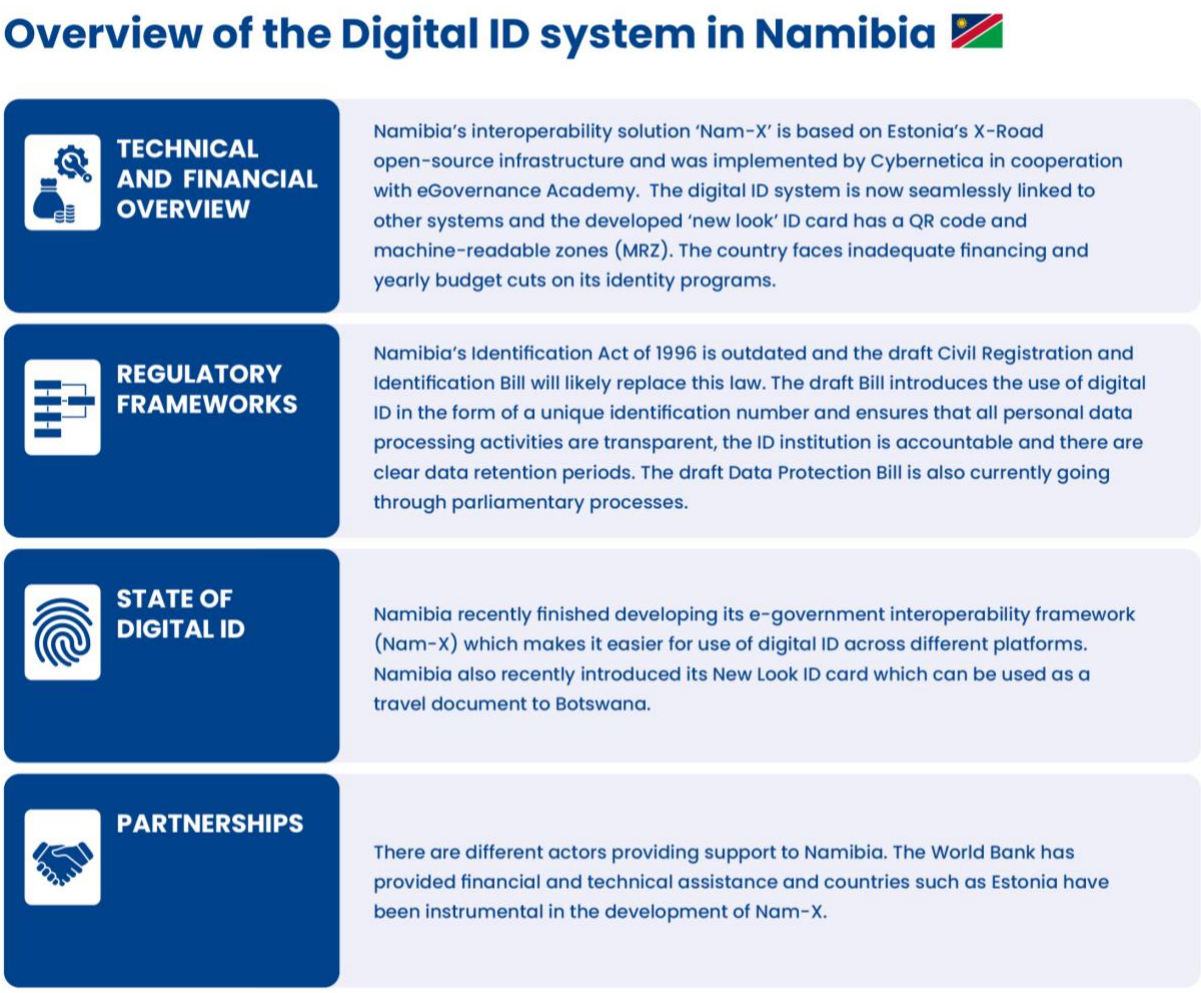
information and the privacy of data subjects. It creates the Nigeria Data Protection Commission (NDPC), an autonomous entity to oversee and control data protection concerns and enforce adherence to the Act (NDPC 2023). The NDPC is now fully operational including the licensing of a Data Protection Compliance Organisation (DPCO) for the purpose of training, auditing, consulting and rendering services aimed at ensuring compliance with this regulation or any foreign data protection law or regulation having effect in Nigeria (NDPC n.d.)

The Nigerian Government is conscious of the need to prevent the ID programme from becoming an ongoing financial drain on the country's coffers. Accordingly, a new arrangement known as the Identity Ecosystem was initiated in 2020 after the Government served as the project's only financier for the first 13 years of its existence (NIMC 17a). The Ecosystem offers a broader range of NIN registration via government bodies and private vendors licensed by the NIMC. In 2020, licences were issued to 173 private sector agents and 30 government/public sector institutions (203 in total) to complement NIMC in carrying out enrollment and NIN issuance services. This brings the total number of active enrollment centres as of the first quarter of 2023 to 5,500 nationwide and 15,000 devices across the federation (Egole 2023). The private vendors are remunerated on a pay-per-play basis, which means they get paid for each successful enrolment of a person, complete with the issuance of a NIN. Enrolment and NIN issuance remain free in Nigeria, but a fee is charged, $30 USD for above 16 years and $20 USD for under 16 years for diaspora enrolment (NIMC 2019; NIMC 2023). Ecosystem is being funded by the World Bank, the EU and the AFD to the tune of $430 million, to be disbursed in the form of a loan with a 30 year maturity (NIMC 2020). As part of the EU's programming for 2021-2027, the EIB made commitments to provide Nigeria a €250 million loan to support the roll-out of its digital ID, which might be disbursed in the following year as Nigeria records progress in setting up a data protection framework (interview).

Digital identification can truly be transformational for Nigeria, where 63% of the population grapples with multidimensional poverty (NBS 2022). However, three critical areas need to be prioritised going forward. These include enhancing programme implementation, focusing on specific use cases, and updating technical systems/infrastructure. To improve implementation, data capture and approach to data capturing would need to be reengineered, since these two components heavily influence budget and pace. It is cumbersome to collect over 70 demographic data per individual during registration as is currently the case in Nigeria. Thus, the number should be lowered to at least 20 data fields. Additionally, the requirement of a supporting document before registration ought to be eliminated. To further strengthen the enabling environment, additional work would be required with regard to legislative environment reform. It is also important that Nigeria focuses on a selected few use cases of the NIN to drive greater adoption and use. In this light, use cases such as social safety net, financial inclusion and security should be the core. Moving ahead, the Government would need to update its existing technology, particularly its NIDB infrastructure, whilst investing in local capacity. In order to secure information access, make longer-term maintenance simple, and ensure that system changes do not necessitate a whole redesign, it is also necessary to actively promote systems that are vendor and tech-neutral.

3.4. Namibia case study: The 'New Look' Digital ID

Figure 6: Overview of the Digital ID system in Namibia



Source: ECDPM

The development of a digital ID system in Namibia is still in its embryonic stages but is growing at a relatively fast pace due to demonstrated political commitment, support from its international partners[21] and the active involvement of the private sector. The Office of the Prime Minister was in charge of guiding and implementing the ICT strategy for Namibia which included the digitalisation of paper records (WB 2016; Government of Namibia 2005). Through this preparatory work by the Office of the Prime Minister, the e-Government Strategic Plan was eventually formed (Government of Namibia 2014). One of the goals of the e-Government Strategic Plan was the adoption and use of the Unique Identification Number (UIN) for every citizen to access services, maximising citizen convenience by eliminating the need to produce identification documents, ensuring that the UIN system is used for authentication across public and private services (Government of Namibia 2014).

The Government of Namibia has been working on improving the interoperability and integration of its systems to enhance service delivery to citizens.[22] Building on its strong ties with Estonia, Namibia implemented its

[21] UNICEF, WHO, AfDB, UNECA and UNFPA have supported the civil registration system in Namibia.

[22] One of the programmes that Namibia's e-Government Strategy highlighted was on the e-Government Interoperability Framework.

interoperability solution dubbed 'NAM-X' which made it possible to develop e-services and for its public sector institutions to exchange data securely. NAM-X was developed using Estonia's X-Road framework (EGA 2014). Cybernetica and the e-Governance Academy worked together on this project (Cybernetica 2021; EGA 2021). Both the Ministry of Home Affairs, Immigration, Safety and Security (MHAI) and the financial regulator, Namibia Financial Institutions Supervisory Authority (NAMFISA), are making headway and demonstrating a high level of interest in ensuring that digital ID solutions are available to the public. NAMFISA, with the support of a Nigerian firm, is building the country's digital ID framework which is hoped to advance its digital economy (Elimian 2023).

In 2021, the President of Namibia launched a 'New Look' ID card. The old national ID card and the South West Africa card are being gradually phased out (Nakashole 2021). The New Look ID card carries more benefits in that it can be used as a travel document to Botswana and complies with the International Civil Aviation Organisation (Xinhua 2023). The New Look ID comes with a QR code and machine-readable zones (MRZ) which make the card more tamper-proof.

Despite Namibia effecting changes to, and digitalising its national identification management system, the underlying Identification Act remains outdated. The Identification Act empowers the Minister of Home Affairs to maintain a population register as well as assign identity numbers and issue identity documents to citizens and permanent residents (Namiblii 1996). The Minister of Home Affairs has updated the regulations relating to the Identification Act by introducing new provisions for the use of QR codes and MRZ in the identity card (LAC 2001). The recently passed Electronic Transactions Act (2019) also regulates aspects of digital ID relating to advanced electronic signature, which is designed with enough security to identify the signer (LAC 2019). Despite attempts by Namibia to digitalise its identity system, the identity regulations still provide manual processes (like capturing fingerprint data) instead of digital capturing of biometric data.

The recently published Civil Registration and Identification (CRI) Bill is aimed at making significant changes to the identity legal framework of Namibia such as the assignment of UIN to each person who registers on the new civil register (Parliament of Namibia 2023). The CRI Bill is one of the few identity laws which unequivocally requires the ID institution to be transparent and accountable in its activities. Important principles such as data subject notification, obligations on entities accessing the Civil Register and data storage and retention requirements are clearly addressed in the CRI Bill.

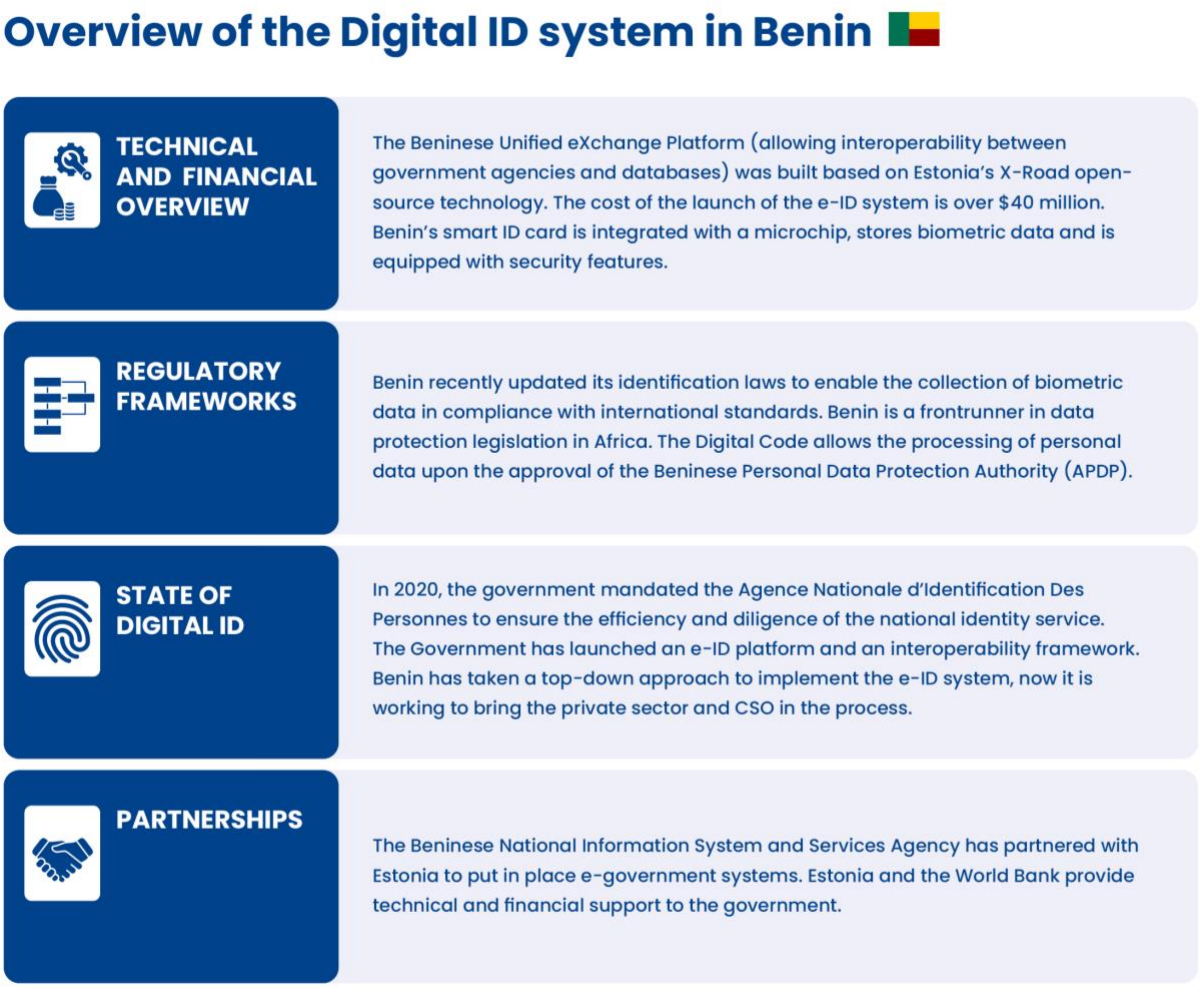
Namibia recently started the legislative process to ensure that personal data (which includes digital ID) is protected. The draft Data Protection Bill is currently going through legislative processes, including public consultation, before it is passed into law. Once passed into law, Namibia should act swiftly to make sure that there are regulations in place to clarify the data-sharing requirements for digital ID data and the flow of data across different institutions and across borders. Once the Data Protection Bill is passed into law, ID institutions will be accountable to a data regulator (MICT 2022). The Bill creates the Data Protection Supervisory Authority which acts independently, impartially, and performs its functions without fear, favour or prejudice across Namibia. The powers of the data regulator under the Data Protection Bill are the same as those prescribed in POPIA for the South African Information Regulator. Once the Data Protection Bill comes into operation, it is expected that the data regulator will be able to carry out its functions independently.

Moving forward, Namibia needs to find innovative solutions to create the demand for digital ID across its least densely populated territory to keep the already expensive digital ID systems operationally sustainable as well as inclusive of rural communities. Proposals of the CRI Bill such as collection of fees from service providers who may want to get identity documents authenticated and verified or from any person accessing certain records need to be carefully considered and substantiated. With the vested interest of financial institutions and telcos in Namibia to

rely on digital ID, authentication fees can be a steady source of revenue for the MHAI. The Government should continue with the legislative process to enact the data protection law and preparatory work to discuss the establishment of the data protection authority and the funding of the authority should be prioritised. Timeously appointing a data regulator ensures that the MHAI complies with the data protection laws. Overall, to ensure universal digital ID coverage, digital infrastructures must be improved to bridge the digital divide which often results in rural communities being excluded from access to digital services, including digital ID.

3.5. Benin case study: Championing the Smart Africa Digital ID vision

Figure 7: Overview of the Digital ID system in Benin



Source: ECDPM

Benin is undergoing a digital transformation of its public sector and the modernisation of its identity system is a key element of this process. As in many other African countries, digital transformation is one of the key sectors for development in the Beninese Government's action programme for 2021-2026 (Bénin Révélé 2021). Benin wants to become the leading country of e-services in West Africa (ID4Africa 2019). In addition to economic development ambitions, the Government aims to roll out the ID system to deepen the digitisation of government administration and efficient and quicker access to public services for citizens and businesses (Bénin Révélé 2021). Political stability and security concerns also appear as an important rationale for the development of digital identification (ID4Africa 2019).

Benin's digital ID project which started in 2016-2017 was split into 4 phases: 1) preparation, 2) building of the initial biometric database, 3) ongoing data capture and update of the database, and 4) exploitation and monetisation of digital ID (Adjovi 2019). The law on the identification of natural persons in the Republic of Benin launched a vast 6-month administrative census (Assemblee Nationale 2017). The objective was to update the National Registry of Physical Persons (RNPP) and to collect biometric data in compliance with international standards. The decision was made to register everyone, even those who came with no ID documents, as 20% of the total number of registered individuals did not have evidence of identity. A process was set to produce locally on the spot a document signed by two witnesses and a municipal officer. This document would have all the necessary basic information required to identify the person. Once the process was completed and verified, it was decided to provide a new and electronic birth certificate to all those who did not have one. This process 'regularised' 2.5 million people. The first e-ID cards were produced in 2018 (ID4Africa 2019).

In July 2020, a government decree described the procedures for implementing the biometric national identity card in Benin and mandated the country's ID institution, the Agence Nationale D'Identification Des Personnes (ANIP), to take appropriate measures to ensure the efficiency and diligence of the national identity service (SGG 2020). Benin has issued 3 million foundational ID credentials with QR codes and registered close to 97% of the population (WB 2023a). The new identity card is a visa-card-like document with an integrated microchip that stores names, surnames and biometric data like fingerprints and comes with security features like a QR code and a holographic code, making it hard to falsify the identification information (Njoya 2022). The programme was extended to the issuance of digital IDs to Beninese citizens in the diaspora (Macdonald 2023). Benin also introduced e-visa processes to promote tourism. A communication campaign was launched to ensure that people embraced the programme (Adjovi 2019). Given that obtaining the card costs 6,000 CFA francs, the Government has launched a survey to identify extremely poor people so that they can receive the card free of charge.[23]

In March 2020, the Government with the support of Estonia, launched an e-ID platform that allows citizens and businesses to access public and private services. Similarly, as other governments that have taken a top-down approach, the Beninese National Information System and Services Agency believes that the Government should create digital public services that require e-ID to access them, thereby creating demand for e-ID (Service-Public n.d.). More than 250 e-services are already available on the platform. To develop the one-stop-shop platform for digital services and the interoperability framework, the Government partnered with the Estonia eGovernance Academy which focused on building the digital capacity of government officials, their engagement with the private sector and review of the national legislative framework. The Beninese interoperability framework is inspired by the European Interoperability Framework (EIF) but it is adapted to the country's own context. The Government also gets financial and technical support from the World Bank, through the WURI project and other broader initiatives. In the same year, Benin also led the development of the Smart Africa Digital Identity Blueprint, which proposes the Smart Africa Trust Alliance to implement interoperable digital ID systems. Pilot projects will be conducted in 8 Smart Africa member states.[24]

Benin has been one of Africa's front-runners in the adoption of data protection laws. Its 2009 Data Protection Law dealt with the protection of personally identifiable information and was later supplemented by the Digital Code (APDP 2009; APDP 2018).[25] The Digital Code deals with the collection, treatment, transmission, storage, and use of

[23] L'identité numérique et sa mise en œuvre - Le cas du Bénin Edgar D. AYENA – Ingénieur Systèmes d'Information, Expert Architecte et Développement Logiciel – Projet WURI BENIN (June 2023).

[24] Smart Africa Alliance - Digital Identity, 2020. In 2020, Benin championed a Smart Africa flagship project to develop the Digital ID Blueprint, supported by a working group that included Rwanda, Tunisia, the AU, the International Telecommunications Union (ITU), the World Bank, Omidyar Network, UNECA, the GSM Association (GSMA), the World Economic Forum, GIZ and several private companies.

[25] The code is applicable to natural persons in Benin regardless of their nationality or domicile and it extends to extraterritorial processing activities governed by Beninese law.

personal data by a person, the state, local authorities, and legal persons, as well as automated processing and non-automated processing of personal data contained in files, or any processing of data for public security, defence, research, prosecution of criminal offences, or the security and essential interests of the state. The Digital Code is one of the most comprehensive efforts to regulate data protection, and related matters, within the region (APDP 2018). The code applies to data controllers located in Benin and the Economic Community of West African States (ECOWAS) region. The Digital Code allows the processing of personal data, including biometric data, only after prior authorisation by the Beninese Personal Data Protection Authority (APDP). The APDP, which was established in 2018 ensures that everyone, including ID institutions, complies with the data protection laws. The APDP is also responsible for ensuring security and confidentiality of public data and has the power to control and sanction infringements related to data use which includes imposing financial sanctions on data controllers for non-compliance. Since its creation, the APDP has only supplied authorisations for the collection or deletion of personal data and registered around ten complaints (Paradigm Initiative 2021).

Even though the Beninese Government is taking an active role in developing the technical and regulatory environment for an inclusive, sustainable and interoperable digital ID, there are some key challenges that should be addressed to make the e-ID fit for purpose. First, despite the fact that the registration for e-ID is open to all people on the territory of Benin, people find it difficult to register due to illiteracy, which affects 60% of the population, particularly women. This is exacerbated by the fact that registration services are not provided in local languages. Secondly, there is a lack of state administration services in the more remote areas of the country, meaning that people in rural villages find it harder to register. Finally, people in Benin sometimes also choose not to register, due to concerns around data privacy and security, as well as the high levels of internal mobility of some groups, such as domestic workers from Togo who move frequently to find work and therefore do not register. To combat some of these problems, there could be better communication to alleviate concerns about data privacy and security, as well as greater state administration services in border zones.

Moving forward, Benin will need to focus on making its e-ID system financially sustainable by creating public-private partnerships. The Government has taken a government-led approach when developing digital ID systems but to ensure the financial sustainability, uptake and inclusivity of its e-ID system it should partner with a different set of players including governments, the private sector as well as civil society organisations. The Government will have to strengthen its communication efforts and further enhance inclusion by tackling issues of access linked to literacy, cost or internet access. Benin should also attract investment in digital skills and literacy beyond building the capacity of government officials and departments.

Initial takeaways from the 5 case studies

Looking at the case studies - South Africa, Kenya, Nigeria, Benin, and Namibia - it is clear that regardless of the stage of digital ID development in each country, what is crucial going forward is assessing the sustainability of these digital ID systems. ID projects are very expensive, and though international organisations may provide financial support, these African countries had to invest huge amounts of money into these projects. Unfortunately, due to poor project management (for example, corrupt procurement process of South Africa's NIS) and poor planning (for example, Kenya-producing Huduma cards despite court processes which were challenging the Huduma Namba project), some of these projects have left these countries financially haemorrhaging. Though donors and development actors are providing financial support for digital ID projects, policymakers need to think of long-term strategic and innovative financing models to keep the digital ID systems operationally and financially sustainable. The monetisation of data is increasingly becoming a lucrative way for financial sustainability but any further steps in negotiating PPPs on data sharing must take place within the confines of data protection laws and the AU Data Policy Framework.

4. Policy recommendations for the EU

By advancing digital cooperation with Africa, the EU has an opportunity to both support and benefit from Africa's youthful population and future digital single market, but such benefits can only be reaped if the EU sufficiently invests in Africa. The various initiatives and projects which shape the Team Europe approach can be improved through increasing investments in both hard digital infrastructure and intermediate infrastructure such as digital ID, as well as providing technical assistance, supporting capacity building, uptake of digital skills and guidance on drafting and implementation of regulatory frameworks (Musoni et al. 2023; Floyd and Musoni 2023). Through the guidance of the AU and bilateral discussions with AU member states, several EU projects can be replicated and extended to other African countries interested in cooperation.

The EU needs to be mindful that it is not the only international player interested in supporting African countries to develop their digital ID systems. It faces competition from other actors like India, offering its own technological solution through the MOSIP project, with China and the USA still dominating the digital economy in Africa. To navigate this digital geopolitical competition successfully, the EU needs to add value and offer solutions that lead to Africa's economic development while helping Africa address the challenges of data exploitation. This also includes framing its offer under a more comprehensive label that can bring cohesion to the different work that EU member states and European companies are doing to support the implementation of sustainable and inclusive e-ID systems across Africa. Conversations towards this have been principally led by Estonia, who see value in a European package of digital building blocks (or stack), yet while the pressure to counter the 'GovStack', and 'Indiastack' narratives is palpable, it is not clear whether this will be taken up by other EU member states. It is advised that the EU extends its offer to Africa beyond market participation, focusing instead on creating an enabling environment for the recognition of African digital ID. This approach entails encouraging reciprocal efforts, allowing African actors to actively partake in the EU's digital single market.

In this section, we discuss the type of cooperation that the EU can envisage with African countries building their digital ID systems. We also recommend some of the policy interventions that the EU must adopt to prove its credibility as a trusted partner with Africa.

Figure 8: Policy recommendations for European policymakers

Source: ECDPM

4.1. Share experiences in developing interoperable systems

As Africa works towards building its free trade area and digital single market, an interoperable digital ID plays an enabling role in cross-border trade, allowing for faster verification and legitimate trade. The AU's Digital ID Interoperability Framework is Africa's attempt to strengthen trust and interoperability among foundational identification systems of AU member states and empower economic integration through the AfCFTA. However, the interoperability framework is yet to be implemented and Africa's experience in continental interoperability is limited to regional efforts such as the WURI or a few countries participating in interoperable payment systems like the Pan-African Payment and Settlement System (PAPSS). Within this context, the EU can showcase its value-add by sharing with African counterparts its own experience in developing digital infrastructure for its single market, including the EU Interoperability Framework for public administrations, the Single Euro Payments Area (SEPA) in the financial sector, and the eIDAS Regulation (Teevan 2023).

The eIDAS Regulation laid the foundations for safely accessing public services and carrying out transactions online and across borders in the EU. There are ongoing negotiations to amend the eIDAS Regulation to extend the rules to the private sector and development of a European Digital ID Wallet which can be used across Europe's single market (EU 2021). The EU can share its lessons on the interoperability challenges faced across its digital single market which led to the development and adoption of the amended eIDAS Regulation. The EU can also draw from the lessons learnt from the 4 large-scale pilot projects testing the EU Digital ID Wallet in digital payments, mobile driving licence, e-Health and education (EU n.d.). There is a lot that African countries have not yet figured out, such as the minimal requirements (legal, operational, and technical) for digital ID systems to be interoperable and fully functional at a continental level. By sharing with Africa its lessons, the mistakes it made and factors leading to the success of its framework, the EU can help Africa pre-empt certain challenges including how to reach common regulatory standards despite the different levels of digital development between African countries, avoid similar mistakes and save time and resources in building interoperable digital ID systems and integration of digital ID wallets within the African DSM.

4.2. Help in developing digital ID standards

The AU's Digital ID Interoperability Framework proposes for Africa to establish its own standards-setting body which can provide guidance on the technical, operational, and legal requirements for the framework to work. The EU can use its reputation as a 'standards maker' and expert in 'norms-setting' to support the implementation of the interoperability framework by providing guidance on establishing minimum standards on digital ID, integration and mutual recognition of digital ID as well as technical standards for interoperability. Team Europe has supported the Smart Africa Alliance in developing the digital ID Blueprint which was piloted in Benin. Similarly, Team Europe has also supported the AU in developing the AU Data Policy Framework which highlights the importance of interoperable digital ID systems in Africa. Through the DataCipation project, Team Europe is now assisting AU member states to implement the Data Policy Framework within their countries. These ongoing projects can be used as pathways to continue to support African countries in developing digital ID standards. Countries like Estonia (through X-Road), Spain, Germany and France (through GovStack) together with the European Commission (EC), the EU Delegations and the D4D Africa Hub can spearhead these discussions as they understand the local context and technical capacities of some of the African digital ID infrastructures.

4.3. Integrate and recognise African digital ID

To demonstrate a commitment to equitable partnership, the EU must actively engage in discussions concerning the recognition and integration of digital ID developed in Africa. The EU's internal and external policies on digital ID

should earnestly explore the feasibility of allowing African digital ID to access certain services during travel to Europe or transactions with European entities. The EU can initiate discussions with African governments around digital ID wallets and how the European Digital ID Wallet or the African Digital ID Wallet (once developed) can be integrated in both regions (EU 2023). The mutual recognition of digital ID from both regions sets the groundwork for future negotiations and discussions on a single Africa-Europe DSM. These discussions should also include multilateral initiatives on data protection, promoting broader dialogues on data transfers beyond the stringent standards of the General Data Protection Regulation (GDPR).

4.4. Increase support on pilot projects and invest in digital ID

The pilot project on digital ID under the Smart Africa flagship is supported by Team Europe, GIZ, with Cybernetica, Orange and SK-ID having contributed to the drafting of the blueprint. In Djibouti, GovStack is developing prototypes for two use cases, one on the implementation of an e-cabinet and another on the digitisation of construction permits. Somalia partnered with GovStack on two priority use cases on digitisation of high school certificates and the development of a content management system. To increase its participation and cooperation, Team Europe must increase its support for more digital ID pilot projects. Such projects should be guided by the understanding that each African country has its unique needs and challenges which can impact its approach to digital ID rollout. Instead of replicating programmes from other countries, each pilot project should prioritise developing use cases relevant to a country's context and offering 'African solutions to African problems' (Teevan 2023). This would mean that the EU needs to have bilateral discussions with each country of interest to identify priorities, the stage of digital ID development, and the country's vision to meet its digital ID goals. The pilot projects can be supported by programmes or initiatives which promote the overall development of that country's digital infrastructure.

4.5. Provide technical support on data protection

The protection of digital ID data is critical. There are several ways for Team Europe to support African countries. First, Team Europe can approach the remaining 15 African countries without data protection laws and offer support to draft and promulgate data protection laws. Secondly, for other African countries, Team Europe can support the implementation of these laws (providing technical support in the setting up of data regulators). Some of the initial work in this area includes a Team Europe data protection awareness training in Nigeria and capacity building of data regulators in East Africa, or GIZ support to the Smart Africa Digital ID Blueprint, as well as the AU Data Policy Framework (D4D hub 2023a; D4D hub 2023b). In providing and scaling up this support, Team Europe should refrain from exporting the GDPR to Africa but allow African countries to develop data protection frameworks in line with their national laws and adherence to the continental frameworks on data protection. In our previous work, we also proposed that the EU should move from supporting a few countries in setting up their data protection authorities to a broader discussion regarding the future of EU-Africa data flows (Musoni et al. 2023). These discussions are a priority and strategic for the EU-Africa relations in light of the implementation of the AfCFTA. If the EU wishes to benefit from the African Digital Single Market, it needs to take the issue of data transfers seriously and negotiate a framework with favourable terms permitting data transfers between the two economic blocks.

4.6. Support investments in capacity building and skills

African countries face a huge digital skills shortage due to the digital divide and lack of technical programmes on digital skills development. If the majority of users of digital ID are not digitally skilled to navigate online platforms, they will not be able to take advantage of the benefits of the digital economy. Similarly, most people working in government also lack the digital skill sets needed to provide support to users of services. There are shortages of skilled data scientists, IT personnel, and cybersecurity specialists in governments. To address the digital skills

shortage, Team Europe, through the Global Gateway investment package can provide financial support for tailored digital skills programmes targeting diverse demographics including schools, colleges, and universities. Special programmes can be designed to support initiatives that promote digital literacy, particularly in rural and economically disadvantaged communities. Through collaborative efforts with African governments, skills development programmes for government employees can be designed and implemented across various government departments to address the skills shortages. This approach ensures that both the general population and government officials acquire the necessary digital skills to fully participate in and benefit from opportunities in the digital economy.

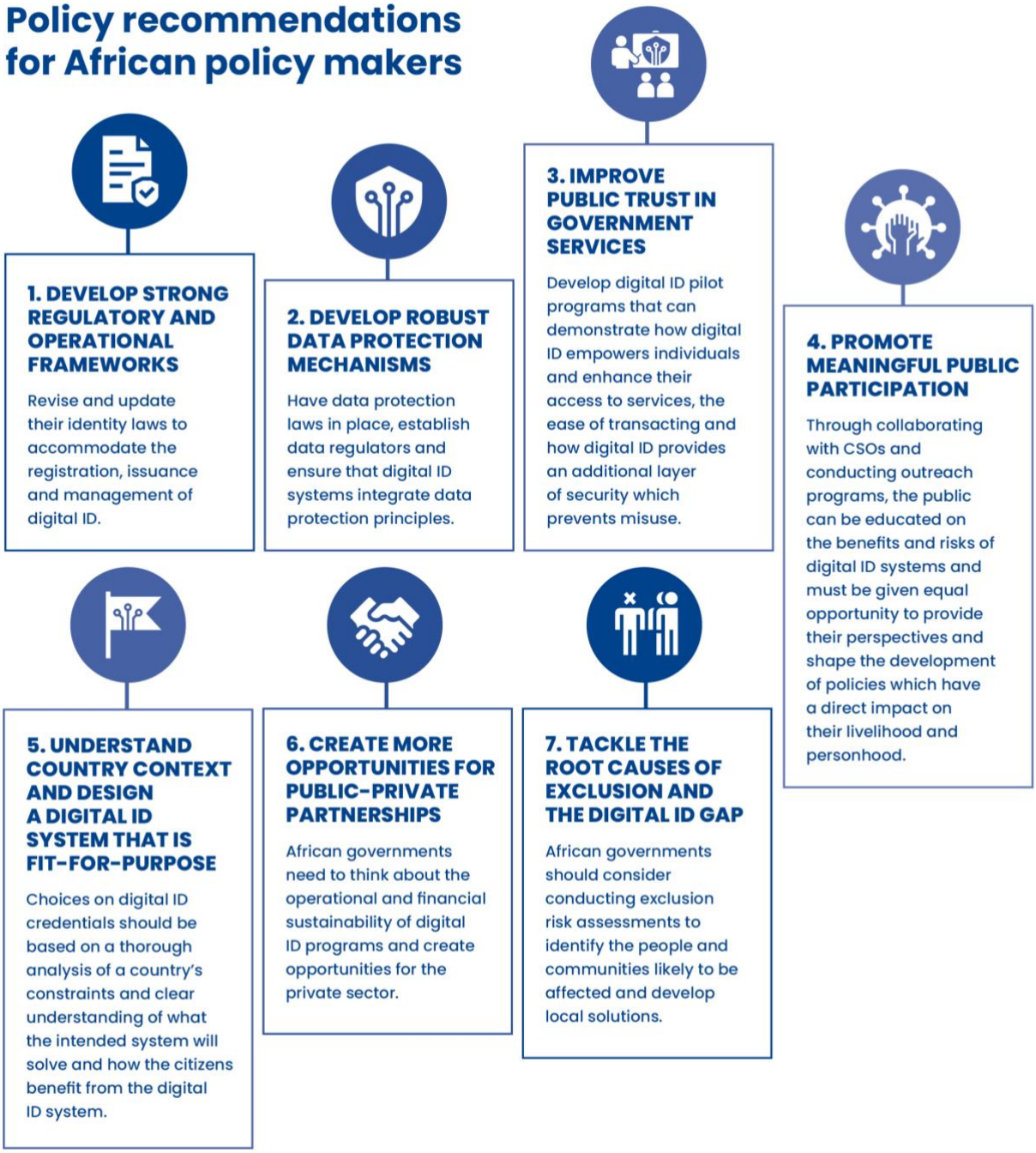
4.7. Play a role in developing donor complementarity

As a growing number of donors in Africa seek to play a role in the roll out of digital identity, e-governance and what some call digital public infrastructure, there is a threat that donors putting forward competing offers end up causing unnecessary duplication of efforts. It is vital for poorly resourced countries, that often rely heavily on external support to develop these systems, that competition between donors is not causing unnecessary wastage. The EU should work closely with other key donors, including notably the World Bank and UN agencies, to ensure that this is not happening. While there may be some differences in approach with these other donors, it should still be possible to engage in a concerted manner and to share information that ensures that each donor is playing a complementary role.

5. Policy recommendations for African policymakers

There is a clear commitment from African governments and their partners to accelerate the implementation of digital ID systems across Africa, with new top-down incentives led by the AU and RECs, and international partners such as the World Bank, emerging to create demand for the roll-out of e-ID systems. However, the experiences of countries that are in the process of developing their own national system show that by failing to meet the infrastructural and regulatory prerequisites for the implementation of ID systems, African governments put citizens at risk of exclusion, privacy violations and other harms.

Figure 9: Policy recommendations for African policymakers



Source: ECDPM

5.1. Develop strong regulatory and operational frameworks

The first step for African countries is to revise and update their identity laws to accommodate the registration, issuance, and management of digital IDs. The changes must align with principles on data protection, international best practices on developing good digital ID and AU frameworks as this promotes coherence and coordination at a

continental level. To promote the demand for digital IDs, all actors in the public and private sectors must be encouraged to recognise digital IDs for transactional purposes and make offline or remote credentialing available.

Instead of African countries applying different standards on digital IDs, the AU should set up a Specialised Technical Committee on Digital ID (STC-Digital ID) which can develop minimum standards on technical, operational and legal requirements which can complement the AU Interoperability Framework (WB 2022a). The minimum standards must pertain to biometrics, Smart ID cards, barcodes, digital signatures, or a continental digital ID wallet. At present, countries apply different standards for digital IDs. The STC-Digital ID can consult with the Smart Africa Trust Alliance and other international and national standards-setting bodies for technical guidance.

5.2. Develop robust data protection mechanisms

Digital ID systems must be developed under the guidance of strong and agile legal and regulatory frameworks which protect individual data, provide clear mandates and accountability, ensure adequate security safeguards and promote the rights of individuals, especially consent, access and notification.

First, African countries which have not embarked on digital ID programmes must prioritise implementing a data protection law which protects different aspects of personal data. Important data protection principles of accountability, lawfulness, purpose limitation, transparency, fairness, data minimisation, accuracy and security must be embedded in digital ID programmes. The laws must also create an obligation for data controllers to conduct Data Protection Impact Assessments (DPIAs) or privacy assessments (Gakunga 2023), before the rollout of digital ID systems and during the digital ID lifecycle. Third parties or relying parties gaining access to digital ID data must be subjected to very strict data compliance requirements.

Second, African countries must establish data protection regulators with oversight over all data processing activities in their countries. These should be given enough legislative power to carry out their functions without fear, favour or prejudice. Identity institutions must work closely with data protection authorities and seek guidance on compliance with the law.

Third, at a more institutional level, ID institutions must have clear organisational policies which ensure that data privacy and security measures (such as privacy-enhancing technologies) are integrated throughout the lifecycle of digital ID and important data protection principles are implemented as part of organisational culture. This can also extend to providing training for front office employees dealing with people on a regular basis and providing them with detailed operational manuals (WB 2019a).

5.3. Improving public trust in government services

Several ID institutions across Africa are facing challenges of lack of skilled resources, administrative inefficiencies and incompetencies, and in some cases corruption. At the same time, there are concerns about possible surveillance as governments can easily trace an individual based on their digital trail. To enhance public confidence in digital ID, African governments should prioritise promoting transparency, privacy, data protection and robust cybersecurity measures. People can only trust a system if they understand the benefits of that system, how the system processes their data, how the data is used or with whom it is shared and what is being done to secure the data against criminal actors. Active stakeholder engagements can also create an environment of trust (WB 2019a). Governments can start with digital ID pilot programmes that demonstrate how digital ID empowers individuals and enhances their access to services, the ease of transacting and how digital ID provides an additional layer of security which prevents misuse. Supporting domestic small, medium and macro enterprises and innovators to develop customised digital products

and solutions for services like finance, health, and social services is crucial for widespread acceptance. African governments also need to demonstrate that they have resilient cybersecurity systems capable of thwarting any cyberattacks and safeguarding against data breaches, this is pivotal in instilling public confidence in digital ID frameworks.

5.4. Promote meaningful public participation

Most digital ID projects in Africa are being conducted without any meaningful public consultation, engagement and receiving feedback. For instance, South Africa's draft ID Policy was not subject to vigorous public consultations. The effect of this is that developed digital ID programmes may not always align with constitutional principles, as happened with Kenya's Huduma Namba or do not address the specific needs of people.

African governments should support or collaborate with CSOs and conduct outreach programmes to educate the public on the benefits and risks of digital ID systems, offering them equal opportunities to provide input and shape the development of policies which have a direct impact on their livelihood and personhood (WB 2019a; WB 2022c). This should be complemented by active coordination and consultation with interested stakeholders on the basis of their different operational needs and priorities (WB 2022b). Several stakeholder workshops must be conducted with representatives from government departments, institutions, ministries, and strategic regulators like data regulators and the private sector. Establishing a multi-stakeholder digital ID committee working in tandem with various technical groups as suggested by Atick (2016) can enhance project efficiency. Given the political complexity of digital ID projects, it is important to have strong government leadership and champions at the highest levels of government to coordinate the adoption, implementation and integration of such projects across the different levels of government and prevent fragmented, duplicated and wasteful efforts (Theodorou 2023; WB 2017a).

5.5. Understanding the country context and designing a digital ID system that is fit-for-purpose

African countries are at different levels of technological development and digital transformation. Some are more advanced than others in the use of technological tools and solutions. Digital ID systems must be designed to meet the needs of the people and communities they are intended to serve. African countries should tailor their digital ID systems to their specific technological development levels and local needs. Rather than replicating digital ID programmes from other countries, each African country should undertake a comprehensive analysis of its constraints, ensuring that the chosen digital ID credentials align with the unique needs, challenges, and risks faced by its citizens (WB 2022b). African countries should offer a range of digital ID credentials (smart cards, 2D barcode cards, and mobile tokens) to cater for different circumstances of the citizens, while also making it possible for new innovative credentials to enter the market. Finally, African countries with challenges of internet access and availability of digital ID technology must develop strategies and programmes to reach remote areas and implement offline solutions (GPFI 2018). This also avoids unnecessary expenditure and wasting of resources, for example, premature design and printing of smart cards for a population that does not need such cards (Atick 2016).

5.6. Creating more opportunities for public-private partnerships

It is expensive to roll out digital ID programmes as well as to operate and maintain biometric databases and digital ID systems. African governments need to prioritise operational and financial sustainability, exploring opportunities for private sector involvement. Public-private partnerships (PPPs) play a crucial role in achieving cross-border interoperability of digital ID systems, particularly in use cases like digital financial services (for example, mobile money, banking, and insurance). Leveraging the presence of private sector entities such as Vodacom, Orange, MTN,

Standard Bank, Safaricom, FNB Bank, and Western Union, operating across several African countries facilitates seamless interoperability of digital ID systems. Due to financial constraints, some African countries may not have the infrastructure or the means to run their own data centres where biometric databases, national population registers and identity systems are stored. PPPs can offer sustainable solutions for data storage, ensuring accessibility and security, with an emphasis on ideally establishing in-country data centres.

5.7. Tackling the root causes of exclusion and the digital ID gap

Identity projects arise within a particular social and political history of exclusion for many African populations (Razzano 2021b). A gap exists with foundational ID and will be widened by the uptake of digital ID. The identification gap is a cross-cutting risk that should be addressed during the early stages of the adoption of digital ID systems in Africa. To mitigate this risk, African governments should be systematic in how they address exclusion problems by relying on evidence-based policymaking. This includes conducting comprehensive exclusion risk assessments to identify vulnerable groups, including women, girls, the disabled, the elderly, IDPs, nomadic communities, people living along national borders, and refugees. The gathered evidence should inform the development of targeted local strategies to reach these excluded populations. African governments should also explore providing offline digital ID solutions to ensure inclusivity and accessibility across diverse communities.

6. Conclusion

Over the past few years, the digital ID ecosystem in Africa has become a very dynamic ecosystem with the potential to grow in the coming years as digital transformation increases further the demand for such infrastructure. Developing a digital ID system to achieve sustainable development is a high priority for African governments. The growth of the digital economy and implementation of digital ID systems is a process that is pushing the update and implementation of data protection legislation as issues around the safe flow of data across borders and the use and storage of personal data have raised concerns over citizens' right to privacy.

Furthermore, the implementation of digital ID systems and their potential to catalyse Africa's economic development are well documented, but there has been less attention paid to the risks that such systems present for vulnerable communities, who face discrimination in accessing foundational ID systems and thereby cannot access government services. The diversity of African governments' political and social contexts calls for more tailored research to understand why some governments are behind in the implementation of ID systems and regulatory frameworks for the governance of such infrastructure. In this research, we have presented some of the challenges that are hindering the uptake of digital ID systems with a view of identifying opportunities for governments to introduce policy changes to improve key aspects of the roll-out of digital ID systems including issues around inclusion, oversight, transparency, interoperability and involvement of the private sector.

The current state of play of the digital ID system offers many opportunities for international actors such as the EU to support African governments' efforts at setting up the infrastructure for digital ID, the design of the system and the update or implementation of data protection and data privacy legislation. Ultimately, what this paper showed is that each African country faces different challenges and that any support should be preceded by a thorough analysis of the challenges that the ID system could face. Working closely with pioneers of digital ID implementation in Africa is essential to understand better why some governments are behind in the adoption of digital ID systems. In this process, there are some trends that can give insights into the areas that African governments and their partners – including the EU – should focus on as part of their digital partnership.

In short, to develop fit-for-purpose digital IDs, governments should ensure public participation throughout the process, set up data protection laws to secure individuals' digital rights as well as trust with digital ID institutions, promote strong public-private partnerships to create demand for digital ID and achieve the financial sustainability of the digital ID infrastructure. The EU can play a unique facilitating and capacity-building role in expanding the roll out of digital ID systems by leveraging its diplomatic ties with African governments. Yet to be able to do so, it has to promote more exchanges between European and African regulators, governments and the private sector. Finally, there are two areas that can have a significant impact in this area which go beyond regulatory support – the EU's area of strength – namely digital skills, as well as support to African CSOs working on digital rights. While there is a high demand for digital skills across Africa, and in particular in the selected case studies, there are little resources allocated to this area. Similarly, if the EU wants to support the implementation of human-centric digital ID systems, it should strengthen its engagement with CSOs working on digital rights, and promote exchanges at the EU policy level.

References

Abuya, K. 2023. Kenya discontinues Huduma Namba, takes another try at digital identities. Techcabal. 2 June 2023.

Access Now. 2022. Open letter: World Bank and its donors must protect human rights in digital ID systems. 7 March 2023.

Access Now. 2023. Past learnings must be 'at the heart of implementing' a digital identity system in Kenya. 24 May 2023.

Adjovi, S. 2019. The Benin recipe and challenges for electronic and biometric identification data capture. ID4Africa.

African Union (AU). 2014. African Union Convention on Cyber Security and Personal Data Protection.

African Union (AU). 2022. AU interoperability framework 2022.

African Union Commission (AUC). 2015. Agenda 2063: the Africa we want. September 2015.

Agence Française de Développement (AFD). N.d. Modernizing and Harmonizing National Digital Identification Policy.

Aljazeera. 2022. In Cameroon, refugees get a new lease of life with digital IDs.

ALT Advisory. 2022. The Malabo Roadmap.

Angira, Z. 2023. One number with all your life's details. People Daily. 1 February 2023.

Aparo, A. 2023. Uganda's Digital ID System Hinders Citizens' Access to Social Services. Cipesa

APDP. 2009. Law n° 2009-09. Beninese Data Protection Authority. 22 May 2009.

APDP. 2018. Law n° 2017-20 of 20 April 2018. Beninese data protection authority.

Assemblee Nationale. 2017. Des procedes d'identification des personnes physiques. 19 Juin 2017.

Atick, J. 2016. Digital Identity: the essential guide. ID4Africa.

Bénin Révélé. 2021. Government Action Programme 2021-2026. Cotonou: Presidency of the Republic of Benin.

Burt, C. 2018. Vendor lock-in hindering African identity projects. Biometricupdate. 13 June 2018.

Burt, C. 2019. Two ideas to break down vendor lock-in in foundational biometric ID systems launch at ID4Africa 2019. Biometricupdate. 20 June 2019.

Burt, C. 2020. Biometric verification reveals 10k ghost workers on Zimbabwe public payroll. Biometricupdate. 23 December 2020.

Burt, C. 2023. Kenya signs digital ID support deal with UNDP, introduces a new Namba. Biometricupdate.com. 14 August 2023.

Chowdhury, A. Lawson, C. Kellison, E. Sheng Chia, H. Kharas, H. Fuller, J. Faye, M. Rutkowski, M. Salvado, R. and Dercon, S. 2022. Accelerating digital cash transfers to the world's poorest. Brookings. 17 February 2022.

CHRGJ.2022. Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID Center for Human Rights & Global Justice.

Cybernetica. 2021. Namibia Governmental Interoperability Framework Nam-X. 5 August 2021.

Citizen TV Kenya. 2023. ICT CS Owalo speaks on the government digital agenda (Part 1). YouTube.

Communications Authority of Kenya (CA). 2023. Joint Statement on Operations of the Worldcoin in Kenya. Government of Kenya.

Data Protection Africa. N.d. Mapping 55 African countries| 35 data protection laws| 3 draft laws.

Desai, V. Metz, A. and Lu, J. 2018. The global identification challenge: Who are the 1 billion people without proof of identity? World Bank (WB). 25 April 2018.

D4D Hub. 2023a. Team Europe and Nigeria collaborate to enhance data protection awareness. 8 November 2023.

D4D Hub. 2023b. Strengthening Data Protection Across East Africa: A Knowledge Exchange Between Data Protection Authorities. 13 September 2023.

Domingo, E. and Tadesse Shiferaw, L. 2022. Digitalisation and democracy: Is Africa's governance charter fit for the digital era? ECDPM Discussion Paper No. 331. Maastricht: ECDPM. November 2022.

Dube, M. 2023. Botswana, Namibia Agree to Abolish Passports for Citizens Crossing Border. Voice of America (VOA) News.

EGA. 2014. Estonia to construct secure data exchange layer X-Road for Namibia. Estonia e-Governance Academy. 29 October 2014.

EGA. 2021. Governmental Interoperability in Namibia. Estonia e-Governance Academy

Egole, A. 2023. 5,500 enrollment centers active nationwide - NIMC. Punchng, 27 July 2023.

Elimian, G. 2023. Nigeria's Prembly partners Namibia's financial regulator to build a digital identity framework for the country. Technext24

Endjala, M. 2023. MTC defies CRAN. Observer24.

EU. N.d. EU Digital Identity Wallet Pilot implementation. European Union. Accessed 22 November 2023.

EU. 2021. Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. European Union. 3 June 2021.

EU. 2023. European Digital Identity: easy online access to key services. European Union.16 March 2023.

European Investment Bank (EIB). 2018. Nigeria digital ID.

Floyd, R. Mussoni, M. 2023. Towards an African digital single market: Opportunities for the AU-EU partnership. ECDPM Policy Brief No. 167. October 2023.

Freedom House. N.d. Explore the map.

Gagliardone, I. Stremlau, N. 2022. It's Time to Revisit the Framing of Internet Shutdowns in Africa. Carnegie.

Gakunga, E. 2023. Kenya's New National Digital ID system Presents Challenges and Opportunities in Equal Measure. Jurist. 18 July 2023.

Government of Ethiopia. N.d. National ID. Accessed 21 November 2023.

Government of Kenya. 2019a. National Information, Communications and Technology (ICT) Policy. Ministry of Information, Communications and Technology, Government of Kenya. November 2019.

Government of Kenya. 2019b. Kenya Gazette Supplement. Acts, 2018. No. 161. Republic of Kenya. 4 January 2019.

Government of Kenya. 2020. Republic of Kenya in the High Court of Kenya at Nairobi Constitutional & Judicial Review Division. Consolidated petitions No. 56, 58 & 59 of 2019. Republic of Kenya. 30 January 2020.

Government of Kenya. 2021. Republic of Kenya in the High Court of Kenya at Nairobi (Milimani Law Courts) Judicial Review Application E1138 of 2020. Republic of Kenya. 14 October 2021.

Government of Kenya. 2022. The Kenya National Digital Master Plan 2022-2032. Ministry of ICT, Innovation and Youth Affairs, Government of Kenya.

Government of Namibia. 2005. The e-Governance Policy for the Public Service of Namibia.

Government of Namibia. 2014. e-Government Strategic Action Plan for the Public Service of Namibia (2014-2018). April 2014.

Government of South Africa. 1997. Government Gazette. N0. 18485. Republic of South Africa. 3 December 1997.

Government of South Africa. 2006. Policy on free and open source software use for the South African Government. Department of Public Service and Information, Republic of South Africa.

Government of South Africa. 2007a. Handbook on minimum information interoperability standards (MIOS). A blueprint to guide seamlessness and interoperability in public service as presented by The Department of Public Service. Department of Public Service and Information, Republic of South Africa.

Government of South Africa. 2007b. Minimum information interoperability standards (MIOS) for information systems in Government. Department of Public Service and Information, Republic of South Africa.

Government of South Africa. 2012. National Development Plan 2030. Our future - make it work. National Planning Commission - The Presidency Republic of South Africa. 1 September 2012.

Government of South Africa. 2019. White Paper on Home Affairs. No. 8. Department of Home Affairs, Republic of South Africa. 18 January 2019.

Government of South Africa. 2020. Draft official identity management policy. Public consultation version. No. 1425. 31 December 2020. Department of Home Affairs, Republic of South Africa.

Government of South Africa. 2023. Publication of the National Identification and Registration Bill, 2022. Department of Home Affairs, Republic of South Africa.

GPFI. 2018. G20 Digital Identity Onboarding. Global Partnership for Financial Inclusion.

GSMA. 2016. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. GSMA- World Bank Group. July 2016.

GSMA. 2019. Digital Identity Country Report: Malawi. GSMA.

GSMA. 2022. The State of Mobile Internet Connectivity 2022. GSMA.

Hersey, F. 2023. Kenya Huduma Namba funding almost entirely cut as UPI, digital birth registration begins. Biometricupdate.com. 1 March 2023.

Howson, K. and Partridge, A. 2022. Policy Brief: Digital identification and rights realisation in South Africa. Cape Town: Research ICT Africa.

Hutchinson, J. Bellman, J. Hurst, S. 2019. The digital citizen; improving end-to-end public service delivery via a unique digital identity. Deloitte. 24 June 2019.

ID4Africa. 2019. A look at Benin eID Experience. 19 June 2019.

Information Regulator (South Africa). 2023. Infringement notice and R5 million administrative fine issued to the department of justice and constitutional development for contravention of popia.

International Telecommunication Union (ITU). n.d. Internet use in urban and rural areas.Accessed 21 November 2023.

IOL. 2017. Home Affairs set to investigate massive data breach. 19 October 2017.

Jaiyeola, T. 2022. 73% Africans in rural areas lack Internet access. Punch. 19 December 2022.

Jarrahi, J. 2021. Massive gender disparities in digital ID systems persist, ID4Africa panel says. 12 March 2021.

Kakaire, A. 2022. Countering Digital Authoritarianism in Africa. Cipesa. 10 November 2022.

Kenya News Agency. 2023. Plans for Kenyans to get new identifier by June 1. 15 May 2023.

King'ori, M. 2022. How the Kenyan High Court (temporarily) struck down the National Digital ID Card: Context and analysis. Future of Privacy Forum. 8 February 2022.

LAC. 2001. Identification Act 21 of 1996 - Identification Regulations 2001-096.Legal Assistance Centre. 18 May 2001.

LAC. 2019. Electronic Transactions Act 4 of 2019. Legal Assistance Centre. 17 November 2019.

Mabuza, E. 2018. Transport department emerges victorious in eNaTIS Con-court battle with Tasima. Times Live. 18 July 2018.

Macdonald, A. 2023. Benin issues digital IDs to citizens living abroad. Bionetricupdate. 27 July 2023.

Malik, T. 2020. Malawi's Journey Towards Transformation. Center for Global Development (CGDEV). August 2020.

McKane, J. 2018. ID and cellphone numbers leaked on Home Affairs website. 19 April 2018.

MICT. 2022. Publication of the Draft Data Protection Bill, 2021. Ministry of Information and Communication Technology.

Musoni, M. 2023. Looking into the crystal ball: Artificial intelligence policy and regulation in Africa. ECDPM Commentary. Maastricht: ECDPM. 18 September 2023.

Musoni, M. Karkare, P., Teevan, C. and Domingo, E. 2023. Global Approaches to Digital Sovereignty: competing definitions and contrasting policy. ECDPM Discussion Paper No. 344. Maastricht: ECDPM. May 2023.

MOSIP. N.d. The MOSIP Project.

Mungadze, S. 2021. Damning report reveals EOH manipulation of R400m tender. ITWeb Africa. 26 May 2021.

NBS. 2022. Nigeria launches its most expensive national measure of multidimensional poverty. Press Release. 17 November 2022.

Nakashole, P. 2021. New ID card launched. The namibian. 19 November 2021.

Namiblii. 1996. Identification Act, 1996. 22 November 1996.

NAN. 2017. NIMC, UNHCR to enroll 100,000 displaced persons in e-identity card. The Guardian.

NDPC. 2023. Federal Republic of Nigeria Official Gazette. No.119. Vol. 110. 1 July 2023.

NDPC. N.d. DPCO Registration and Requirements. Accessed 22 November 2023.

Ndemo, B. Ndung'u, N. Odhiambo, S. and Shimeles, A. 2023. Data Governance and Policy in Africa. Palgrave Macmillan.

NIMC. N.d. Harmonization Integration Policy. National Identity Management Commission.

NIMC. 2007. National Identity Management Commission Act 2007. National Identity Management Commission.

NIMC. 2010. The NIMS Strategy and Technology Document. National Identity Management Commission. August 2010.

NIMC. 2011a. Harmonization and Implementation Committee National Identity Management System. Biometrics Standards and Specifications. National Identity Management Commission. 11 February 2011.

IMC. 2011b. National Identity Management System Handbook on Business Processes, Standards and Specifications. National Identity Management Commission. 6 January 2011.

NIMC. 2017a. A Strategic Roadmap for Developing Digital Identification in Nigeria. National Identity Management Commission. June 2017.

NIMC. 2017b. Federal Republic of Nigeria Official Gazette. No. 121. Vol. 104. 13 November 2017.

NIMC. 2017c. Federal Republic of Nigeria Official Gazette. No. 122. Vol. 104. 14 November 2017.

NIMC. 2019. Schedule of fees for NIMC services. December 2019.

NIMC. 2020. World Bank Approves Nigeria's Identity Project, Five Others. 19 February 2020.

NIMC. 2021. Revised National Identity Policy Form Sim Card Registration. Government of Nigeria. National Identity Management Commission.

NIMC. 2023b. Diaspora Services Fact Sheet. 18 April 2023.

Njoya, S. 2022. Benin cancels issuance of non-biometric cards. 11 July 202.

Nortal. 2022. The X-Road infrastructure is used by public authorities in the digital showcase state of Estonia to exchange data. The software is now also being tested in Germany.

OHCHR. N.d. International Covenant on Civil and Political Rights. United Nations Human Rights office of the High Commissioner (OHCHR). Accessed 21 November 2023.

Omidyar Network. 2017. Digital Identity and Privacy. 14 October 2017.

Onwuaso, U. 2018. Lack of Funds Stops Nigerians from Getting e-ID cards —NIMC boss. Nigeria Communications Week. 24 April 2018.

Otieno, S. 2023. Digital IDs will help us improve service to citizens, President Ruto says. Nation. 25 May 2023.

Paradigm Initiative. 2021. Data Protection Authorities (DPAS) in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of Their Existence on the Continent.

Paradigm Initiative. 2022. Londa: Digital Rights and Inclusion in Africa report.

Parliament of Namibia. 2023. Civil Registration and Identification Bill.

Privacy International. 2019. Timeline of SIM Card Registration Laws. 11 June 2019.

Razzano, G. 2020. Good ID and Financial Inclusion: a call for context. Research ICT Africa. 5 February 2020.

Razzano, G. 2021a. Digital Identity in South Africa. Research ICT Africa.

Razzano, G. 2021b. AI4D- Digital and Biometric Identity Systems. Research ICT Africa.

Saka, S.. 2021. Londa: Benin Digital Rights and Inclusion. Lagos: Paradigm Initiative. April 2021.

Schwab, K. 2016. The Fourth Industrial Revolution: what it means, how to respond. World Economic Forum (WEF). 14 Jan 2016.

Seck, M. 2023. Dite for Africa. UNECA.

Service Public. N.d. e-Services. Accessed 22 November 2023.

SGG. 2020. Décret No 2020-396 Du 29 Juillet 2020. Secrétariat Général du Government.

SIHMA. N.d. Exclusion of Migrant Women in Africa: Access to Identity Documentation for Migrant Women. Accessed 21 November 2023.

Smart Africa. 2020. Blueprint: Smart Africa Alliance - Digital Identity.

Statista. 2023a. Number of internet users in selected countries in Africa as of January 2023, by country. Statista Research Department. 22 September 2023.

Statista. 2023b. Number of internet and social media users worldwide as of October 2023. Statista Research Department. 25 October 2023.

Statista. 2023c. Percentage of individuals using the internet worldwide and in rural and urban areas as of 2022, by region. Statista Research Department. 21 February 2023.

Sullivan, C. 2011. Digital Identity: An Emergent Legal Concept. University of Adelaide Press.

Tanager. 2023. National Identity Cards as a Critical Step Toward Economic Empowerment. July 2023.

Tanzania Communication Regulatory Authority (TCRA). 2020. The Electronic and Postal Communications (Sim Card Registration). 7 February 2020.

Theodorou, Y. 2022. On the Road to Digital-ID Success in Africa: Leveraging Global Trends. Tony Blair Institute for Global Change. 13 June 2022.

Theodorou, Y. 2023. Ten Actions Countries Should Take to Create a Digital-Identity Ecosystem. Tony Blair Institute for Global Change. 16 July 2023.

UNECA. N.d. Concept note on the EAC on Digital Identity, Trade and Economy Initiative and Center of Excellence. United Nations Economic Commission for Africa.

UNICEF. 2020. A Statistical Profile of Birth Registration in Africa. Division of Data, Analytics, Planning and Monitoring. United Nations Children's Fund. November 2020.

UN. N.d.- a. Universal Declaration of Human Rights. United Nations. Accessed 21 November 2023.

UN. N.d. -b. Goal 16| Department of Economic and Social Affairs. United Nations. Accessed 21 November 2023.

UNDP. 2023. Digital Public Goods for the SDGs: Emerging Insights on Sustainability, Replicability & Partnerships. United Nations Development Programme.

UNDP. 2023b. UNDP Unveils Digital Public Infrastructure Portfolio and Signs MOU to Drive Inclusive Digital Transformation. United Nations Development Programme.

van der Spuy, A. Bhandari, V. Trikanad, S. and Tshering Paul, Y. 2021. Towards the Evaluation of Socio-Digital ID Ecosystems in Africa. Research ICT Africa.

WB. 2016. Namibia Identity Management System Analysis Report. World Bank.

WB. 2017a. The State of Identification Systems in Africa. World Bank.

WB. 2017b.Technical Standards for Digital Identification. Draft for Discussion. World Bank.

WB. 2018a. African Leaders, the World Bank Group, and partners catalyze action to ensure that everyone in Africa has a digital identity by 2030. World Bank.

WB. 2018b. Understanding Cost Drivers of Identification Systems (English). World Bank.

WB. 2019a. Digital ID and the Data Protection Challenge. World Bank.

WB. 2019b. Practitioner's Guide. World Bank.

WB. 2021a. Principles on Identification for Sustainable Development: Towards the Digital Age. World Bank.

WB. 2021b. Annual Report. World Bank.

WB. 2022a. Catalog of Technical Standards for Digital Identification Systems. World Bank.

WB. 2022b. A Digital Stack for Transforming Service Delivery: ID, Payments, and Data Sharing. World Bank. 22 February 2022.

WB. 2022c. Engaging Civil Society Organizations (CSOs) for Successful ID systems: Guidance Notes. World Bank.

WB. 2023a. The West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program: Unique identifiers to Enable Access to Human Development Services. World Bank.

WB. 2023b. Nigeria Digital Identification for Development Project. World Bank.

Xinhua. 2023. Botswana, Namibia launch usage of national identity cards for cross-border travel. 25 February 2023.

X-Road. N.d. Global.

Yousif, M.M. 2022. Huduma Bill: Opportunity to Shape Law on Identification Systems and Inclusion. Namati. 19 February 2022.

About ECDPM

ECDPM is an independent 'think and do tank' working on international cooperation and development policy in Europe and Africa.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of ECDPM and can under no circumstances be regarded as reflecting the position of the European Union. This publication also benefits from the structural support by ECDPM's institutional partners: Austria, Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, The Netherlands and Sweden.

ISSN1571-7577

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Avenue des Arts 44, 1000
Brussels *Bruxelles*
Belgium *Belgique*
Tel +32 (0)28 825 008

info@ecdpm.org
www.ecdpm.org
KvK 41077447