
# Landscaping a digital financial identity for SADC

10 January 2018

**Research done by:**
Bankable Frontier Associates, LLC (BFA)
259 Elm Street, Suite 200
Somerville, MA 02144 USA
617 628-0711
www.bfaglobal.com

# Contents

## 1. INTRODUCTION

The target of providing legal identity for all people by 2030 is now a part of the UN Sustainable Development Goals (SDG) framework adopted in 2015[1]. To reach this target, the World Bank estimates that 1.1 billion people will need to receive a form of identification.[2] Of this total, 138 million live in SADC countries today.[3] This shortfall matters since the presence of accessible legal identity is considered a cornerstone of a peaceful society, as the basis for trusted voting procedures, anti-crime measures, as well as an inclusive environment, since robust identity enables citizens to qualify for and receive social benefits and responsibilities. In the financial sector, regulators' drive to promote financial integrity has led to the adoption of higher standards of Know Your Customer (KYC) laws and regulations, all of which rest on the ability of providers to identify clients correctly as the basis of starting a relationship, opening an account with a formal Financial Service Provider (FSP), or getting access to credit from an FSP based on available credit information. Clients may be individuals managing personal finances or small, medium or micro enterprises (SMMEs).

The SDG target neither specifies that identity should be issued by a national government (a national identity) nor does it specifically mention the ways in which the identity could be asserted, for example allowing for digital channels. However, as more people connect online and as societies and governments digitize their relationships and transactions, so the need for effective forms of digital identity have grown: an identity which can be used securely, robustly and conveniently online.

This report does not argue the general benefits for having universal legal identity – that case has been argued cogently elsewhere.[4] Rather, in this report, we seek to focus on a more specific and

[1] SDG Target 16.9
[2] See http://www.worldbank.org/en/programs/id4d
[3] World Bank ID4D dataset https://data.worldbank.org/data-catalog/id4d-dataset
[4] See list of benefits of having ubiquitous identity provided in http://www.worldbank.org/en/programs/id4d

potentially tractable subset of the wider identity issue in SADC countries: the identified pain points for which a **digital financial identity** might be a workable solution.

In that context, this report provides an introduction both to the identity landscape in SADC countries and to relevant sets of digital identity solutions internationally that incorporate financial use cases. This report aims to create a background of knowledge, information and language which can help catalyse debate within SADC over potential approaches to the creation of a digital identity which might be used in the financial sector across SADC countries at least. However, note first, that this report does not aim to be a full primer on digital ID: there are useful general resources already available listed in the Annex for those wishing to do further general reading. And second, this report explicitly does not recommend specific solutions or even solution sets for SADC: to reach valid recommendations would require further research into the needs and circumstances of SADC countries, which could be a next step after this. Rather it seeks to illustrate the broad solution spaces in the digital ID landscape to help inform the discussion over the paths that SADC could consider taking up based on regional fit and needs.

To get to that outcome, the report first sets out a framework for defining digital financial identity and its general use cases. Then, it considers in Section 3 the current available information about the drivers and needs in SADC identity environment. In Section 4, the report describes examples of solutions positioned on the digital ID landscape to inform SADC thinking. The Conclusion then summarizes some design principles arising from the review to be considered for SADC solutions; and suggests some potential directions for follow-up action.

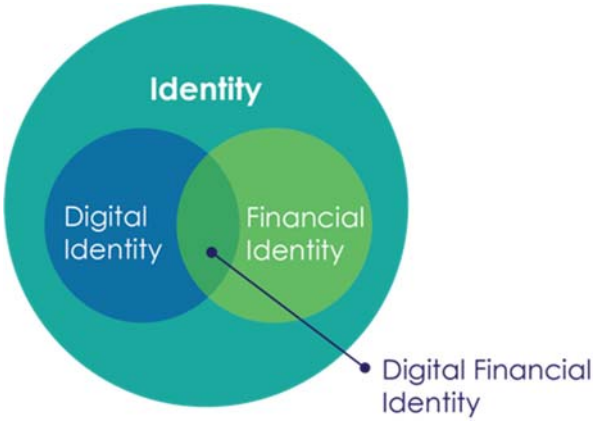
## 2. DIGITAL IDENTITY—WHAT IS IT AND HOW IS IT USED?

This section provides a succinct introduction to the core concepts and terms within identity so that readers who are less familiar may receive an introduction. This section focuses on those concepts relevant to the scope of this paper: those who wish to read further will find helpful the recent landscaping papers by Nyquist et al (2016) and US AID (2017), listed in the general references. Those who are already familiar with this introductory material may choose to skip to Section 3.

### 2.1 Definitions

At the broadest level, identity is simply the collection of attributes which uniquely identify an individual or legal entity such as an SMME or larger business for particular use cases. When some or all of these attributes are captured and stored digitally the composite resulting is known as a **digital identity**. A key use case for digital identity is to assert one's identity online by authenticating identity remotely without human interface. Not all digital identities are accepted or used in the financial sector, however, hence financial institutions may choose to create a form of sectoral or functional identity. Figure 1 below depicts how these concepts of identity are nested, with a digital financial identity, such as SADC is contemplating, sitting at the overlap of digital identity and financial identity.

**Figure 1: ID vs. digital ID vs. financial ID**




### *2.1.1 Digital identity*

Many common forms of identification today are not digitally enabled; in particular, many national identity systems operated by governments involve issuing credentials such as cards or passports or other documents which can only be verified physically. However, it is more common now to issue credentials which contain a chip or some machine-readable form factor which can be used to assert identity online. This is what digital identity refers to. That is, unlike paper documents, identifying attributes are captured in a digital system like a database from where the information is transferred to a chip or other machine-readable item like a barcode.

The use cases for digital identity cut across public and private-sectors. A digital ID can be used to pay taxes or other fees, receive social allowances or other payments. In the private sector, digital identities created by banks and other FSPs to authenticate their customers for online transactions are commonplace.

### *2.1.2 Financial identity*

Equally, financial identity is one particular form of functional identity – that is, a form which is issued by and relied on by financial sector players, such as banks. Financial identity functions within a trust framework developed by the financial sector suited to its purposes. One example of a trust framework is that used by financial institutions to open accounts for new customers. The financial institution relies on data about who the individual is in order to decide whether to do business with them; and the requirements within this framework are usually heavily influenced by AML-CFT regulations. Credit reference bureaus are another, whereby lenders rely on the information collated and presented by the bureau as part of establishing who a borrower is, and what their credit worthiness is. As a sub-category of functional identity solutions, financial identity is similar to other solutions developed to address specific use cases such as:

- ***voting****, w*here IDs are designed to ensure the integrity of electoral procedures;
- ***entitlement schemes***, in terms of which a beneficiary is able to assert a claim to a defined benefit, such as a government cash transfer;
- ***access to physical premises***, where a card or key signifies the right of entry to the specified individual;
- ***the right to drive a vehicle***, demonstrating that the necessary prerequisites have been fulfilled.

Functional identities do not carry the degree of acceptance of foundational identities. Usually, foundational identities are issued by governments as part of national identity schemes, and as the name implies, create a basis for reliance within functional schemes. National ID documents can therefore serve as 'breeder documents' which are used to verify identity within functional schemes.

In most countries, there is a proliferation of identity schemes for different purposes. This is not in itself a bad thing since the functional needs differ, as do their levels of assurance which we describe further below. But proliferation of schemes can lead to waste and inefficiency if functional schemes

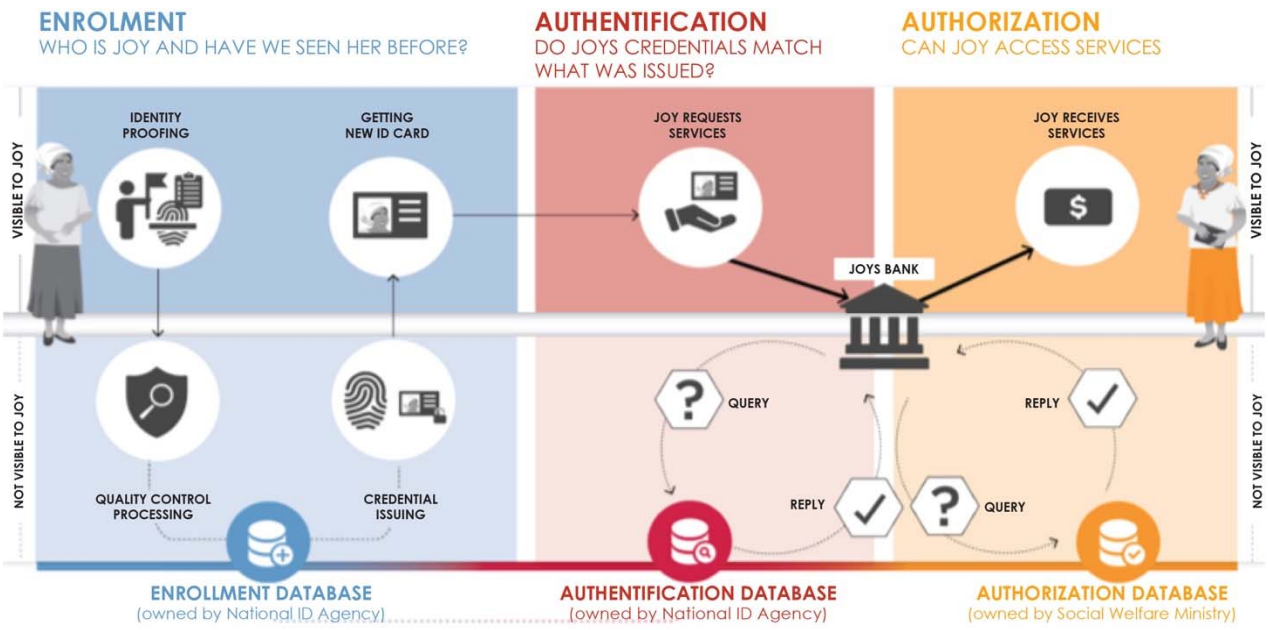
have to recapture and verify attributes which could be more efficiently accessed through a functional identity system with the appropriate attributes and channels for verification. Hence, donors which have supported different functional schemes in the past increasingly are thinking of ID schemes in the context of systems, which exist within a wider national or international ecosystem.[5]

So, even though the focus of this report is the case for a **digital financial identity**, which represents a particular subset of the identity space for SADC countries, the analysis needs to consider the wider identification system and use case ecosystem into which such a scheme would have to fit. We will pick up the background on SADC in section 3.

[5] See USAID report – Identity in a digital age: Infrastructure for inclusive development: https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

## 2.2 Identification lifecycle

### Figure 2: Identity process




*Source: USAID (2017)*

The standard life cycle of identity use within an identity scheme is depicted in Figure 2. It involves these three key steps:

1. ***Enrolment:*** this is the process by which defined attributes, such as full name, date of birth, current residential address, phone number, email, a national ID number are captured. This capture process may take place in person, using identity agents or registrars to verify physical documents and capture biometrics, for example, and/or remotely verifying details against other data sources, such as validating against a central birth register or against a national ID list for uniqueness. Successful verification leads to the ID provider issuing credentials. These

are the tokens which the user has to provide under the scheme – examples of these are a bank card or a national ID card, for example. For this reason, enrolment is sometimes known as ID proofing and verification (IPV).

2. ***Authentication:*** this next process applies when the user needs to assert her identity to a relying party. Authentication is the process of confirming that the user is who she claims to be; and the type of authentication required varies under different schemes, depending on the level of assurance required. Typically, authentication depends on the user providing credentials from one or more categories of factors. Typically, three categories of factors are recognized:
    a. Knowledge factors (what you know), such as a password or PIN number or the answer to a 'secret' question, which only you are meant to know;
    b. Possession factors (what you have in your possession) such as a card or a cell phone;
    c. Inherence factors (who you are), which include biometrics and behavioural analytics.

    In the early days of online banking, typically a username and password – both knowledge factors – were sufficient for authentication. But rising online fraud has led to the adoption of two-factor authentication as standard, in which a user name is presented together with a one-time password sent to a device known to be in your possession (typically a mobile phone).

3. ***Authorization:*** the final step in a transaction is authorization in terms of which the service provider, such as a bank or government agency, checks the authenticated identity against the rights attached to it, hence authorizing the holder of the authenticated credentials to transact on a specified account within the rules of that account.

Note that these three steps are really an extract of the longer life cycle of an identity scheme. In reality, a robust identity scheme requires ongoing steps to maintain the integrity of credentials by refreshing them (for example, re-issuing after an expiry date) as well as handling processes like

disputes and lost credentials. The eIDAS framework[6] adopted into law in Europe has set specifications and standards for each of the steps so that it is possible to assess adherence, and achieve acceptance and require reliance across national ID schemes in EU countries.

### 2.3 Levels of assurance for identification

We have mentioned above that the degree of certainty required in an identification process varies greatly with the risks faced by the party relying on the identification. There is no need for much assurance if one signs up for a free news service online for example, since no reliance is placed on that identity; but if money or legal obligations flow, then the level of assurance rises commensurate with the risk involved.

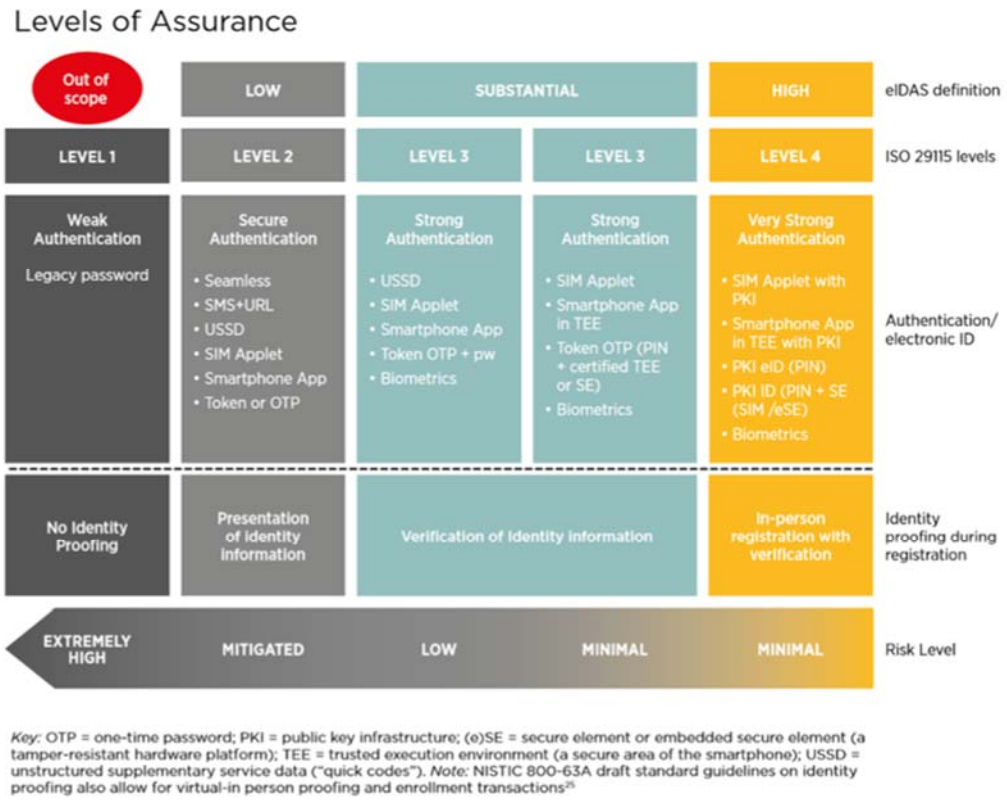
These degrees of certainty have been categorized into different levels of assurance, as depicted in Figure 3 below. The diagram shows four standard levels of increasing assurance, mapping them to the three eIDAS categories of low, substantial and high levels of assurance. Those levels can be translated into what is required during the authentication process to produce the required level. As the levels increase from left to right, more and varied factors are required in the digital authentication process adding security protocols on secure channels, as well as biometrics. Equally, the level of assurance is affected by the nature of the enrolment process which undertakes identity proofing at the outset: to reach the highest level of assurance, physical proofing is required i.e. no remote onboarding is allowed. However, remote onboarding may still lead to strong authentication.

In the financial sector, the level of assurance required depends upon the perceived risk and regulatory considerations. If an individual wants to open a low value bank account, then the level of assurance required is usually lower than if high value transactions are involved. In many countries, banks now require Level 2 assurance to authenticate online payment transactions, which is achieved by adding a

[6] See https://www.eid.as/home/

one-time password delivered to a different device. Higher levels of assurance are often preferred when financial use cases are applied across borders.

## Figure 3: Levels of assurance




*Key:* OTP = one-time password; PKI = public key infrastructure; (e)SE = secure element or embedded secure element (a tamper-resistant hardware platform); TEE = trusted execution environment (a secure area of the smartphone); USSD = unstructured supplementary service data ("quick codes"). *Note:* NISTIC 800-63A draft standard guidelines on identity proofing also allow for virtual-in person proofing and enrollment transactions[25]

*Source: World Bank and GSMA (2016) Figure 3*

# 3. SADC CURRENT REALITY

This section summarises the current available information on SADC's national identity environment. It discusses the various converging forces behind the case for a regional digital financial identity, outlines the current national identity environment across member states, highlights important regional trends and issues faced by FSPs, and puts together a basic framework to help stakeholders think about and prioritise the different use cases that a regional digital financial ID can address. The framework is intentionally incomplete as its aim is to encourage a healthy conversation that results in identifying use cases that are both relevant and important to SADC.

## 3.1 Driving forces in SADC

As a result of increased regional growth and integration through the years, there are rising forces that point to the case for a regional digital financial ID in SADC. Three key forces are discussed below.

### 1. Increasing digitization of financial services and growth of e-commerce

Financial services in terms of online and mobile banking, payments and remittances both local and cross-border, are on the rise. Cross-border remittances have grown especially due to high migration rates. Digital identification can ensure that transactions are linked accurately to the participants, increasing transparency and ultimately decreasing the risk of fraud.

According to GSMA, the adoption of smartphones in the SADC region is going to increase from a 28% adoption rate in 2016 to 58% in 2020. Mobile subscriber penetration is also due to increase from 42% in 2016 to 48% in 2020.[7]

[7] GSMA Mobile Economy - Sub Saharan Africa Report https://www.gsma.com/mobileeconomy/sub-saharan-africa-2017/

E-commerce has also gained popularity with orders being made both locally and across borders. This is linked to the surge in smartphone adoption and requires a robust form of digital identity management to authenticate buyers and sellers, and track payments and money flow.

### 2. Regional electronic payment arrangements have progressed

As of March 2017, SADC's regional RTGS – SIRESS – had 14 participating countries, 76 commercial banks and seven central banks. Madagascar is the only non-participant SADC member. The average value per transaction was a little over $315,000 and the total number of transactions settled since inception in July 2013 amounted to 712,099.[8]

The SADC Payment System Oversight Committee's (PSOC's) aim is to encourage greater bank participation especially for cross-border settlements. The SADC Bankers Association is promoting the establishment of a SADC regional ACH which will offer retail credit push transactions. As a result, the volumes of cross border payments are expected to rise in the future. This example illustrates what has already been done to create cross-border digital infrastructure as well as to create a driver for further standardization to boost rising volumes of cross border payments for trade and remittances.

### 3. Public policy drivers favour digital financial ID

In a push to formalize economies for tax purposes, a Memorandum of Understanding (MoU) on Cooperation in Taxation related matters entered into force in 2002 after 11 out of the 15 current SADC members signed the agreement. According to the MoU, member states should be transparent about their tax policies while creating incentives to increase regional integration. SADC hosts a

[8] SADC Payment System Oversight Committee (PSOC) Report 2016/2017 https://www.sadcbankers.org/subcommittees/PaySystem/sadcpsoc/Pages/Documents.aspx; conversion rate used: 1 USD = 13.66 ZAR

regional tax database that offers information about tax policies for every member state.[9] A regional digital financial ID could take this a step forward and allow financial institutions to see the tax status of citizens, making tax-related transactions – filing and returns – transparent.

Owing to an increasing agenda around financial inclusion, a regional Financial Inclusion strategy has been adopted by SADC, and the region requested FinScope surveys to be run in each member state every three years. Regional and national bodies are actively participating in financial inclusion strategy workshops and some member states like Zimbabwe have already released their national strategies.[10] FinMark Trust and UNCDF together supported seven countries in the region to develop financial inclusion strategies/roadmaps under the MAP program.[11] Developing cross-border and domestic digital payments, and building a credit market for SMMEs are key aspects of the strategies for which a digital financial ID would be greatly advantageous.

Efforts to improve regional KYC regulations are underway as well. Initial steps have been taken to harmonize AML/CFT regulations across member states with a detailed study identifying the differences across each member state.[12]In 2017, South Africa adopted a full risk based approach to AML-CFT and other SADC members are likely to follow. In terms of this approach, anonymous transactions will not be allowed, but financial institutions will be left with more choice of which documents they rely on to verify identity of potential customers. This creates opportunity for agreements among accountable institutions to standardize their approach to identity proofing and verification.

---

[9] SADC Tax Cooperation http://www.sadc.int/themes/economic-development/investment/tax-coordination/ ; SADC Memorandum of Understanding in Cooperation in Taxation Related Matters http://www.sadc.int/documents-publications/show/Memorandum_of_Understaning_in_Cooperation_in_Taxation__Related_Matters.pdf

[10] See https://www.finmark.org.za/the-sadc-financial-inclusion-forum/,

https://www.microfinancegateway.org/library/excluded-society-financial-inclusion-sadc-through-finscope-lenses

[11] The seven countries covered so far are Zimbabwe, Swaziland, Lesotho, Madagascar, Congo DR, Malawi, and Botswana

[12] See FMT study on Anti-Money laundering and CFT in SADC countries http://www.finmark.org.za/anti-money-laundering-and-cft-in-sadc-countries/

These public policy drivers contain some tensions, however, creating a trade-off towards how much weight states should put on one force versus the other. For example, state decisions on stringent KYC regulations may discourage businesses from expanding across borders, which may adversely affect remittance services and eventually hurt the financial inclusion agenda. Determining how to balance the policies to optimise benefit is therefore challenging.

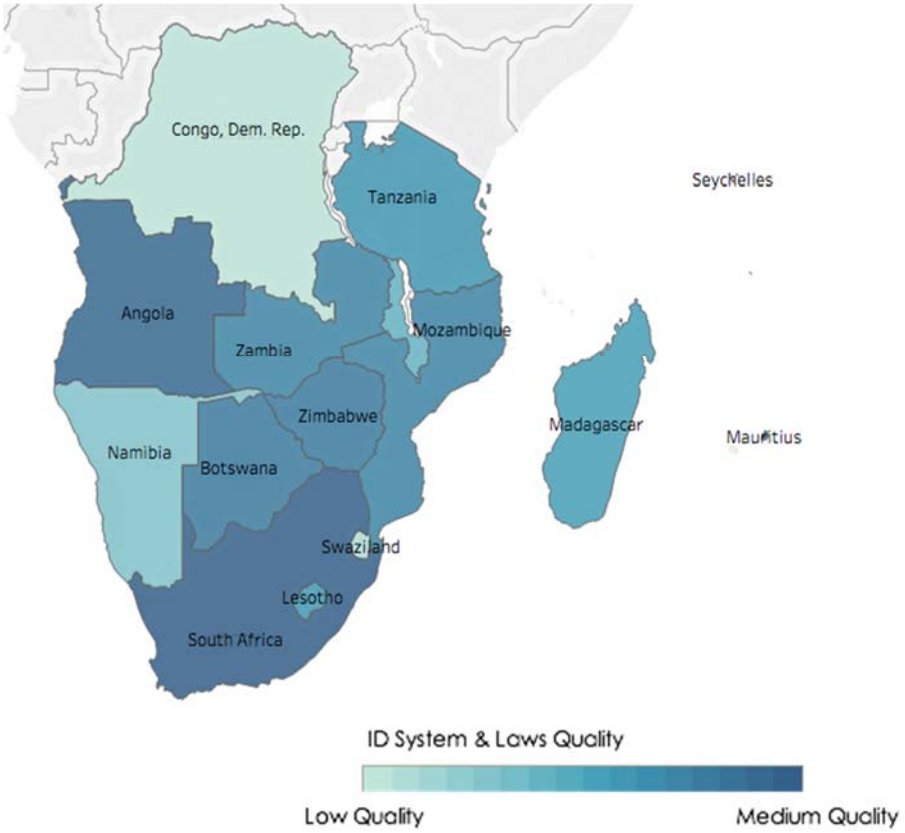
A regional digital identity can help ease the trade-offs by allowing governments to avail information about individuals and businesses more easily, lowering KYC costs, and improving tax management.

### 3.2 SADC's National Identity (NID) context

Even though the forces discussed above push towards the spread of national identification systems, there remains large variation in the extent of development of the NID and registration systems across SADC. In Figure 4.1, the map shows the difference in NID environments across the region based on a scoring criteria used by ID4D which includes a range of parameters from NID issuance and category to data protection laws and right to information.[13]

[13] From World Bank ID4D Dataset; and World Bank, The State of Identification Systems in Africa: Country Briefs http://pubdocs.worldbank.org/en/940071497322166382/ID4D-country-profiles-report-final.pdf

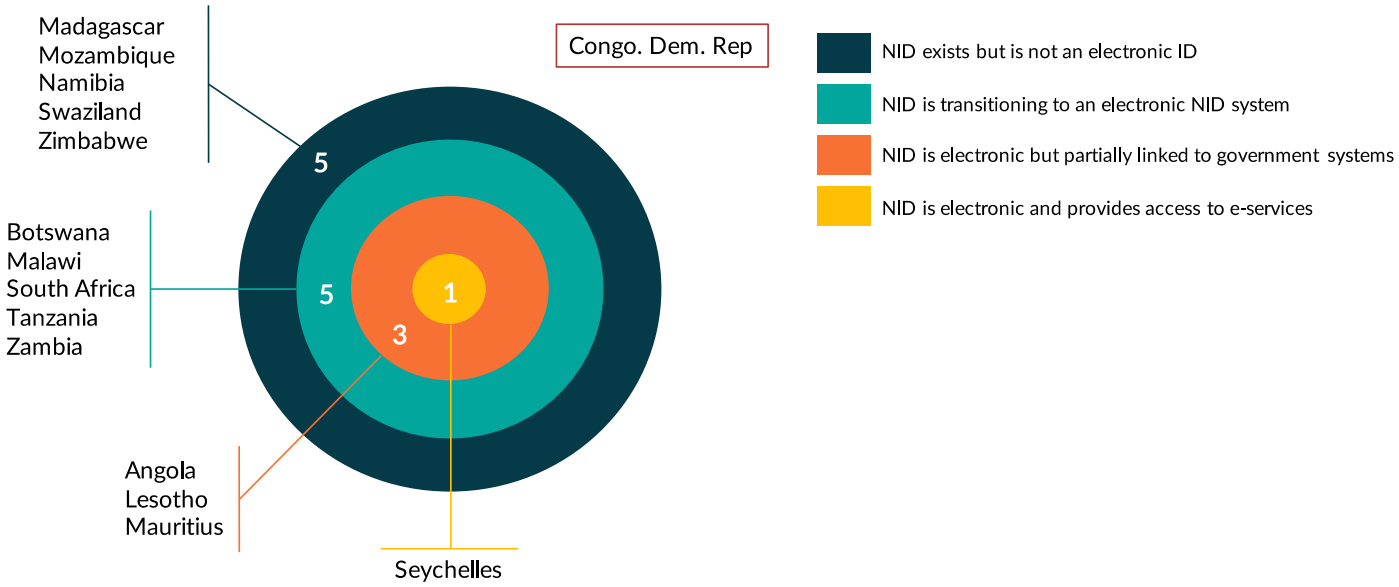
**Figure 4.1: State of NID environments**




*Source: World Bank ID4D 2017 database*

A closer look at the level of digitisation of NID systems across the region also shows great variation. Figure 4.2 depicts these differences. Most countries either do not have an electronic ID (e-ID) system, or are transitioning from a traditional paper-based NID to an e-ID that can later be linked to various e-services. Angola, Lesotho and Mauritius are at early-stage e-ID systems which means that they can start linking the NID database to various government services. Seychelles is the only country in the region with an NID system that links with e-services. Congo Dem. Rep. does not have an NID system at the moment.

## Figure 4.2: Level of digitisation of NID systems

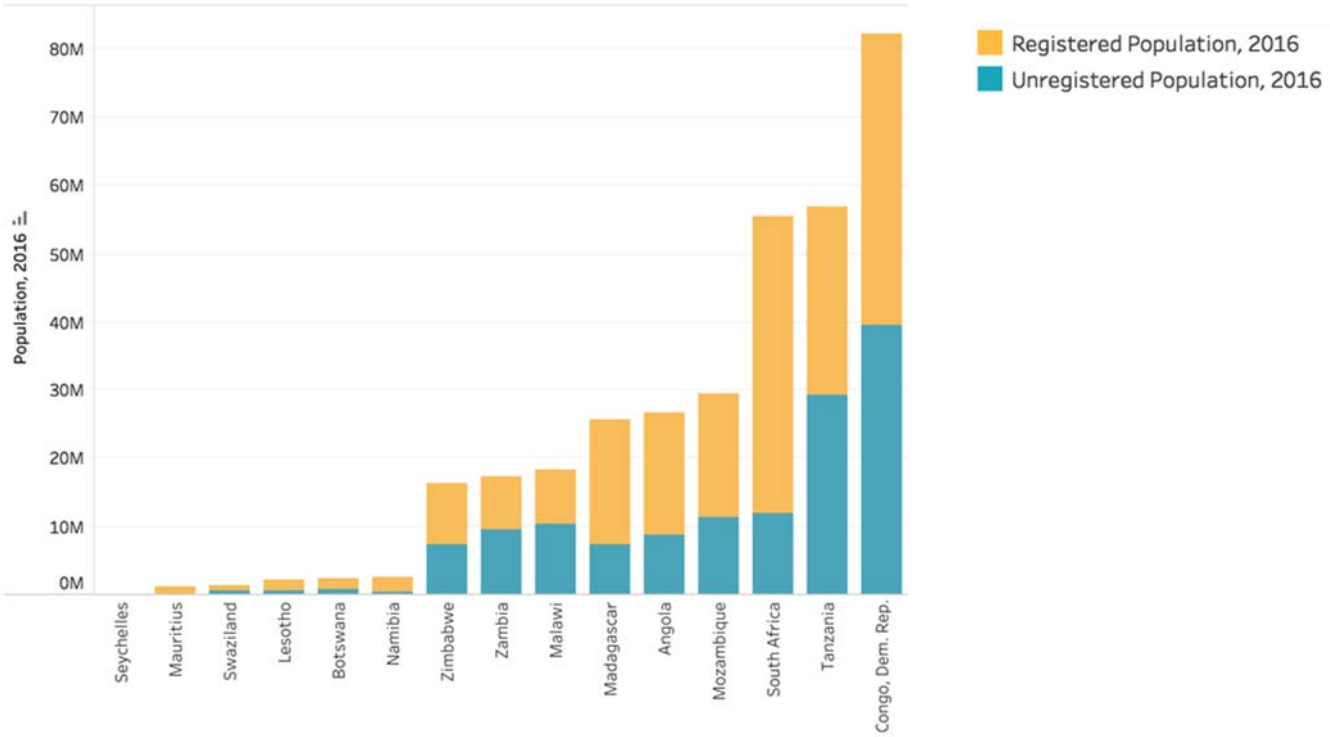



Source: World Bank State of ID country briefs & ID4D 2017 dataset

The degree of registration for the most common ID varies greatly across the region as well. The most common ID across most states is the voter's ID and has the highest registration rates amongst functional IDs. Over 138 million individuals are unregistered across the region, this is equivalent to approximately 41% of the total SADC population.[14] Figure 5 below shows this variation across the member states. See Annex A for other ID-related statistics in the region.

[14] World Bank ID4D Dataset

**Figure 5: Unregistered vs. registered population**




*Source: ID4D 2017 database*

The regional forces discussed and the country-level ID variations suggest that an effort to harmonize NID standards across member states would help improve overall registration and regional integration. SADC has begun to take some steps in this direction by addressing one particular case relevant to cross border usage—that of drivers' licenses discussed in the next section.

### 3.3 Cross border IDs: a precedent from regional driver's licenses?

SADC governments have recognized the need for addressing impediments to cross-border trade. As one part of a wider package of measures, in 2011, SADC started assessing the need to develop a standardized format for driver's licenses and a nationally linked regional transport information

system to trace drivers as they travel across borders. This plan eventually expanded its scope to include the Tripartite Regional Economic Communities (COMESA, EAC, and SADC).

Some key activities as part of this project include harmonizing national transport laws and regulations, and establishing a *Transport Registers, Information Platform and System* (TRIPS) that captures information about various categories of drivers, vehicles and operators, and traffic flow across borders.[15]

TRIPS is a first major step to creating a common platform to track and monitor traffic flow into and out of a participating country, and hold a record of various driver and operator offences ensuring greater safety across the markets.

The project has taken a number of years from ideation (with initial discussions in 2001) to implementation for which the plan stretches until 2030. The primary entities involved are the regional bodies of the Tripartite REC with some private sector involvement through subcontracting parts of the project. While this is one example of a digital ID implementation model, there may be other models that can fit into the SADC context which could fast-track digital ID efforts. Section 4 will discuss these models in greater detail but first, it is important to determine what other relevant use cases could be addressed. The next section attempts to tease these out.

[15] See SADC report on Implementation of the Tripartite Transport and Transit Facilitation Programme Eastern and Southern Africa (TTTFP) http://www.sadc.int/themes/infrastructure/transport/roads-road-transport/implementation-tripartite-transport-and-transit-facilitation-programme-eastern-and-southern-africa-tttfp/; and SADC's Official Launch of the Tripartite Transport & Transit Facilitation Programme (TTTFP) https://www.sadc.int/news-events/news/official-launch-tripartite-transport-transit-facilitation-programme-tttfp/; and SADC's Tripartite Transport and Transit Facilitation Programme: Overview of the Program. http://www.sadc.int/files/6815/0668/7619/Overview_of_the_TTTFP.pdf

## 3.4 Potential use cases for digital ID & weightings

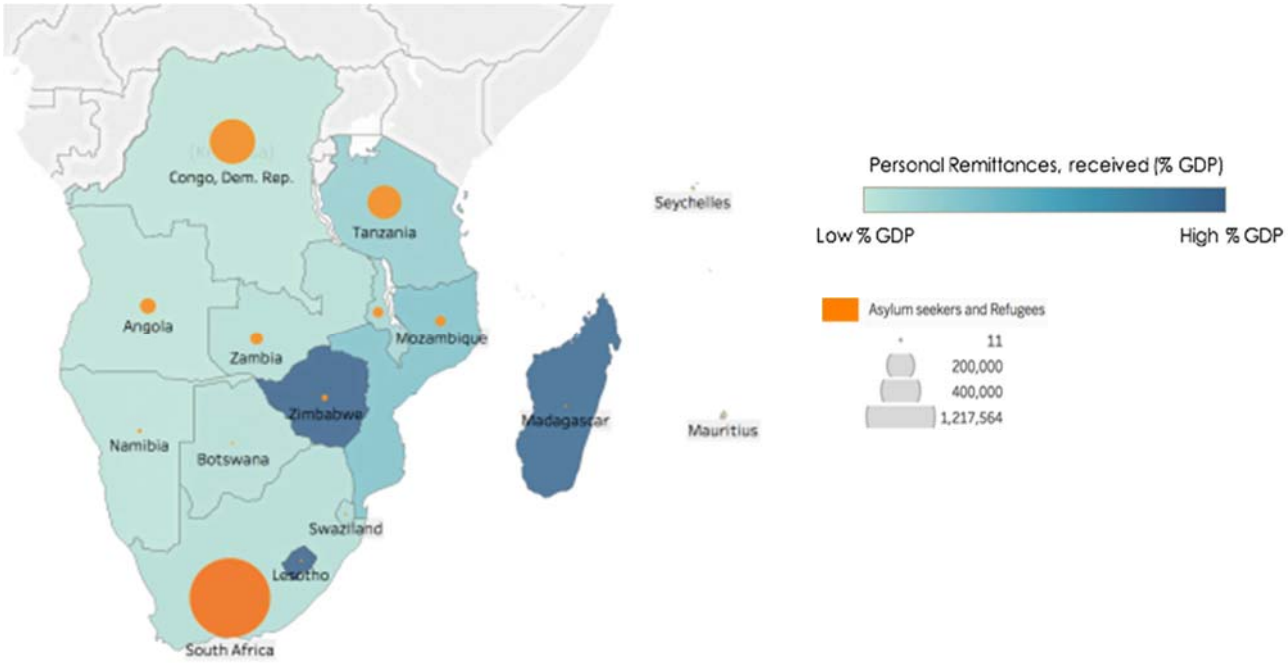
One way to identify relevant use cases for digital ID is by assessing cross-border trends and the different issues which FSPs and regulators face. This section looks at two main categories – the flow of people and the flow of goods across borders.

### *3.4.1 Flow of people*

People moving across borders for work, asylum seekers and refugees, all need an identity to prove who they are and have financial institutions trust them. Figure 6 below shows the levels of refugee and asylum seeker migration and personal remittances across the SADC states. According to IOM, the total refugee and asylum population in the region is about 1.9 million and countries with the largest numbers are South Africa, Congo Dem. Rep., and Tanzania. Countries with the highest overall remittances received as a percentage of GDP include Lesotho, Zimbabwe and Madagascar.[16] Lesotho is the highest with about 15.7% of GDP made up from personal remittances.[17]

[16] IOM http://gmdac.iom.int/forced-displacement-globally-2015 and World Bank World Development Indicators
[17] Ibid.

**Figure 6: Refugee and asylum seeker flows vs. personal remittance trends**




*Source: IOM, World Bank*

A separate study by FMT on remittance flows from South Africa shows that the total number of migrants coming into South Africa for work amount to approximately 3.3 million and the total outbound remittances amount to roughly $1.3 billion. The largest proportion of immigrants for work in South Africa come from Zimbabwe, Lesotho and Mozambique. These three countries are also the largest remittance recipients from South Africa.[18]

Some of the SADC remittance corridors are ranked amongst the costliest when compared to remittance corridors around the world. Average transaction costs as estimated by the World Bank amount to 16% while FinMark Trust estimates them to be 7%. To put this cost factor in perspective,

[18] See FMT report on Cross-Border Remittance Pricing: http://www.finmark.org.za/cross-border-remittance-pricing/

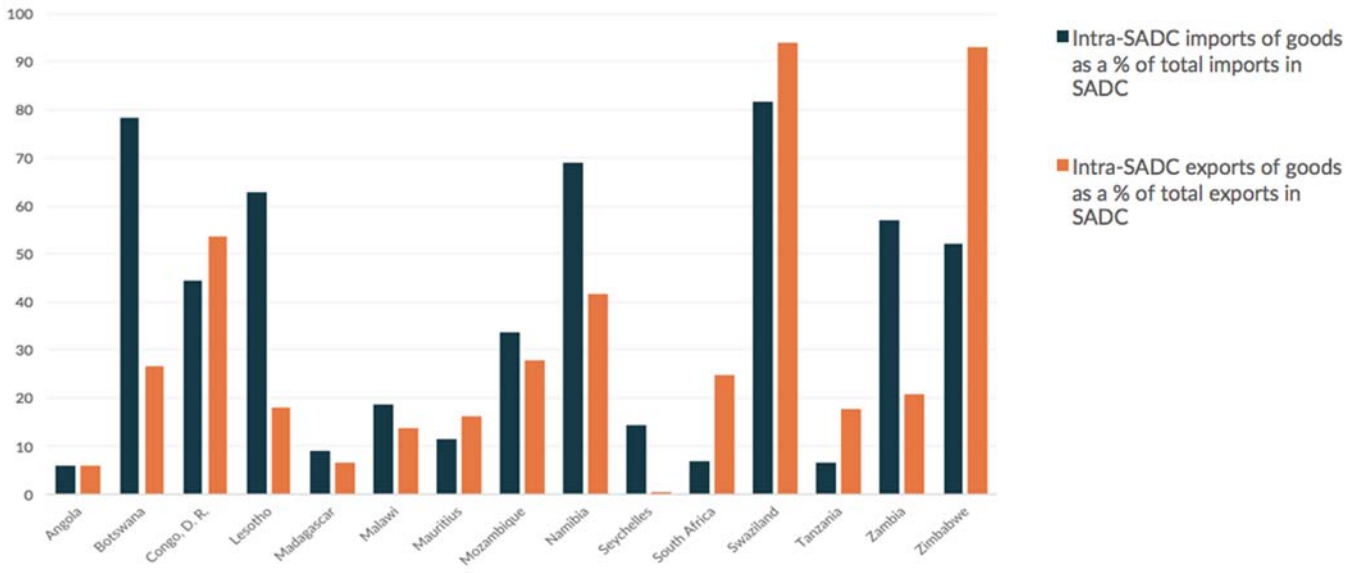
the target for the global SDGs is that by 2030, transaction costs for migrant remittances should be less than 3% and those corridors with costs greater than 5% should be eliminated.[19]

With such high migration and remittance rates, a digital ID to help migrants move across countries and settle down more easily while affording them the ability to send money home at lower costs makes for a relevant and compelling use case.

### *3.4.2 Flow of goods*

Intra-SADC import and export of goods varies a lot across the member states as well. Figure 7 below shows this variation suggesting that some countries have greater involvement within the region.

**Figure 7: Intra-SADC exports/imports of goods as a % of total SADC exports/imports**




*Source: SADC report*

[19] See Accion CFI blog post: https://cfi-blog.org/2017/12/08/sadc-needs-a-regionally-accepted-digital-financial-id-and-it-is-feasible-to-contemplate/ and SDG goal 10 targets: http://www.un.org/sustainabledevelopment/inequality/

One reason for this variation is arguably the high KYC standards in some SADC states that discourage companies from trading across borders. While a harmonised transport system is on its way, FSPs and regulators say that the time, effort, and money involved to send money for payments across borders is still high. More granular insights are shared in the next section. Easing regulations can lower costs for businesses encouraging them to trade or expand their work across SADC. A regional digital financial ID can help lower costs while maintaining high KYC standards.

### *3.4.3 A view from FSPs and regulators*

Apart from the overall trends, FSPs and regulators in the region identify numerous pain points with regard to those trends.[20] Figure 8 below describes three key concerns that they highlight, links these concerns to particular use cases that will be discussed further in the next section, and also identifies the stakeholders that are impacted.

[20] These arose from a DFI convened seminar on Digital ID in October 2017, at which Aurora Bila from Banco do Mocambique brought a perspective from the financial regulator and Kim Dancey from FNB International a view from a regional bank engaged in cross border flows of all types. This seminar conversation built on an earlier discussion at a FinMark Trust Financial Inclusion conference held in Jo'burg.

### Figure 8: FSP and regulator concerns

| Identified Pain | Affected use case | Whose pain? | | | |
|---|---|---|---|---|---|
| | | Financial sector | Users (Individuals) | Users (Business) | Govt. |
| 1. It is costly, slow and ineffective to capture and validate sender and remitter details as required by KYC laws—hence **intra-SADC remittances are costly and not easily accessible** | P2P, P2B, B2P, remittance (KYC) | X | X | X | X (inclusion objective) |
| 2. **Banks suffer fraud** because of inability to identify and trace borrowers across SADC | Loans | X | | | |
| 3. **Remote deposit taking channels** may be closed down due to inability to verify identity | Automated deposit capture | X | X | X | |

*Source: Discussions with SADC practitioners*

While a digital ID would help improve customer due diligence processes, it would also make it more cost-effective, faster and safer to offer financial services. The low cost of implementing KYC would ultimately improve financial inclusion prospects. The ease of tracking transactions and credit histories, especially across banks, would decrease fraud likelihood especially as credit defaulters would be identified in no time.

Figure 9 below takes the learnings from the discussion so far and provides a non-exhaustive list of use cases that could be used as a starting point for creating a business case for a regional digital financial ID.

**Figure 9: Some possible use cases for a regional digital financial ID**

| 1. Store of value (SoV) to SoV | 2. Pre-migration account opening | 3. Post-migration account opening | 4. Post-migration access to credit |
|---|---|---|---|
| Money saved in various accounts that can be sent across borders | Opening a bank account in a country that one plans to migrate to but hasn't yet migrated | Opening a bank account in a country that one migrated to | Getting access to credit based on available credit information n a country that one migrated to |
| • Personal<br>• Business | • Personal<br>• Business | • Personal<br>• Business | • Personal<br>• Business |

### *3.4.4 Prioritising use cases*

Given the numerous possible use cases for a digital financial ID in SADC, the next question is how to determine which use case to start to build a business case around. One way to do this is by answering questions around the impact on stakeholders, regulations, and market opportunity among other factors.

For example, in looking at the use case of 'Store of Value (SoV) to SoV (or account to account) for personal use', a subset of such questions would include:

- What's the business case for FSPs? How easy is it for FSPs to implement this use case?
- What customer pain points are addressed? How easy is it to alleviate them?
- How feasible is implementation from a regulatory standpoint?

Answering these questions by assigning weights based on a combination of implementation feasibility and impact potential can help identify the more plausible use cases. Figure 10 below provides an example of how this can be done. The weights assigned are only for illustrative purposes and may likely change based on further discussion with regulators and financial service practitioners in SADC.

## Figure 10: Assigning weights to use cases

| | | Criteria affecting ease of implementing use case | | | | Overall weight |
|---|---|---|---|---|---|---|
| | | FSP business case | Customer pain points | Regulatory feasibility | … | |
| Possible use cases | 1. Store of value (SoV) to SoV<br>1A. Personal | M | H | L | | |
| | 1B. Business | H | M | H | | |
| | 2. Pre-migration account opening<br>2A. Personal | | | | | |
| | 2B. Business | | | | | |
| | 3. Post-migration account opening<br>3A. Personal | | | | | |
| | 3B. Business | | | | | |
| | 4. Post-migration access to credit<br>4A. Personal | | | | | |
| | 4B. Business | | | | | |
| | … | | | | | |

With this simple framework in place, the next step is for stakeholders to consider the following key questions that still need to be asked in order to strengthen the narrative for SADC's digital financial ID:

- What are some other scenarios and use cases that can be impacted with a regional digital financial ID?
- What are some other criteria that should be considered when prioritizing use cases?
- What's the most feasible business model that fits the SADC landscape?

The following section will provide perspective on the question of identity management system models for deployment by introducing global comparators.

## 4. DIGITAL IDENTITY GLOBAL OPTION SETS

There are many different digital ID schemes of all types in use around the world today and there are many different ways of characterizing them. One way, shown in Figure 11 below, is to show who performs each of the key functions—enrolment, authentication and authorization. Each function could be performed by different entities which are either:

- One or more specialized **ID providers**, where federated or brokered schemes (categories 2 & 4 below) involve multiple providers under a framework of standards, with or without a central hub for access;
- **Service providers**, such as financial institutions who actually offer the digital service in question and therefore usually authorize the transaction once identity is authenticated.

Among the entities which play the role of ID providers, it is possible to further differentiate whether the ID Provider is a government agency (category 3) or a private player (category 1), such as FacebookID which is widely used for access to online services with a low level of assurance. The category of personal ID providers (#6 below) is a rapidly growing segment in which private firms, many of which are startups, offer secure containers in which individuals can seek to build their own ID records, seeking attestation for certain attributes from third parties, and often using distributed ledger technology including public blockchains to store and allow access to this information in a decentralized way.

For completeness, the table below also shows categories of scheme which are not very common at present, such as 5: Credential Service Provider (found in Canada today), and 7: No IDP (exemplified by Bitcoin, the cryptocurrency in which the identity of the owner is solely reflected by the possession of a private key).

**Figure 11: A landscape of digital ID Schemes**

| Category | Enrolment | Authentication | Authorization | Example |
|---|---|---|---|---|
| 1. Monolithic | ID Provider (IDP) | | Service Provider (SP) | FacebookID |
| 2. Federated | IDP2<br>IDP1[21] | | SP | BVN, BankID<br>GSMA MobileConnect |
| 3. State eID | IDP | | SP | eEstonia, Aadhaar |
| 4. Brokered | IDP2<br>IDP1 | | SP | Gov.uk Verify |
| 5. Credential Service Provider | SP | CSP | SP | Canada<br>(& FIDO) |
| 6. Personal ID provider | Attribute providers | Personal data store | SP | Sovrin, GlobalID, Banqu, Civic, uPort |
| 7. No IDP | N/A | | | Bitcoin |

*Source: Drawn from Nyqist et al (2016)*

As explained in the introduction, our interest here is particularly in ID schemes which may be relevant to a potential SADC *digital financial* ID. This latter emphasis raises the level of assurance required

[21] The notations IDP1 and IDP2 signify that more than 1 IDP is involved

both from FSPs as relying parties as well as financial regulators beyond that currently offered by FacebookID (or Google), for example, which is widely used as a convenient means of authenticating digital access online, because the credentials collected at most allow a Level of Assurance 1 in which verification is very limited.

So, in this section, we will extract leading examples from relevant categories to highlight. However, since our main interest at this stage is in the comparison of the schemes, and how they map to the priorities and circumstances from which they originated, we wish primarily to contrast the key dimensions of the chosen schemes. In Annex B, we provide a summary table for each scheme with more details and references. But to enable the contrast here, we first provide a comparative introduction to the basic elements of each of the schemes chosen for their relevance to SADC digital financial ID in the Table below. They differ from very large (India's Aadhaar) to very widespread in their countries (BankID, eEstonia) in which most adults have and use the digital IDs, or where at least the banked do (Nigeria's BVN). They also differ in their form factors: some are based on smart cards (eEstonia) while others are mainly or only used via mobile apps (Mobile Connect, BankID, Global ID). BVN and Aadhaar have no physical form factor (beyond an enrolment letter containing the Unique ID number), but are biometrically authenticated online.

Figure 12: A landscape of selected digital ID Schemes

| Category | Name of scheme | Country | Year started | Scale of issuance [% pop] | ID issued by | Financial sector use cases | Potential relevance to SADC |
|---|---|---|---|---|---|---|---|
| 2 | BVN | Nigeria | 2014 | 30m IDs (2017) [16%] | Banks via central switch | Unique biometric identification of all existing bank account holders | Issued by financial providers alongside but separate from national ID |
| 2 | BankID | Sweden | 2003 | 7.5m [76%] | Banks | Online banking | Started by banks but widely used in other transactions now |
| 2 | Mobile Connect | n/a (GSMA) | 2015 | Not disclosed | Mobile operators | Can authenticate | Mobile phones are widely held across the region |
| 3 | eEstonia | Estonia | 2002/ | 1.2m | Estonian govt. agencies and | ID as a service; can be used to open Estonian (and in future | Becoming a digital Estonian is already available to |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | e-residency: 2014 | 27,000 applicants; 4272 cos established [22] | private providers of elements | EU) bank accounts | SADC citizens and businesses; and gives access to a robust ID |
| 3 | Aadhaar | India | 2009 | 1.1 billion [85%] | UIDAI, Indian govt. agency | eKYC for account opening | A centralized state scheme on large scale which has been used to promote inclusion |
| 6 | GlobalID | US | 2017 | Not disclosed—beta mode | GlobalID | Smartphone app which enables a user to build a profile to which s/he controls access | This scheme is data subject-user centric but is becoming increasingly common |

*Sources: see Tables on each scheme in the Appendix*

In addition to these examples, it is important to note a key example of a recent law which promotes for cross border interoperability of IDs, namely the EU's **eIDAS legislation** which was passed in 2014 and became effective in 2016 across the EU. This is because eIDAS is not an ID scheme itself but

[22] Website of eEstonia, https://e-resident.gov.ee/, accessed 4 December 2017.

rather a framework in which national ID schemes can and must interoperate across Europe as part of EU initiatives to encourage a digital single market and greater innovation among countries. eIDAS regulations were promulgated in 2016 which define and provide detailed standards in terms of which national ID schemes can be classified based on the ways in which they operate their schemes.[23] This relatively new legislation is important because it provides one of the first attempts to create a rigorous way of comprehensively assessing the standards of national ID schemes for the purpose of facilitating cross border commerce and trade.

We should also note here several other recent developments relating to cross border identity which have not yet resulted in new digital ID schemes per se, but which are of interest since SADC has many members.

- **East African Regional Identification Project:** supported by the World Bank, the East African Community comprising 6 member states with 170m people is aiming to implement Article 7 of Common Market Protocol on free movement of persons, with a regional roadmap to be developed by December 2017. This includes mutual recognition of each other's IDs based on common market protocols; and the upgrade and connectivity of border control posts, interoperability of national ID authorities.[24]

- **SWIFT KYC Registry[25]** : SWIFT runs a widely used secure financial messaging system which is at the heart of the international inter-bank payment system in the world, but has added value adding functions for its members, mainly banks, in recent years. One of the most recent is the KYC Registry which is a data storage utility which enables correspondent banks to submit questionnaires about counterparties which are stored centrally. Banks can use the SWIFT data

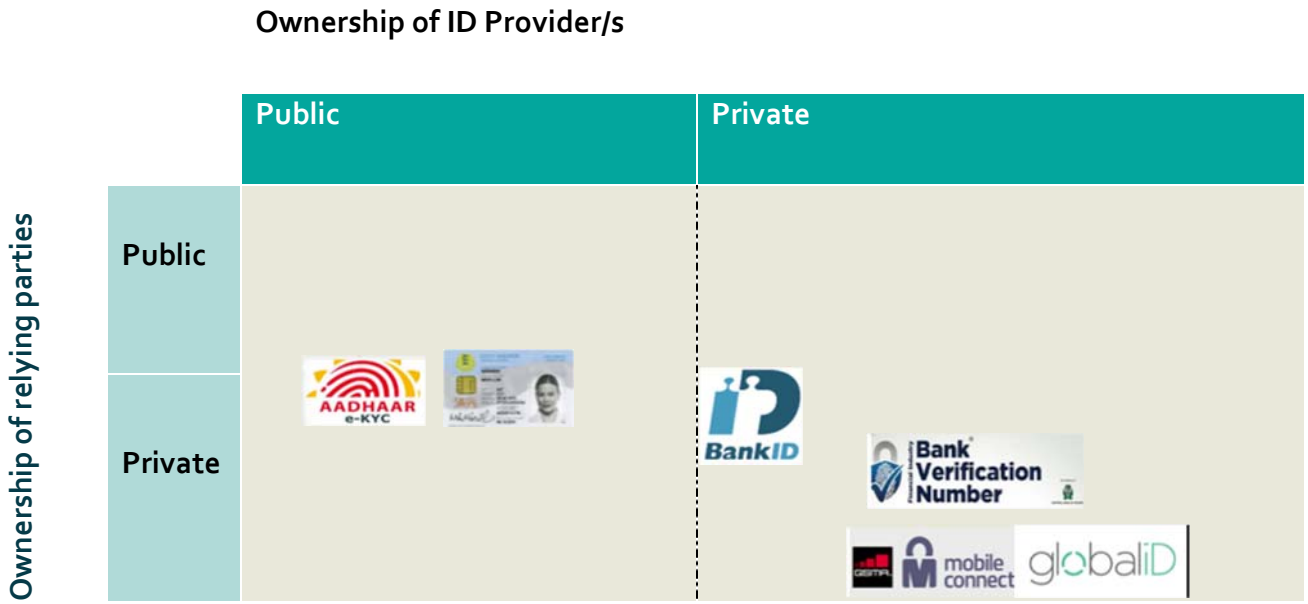
[23] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0...
[24] See presentation by Laura Rawlings at ID4Africa Conference April 2017, available via http://www.id4africa.com/2017_event/Presentations/2-F7-2_The_World_Bank_Laura_Rawling.pdf
[25] https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-registry

hub to store data to access across internal units as well as externally. This is not an ID system per se, but rather a means of facilitating the storage and exchange of counterparty profiles especially for businesses which are making international payments in a secure way.

However, most financial ID schemes today are relied on only within a national jurisdiction. Let us contrast the range of schemes selected along various axes of comparison.

First, in the table below, we contrast the difference between whether the issuer is public or private on one axis, and then on the other axis, who the relying parties are (i.e. those who rely on the ID presented to authenticate or authorize).

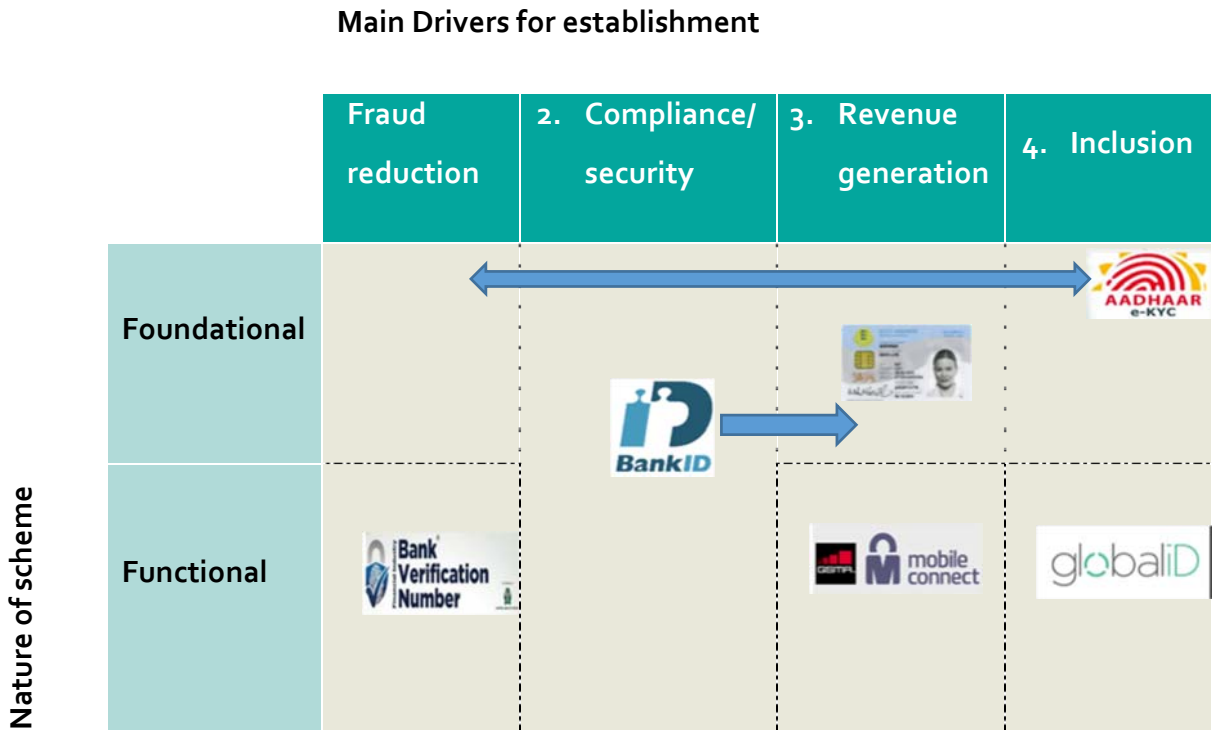
**Figure 13: Contrasting the nature of ID providers and relying parties**




As you can see above, two of the schemes are effectively national IDs, extended to residents (Aadhaar, Estonia) and also to non-residents as a service (Estonian eID), however, their positioning on the vertical axis towards the middle reflects the fact that many private relying parties depend on them. The Estonian scheme also has a private issuer of soft digital certificates for mobile and other

devices alongside the public eID card. The private schemes mainly serve private relying parties, although the Swedish BankID is also extensively relied on by government for services, hence its more central location. Next, let us consider how different drivers have shaped the selected sample ID schemes in the Figure below.

### Figure 14: Drivers and relaying parties




The locations of the selected schemes require some explanation. First, the two state-issued IDs, Aadhaar and Estonia eID clearly sit in the foundational ID space (top row), intended to support a range of applications. But whereas Aadhaar has its roots in first enabling access to state benefit schemes (where elimination of fraud and duplication was and is a major driver) and also the economy more generally, Estonia's eID as a service extended to non-residents intended to grow the base of companies located in Estonia not so much for tax revenue, but for other growth benefits narrowly defined. BankID may have originally started as a functional scheme but has become foundational

supporting a wide range of use cases. Of the remaining functional private schemes, they vary in their focus: Nigeria's BVN was instituted primarily to reduce fraud suffered by banks, whereas MobileConnect has been targeted more to enable e-commerce by providing secure convenience online: one of the motivations cited is the number of e-commerce transactions which fail to complete. GlobalID is the most recent of all these schemes, formed in 2017, and on its website and in its White Paper, it makes much of the case for inclusion of all through a secure digital ID, although by its nature as a VC funded fintech entity, like many others in similar space, it is probably more driven by the desire to create private, user-controlled personally identifiable information which can be the basis of profitable business models in time.

Finally, let us contrast the business models of these schemes in the Table below. Clearly, foundation schemes are most often the responsibility of government to resource, although Estonia charges non-residents for its ID-as-a-service business model. Other federated forms of ID such as BVN or BankID or Mobile Connect have typically relied on industry levies and investments, much as collaborative infrastructure in payment systems is funded. GlobalID is one of an increasing number of new startup ID providers, which have been funded by private VC companies. Such has been the volume of interest in this space, that at least one US VC investor has announced the establishment of a specific investment thesis for ID, potentially leading to the setup of a fund.[26]

[26] Listen to OWI Podcast in September 2017 with PTB Ventures Managing Partner Dave Fields, available here https://itunes.apple.com/us/podcast/state-of-identity/id1183881265?mt=2

**Figure 15: Who pays for what in these ID schemes?**

| Scheme | Capex/ startup costs | ID enrolment | Ongoing costs |
|---|---|---|---|
| BVN | Banks/ NIBSS | Banks;<br>outside Nigeria: individual pays fee | Banks |
| BankID | Swedish banks (set up of utility company) | Banks absorb; individuals pay for mobile ID | Fee paid by relying parties |
| MobileConnect | GSMA (set up of API Exchange) | Set by mobile operators | Fee by relying parties on usage |
| Aadhaar | Indian government | Indian government<br>(free to first time applicant) | Indian government |
| eID Estonia | Estonian government (designed for residents) | Eu100 per non-resident | Meant to become sustainable |
| GlobalID | VC funders (3 investors in seed round 2017)[27] | Free for one ID; pay for more than one | Global ID plans to charge relying parties for usage |

*Sources: various, see Annex B*

[27] See https://www.crunchbase.com/organization/global-id

# 5. Conclusion

This report has provided an introduction and a contextualization of the issues surrounding a potential digital financial ID which can be used in and across SADC member countries.

This report aimed to create a landscape within which to discuss options for SADC, not yet to recommend specific options or to opine on the desirability or feasibility, which only can follow further investigation.

However, this short 'tour' of the digital ID landscape suggests some design principles at least which can be considered in architecting a new ID framework. These are:

1. ***Clarify and prioritize the objectives at stake, since this will affect the nature of the scheme*:** for example, if financial inclusion of unbanked people were the main objective, this would have big implications for scheme design, since unbanked people likely also lack foundational ID documents. However, if the main driver were trade or economic efficiency, then a scheme may target already banked businesses as a starting point.

2. ***Clarify which party or parties can be the ID issuers and who the relying parties are likely to be:*** another way of saying this is if the relying parties (e.g. banks) are mainly private, then they can drive the creation of a new ID scheme used among them; however, if parties beyond a narrow group are intended to rely on the ID, then their interests must also be considered early in the process. In the case of identity used in the financial sector, regulations arising from AML-CFT laws will inevitably affect the acceptability of schemes; so that, even if a scheme were driven by private providers, engagement with regulators would be required.

3. ***Consider the business case for all parties:*** ID schemes cost considerable resource to design, roll out and maintain; they also bring potential liability risks arising from false reliance. This

applies to public as well as private ID schemes. Hence, it is important to identify the categories of costs upfront and who will bear them, against potential returns.

4. ***If found to be feasible, prototype around a chosen use case, within a subset of countries:*** the very diversity of circumstances in SADC – both in terms of the state of existing national IDs and the reach of national banking systems – means that a feasible solution is unlikely to start as a "one size fits all"; hence a process of agile design and development should prioritize use cases in line with design principle #1 above with subsets of countries most relevant to testing the use case.

If SADC stakeholders determine that there is a *prima facie* case to investigate, the next step would be to identify specific use cases in line with the prioritized drivers. The business case and functional requirements for each use case could then be explored further.

## GLOSSARY OF ID TERMS USED

| Word/ Term/ Acronym | Working definition |
|---|---|
| Attributes—core and assigned | A piece of information associated with an identity |
| Authentication | "this is the process of asserting an identity previously established during identification. Typically, this involves presenting or using an authentication credential (that was bound to the identity during identification) to demonstrate that the individual (or organization) owns and is in control of the digital identity being asserted" |
| Authorization | "this is the process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity." |
| Binding | The process of linking an authentication credential to an identity in order that the authentication credential can be relied upon later on as a means of asserting the identity. |
| Breeder documents | Documents establishing identity, usually from an official source (such as passports or national ID cards), which are used as a basis by other identity schemes |
| CA | Certificate Authority |
| Credential | An authentication token (e.g. smart card) used to assert identity or a verifiable attribute, e.g. a digital certificate that demonstrates an entitlement or qualification |
| Digital ID | "A digital identity is then a (usually) cryptographically-protected record that is associated with a legal identity, and which can therefore be used to assert, or provide assurance of, the identity of the holder in either face to face or remote (Internet or mobile) environments" (CHyP) |
| Digital signature | A cryptographic technique to validate the authenticity and integrity of a digital message or document |
| eID | Digital ID |

| | |
|---|---|
| eIDAS | European law setting standards for cross border identity interoperability in member states |
| IPV | Identity Proofing and Verification |
| Foundational identity | An identification scheme, usually managed by a government agency or official authority, which is used as the recognized basis for establishing identity for the purposes of other schemes |
| Functional identity | An identification scheme used for a particular purpose e.g. voters' roll |
| Identification | "…the process of establishing information about an individual (or organisation). It may involve examining "breeder documents" such as passports and birth certificates, consulting alternative sources of data to corroborate the identity being claimed and potentially collecting biometric data from the individual." CHyP |
| Identity | A collection of attributes that uniquely define a person or entity. |
| Identity assurance | The process that determines the level of confidence that an applicant's identity is true |
| IDP /ID Provider | A trusted organization that verifies an individual identity according to agreed standards |
| idMS | ID Management system |
| KBV (Knowledge Based Verification) | Static—where a secret has been previously exchanged, one party uses the secret to verify that they are the other party of the original exchange Dynamic—a process where the applicant is required to provide answers to questions relating to claimed identity |
| KYC | Know your Customer—rules set by financial authorities in terms of AML-CFT laws requiring authorized institutions to verify identity |
| Legal identity | "Identity that is associated with an individual who it has been formally established has a right to reside in a country, with all of the rights and responsibilities that flow from that." |
| Level of assurance | "A measure of the quality of the identity derived from the both the quality of the identification process and the strength of the authentication credential used when asserting the identity." |
| Mobile Connect | GSMA's ID initiative involving MNOs |
| OAuth | Protocol for digital authentication |

| | |
|---|---|
| Onboarding | End to end process of taking on a new client e.g. for a bank |
| Personal Data Store | A personal proof bank for individuals to store identity documents and manage how they are accessed by others |
| PII | Personally Identifiable Information |
| PKI | Public Key Infrastructure |
| Privacy by design | An approach to systems engineering which takes privacy considerations into account throughout a process |
| RA | Registration authority |
| Relying parties | The party in a transaction that relies on an assertion by the other party |
| SIMs | Subscriber Identity Modules (in Mobile phones) |
| Token (for ID) | An object containing the security credentials for a user |
| Transactional identity | Set of identity attributes which defines an individual's identity for the purposes of executing defined transactions |
| Trust anchor | An authoritative entity for which trust is assumed and not derived from which the whole chain of trust is derived. |
| Trust framework/ scheme | The organizational, regulatory, legal and technical measures to assert trust relevant attributes within a domain of trust |
| Trust list | Provides relevant attributes of enrolled entities |
| UMA | User Manager Access (extension of OAuth) |
| Verification | The process performed to determine whether an applicant owns an identity |

## ANNEX A: NATIONAL ID & REGISTRATION STATISTICS

| Country | Private credit bureau coverage (% of adults) | Public credit registry coverage | % banked | % mobile account | Mobile subscriptions per 100 people | Smartphone penetration | Birth registration rate | Registration method | % population above voter ID eligibility age that's registered | Birth registration info linked with NID? |
|---|---|---|---|---|---|---|---|---|---|---|
| Angola | 0.00% | 1.90% | 29.32% | - | 55.28 | 34% | 56% | Paper-based | 36.61% | - |
| Botswana | 53.50% | 0.00% | 49.24% | 20.75% | 158.53 | 69% | 72% | Digital | 35.16% | Y |
| Congo, Dem. Rep. | 0.00% | 0.70% | 10.91% | 9.21% | 39.48 | 26% | 28% | Paper-based | 38.94% | N/A |
| Lesotho | 7.10% | 0.00% | - | - | 106.57 | 62% | 45% | Digital | 55.38% | Y |
| Madagascar | 0.00% | 3.00% | 5.73% | 4.36% | 41.79 | 23% | 83% | Paper-based | 31.12% | N |
| Malawi | 0.00% | 0.00% | 16.14% | 3.84% | 40.32 | 26% | 2% | Paper-based | 40.83% | N |
| Mauritius | 0.00% | 83.30% | 82.21% | 0.86% | 144.24 | 69% | 90% | Digital | 73.12% | BR required to attain NID but systems not linked |
| Mozambique | 0.00% | 5.30% | - | - | 66.25 | 47% | 48% | Paper-based | 36.85% | Y |
| Namibia | 61.20% | 0.00% | 58.06% | 10.36% | 109.19 | 45% | 78% | Digital | 48.32% | Y |
| Seychelles | 0.00% | 100.00% | - | - | 161.23 | 69% | 90% | Digital | 72.58% | BR required to attain NID but systems not linked |
| South Africa | 63.70% | 0.00% | 68.77% | 14.43% | 142.38 | 68% | 95% | Digital | 45.80% | - |
| Swaziland | 46.10% | 0.00% | - | - | 74.36 | 52% | 50% | Paper-based | 31.43% | Y |
| Tanzania | 6.50% | 0.00% | 19.04% | 32.36% | 83.18 | 42% | 15% | Paper-based & Digital | 40.89% | N - not yet but will do so eventually |
| Zambia | 16.80% | 0.00% | 31.29% | 12.11% | 74.95 | 53% | 11% | Paper-based | 38.86% | N |
| Zimbabwe | 31.40% | 0.00% | 17.19% | 21.60% | 76.37 | 58% | 49% | Digital | 39.17% | BR required to attain NID but systems not linked |
| Sources | Doing business 2016 | Doing business 2016 | Findex 2014 | Findex 2014 | World Bank WDI | GSMA | ID4D country briefs | ID4D country briefs | ID4D 2017 dataset | ID4D country briefs |

| Country | NID as e-ID? | % of population registered with NID | Data points stored as part of NID | Cost of acquiring NID | Data protection measures |
|---|---|---|---|---|---|
| Angola | NID exists and is an e-ID (at least partially) | 28% | Two thumb fingerprint biometrics, iris images, birth certificate, demographic data | $0.14 | No specific authority present; the country refers to the "Lei da Protecção de Dados Pessoais" legislation for personal data protection |
| Botswana | NID exists and is an e-ID (at least partially) - plans to deploy an electronic NID card system | 90% | Photo, nine-digit ID number, full name, date of birth, place of birth, and the cardholder's signature, thumbprint, gender, eye color, place of application, the issuing authority's signature, and a bar code consisting of the card number and the cardholder's last name | Free (renewal fee $0.50, lost/replacement $11, more than 30 days after eligibility $65) | Plans (from 2014) to have a data protection agency |
| Congo, Dem. Rep. | No NID | 0% | N/A | N/A | None; no legislation either |
| Lesotho | NID exists and is an e-ID (at least partially) | 57% | Machine readable fingerprints, biographical information, photo, other info; 2D barcode | Free (late fees of $0.32) | National legislation: personal data protection legislation |
| Madagascar | NID exists but is not an e-ID | Unknown | 12-digit number (that captures geolocation and a sequential number comprising region, district, commune, and gender, plus a six-digit sequential number) + fingerprints on a laminated card | N/A | data protection law, the Loi N° 2014-038, Sur la protection des données à caractère personnel |
| Malawi | NID exists and is an e-ID (at least partially) - had papercards but plans to use setup the NRIS | 5% | As part of the National Registration and Identification System (NRIS) multi-modal biometrics | Free | Plans to comply with international standards of data protection |
| Mauritius | NID exists and is an e-ID (at least partially) - transitioned from paper-based to electronic ID | 90% | As part of e-ID, The card contains: name, gender, signature, photo (b/w), ID number, MR bar code, card control number, issue date; The chip contains photo, ID number, surname, first name, surname at birth, sex, date of birth, residential address, four fingerprint templates (two thumbs and two index fingers), and a digital certificate that ensures that the data on the card can be read only when validated through the Mauritius National Identity Scheme (MNIS) Certificate Authority. | Free (if lost once: $5.49; second loss: $10.99; subsequent loss: $15.70) | National Data Protection Act (2004); Data protection agency: "Commissariat à la protection des données personnelles" |
| Mozambique | NID exists but is not an e-ID - laminated card with magnetic strip | Unknown | National identification number, photo, name, gender, DoB, nationality, address, biometrics (fingerprints), place and date of issue, height, occupation, marital status, expiration date, and signature of the user. | $4.99 (with an additional $2.50 per child attached to the card) | None; no legislation either |
| Namibia | NID exists but is not an e-ID | 90% | personal identification number, date of birth, name, signature, country of birth, gender, height in meters, date of issuance, unique application number, nationality, eye color, biometrics (fingerprints), and a machine readable bar code | Free (replacement: $3.80) | None; no legislation either |
| Seychelles | NID exists and is an e-ID - allows access to e-services | 90% | National ID number which contains regirstration year, folio number, place of registration, and gender | $3.57 | Seychelles Law for Personal Data Protection (2002) |
| South Africa | NID exists and is an e-ID (at least partially) - transitioning from NID book to smart ID system | 99% | Photo, DoB, signature, other information | Free | South Africa Protection of Personal Information Act (2013) |
| Swaziland | NID exists but is not an e-ID | Unknown | Name, DoB, PIN, chief code, gender, biometrics | Free | None; no legislation either |
| Tanzania | NID exists and is an e-ID (at least partially) - transitioning to a nation-wide smart system | 10% | 20 digit NID containing DoB and registration location; there are 74 fields captured in the unferlying system including fingerprint information | Free | Unknown |
| Zambia | NID exists and is an e-ID (at least partially) - transitioning to a nation-wide smart system | 83% | Current low-tech card: Right thumb print | Free | None; no legislation either |
| Zimbabwe | NID exists but is not an e-ID | 77% | Barcode with thumb print, n ID number, full name, date of birth, village of origin, place of birth, date of issuance, and signature | <$5 (replacement fees range: $2 - $20) | Personal data protection law present |
| Sources | ID4D 2017 dataset<br>ID4D country briefs | ID4D country briefs | ID4D country briefs | ID4D country briefs<br>ID4D 2017 dataset | ID4D country briefs |

## ANNEX B: CATALOGUE OF SELECTED ID SCHEMES


### 1. Bank Verification Number (BVN), Nigeria

| **Started** | **2014** |
|---|---|
| No. individuals enrolled | 30m (mid 2017) |
| Main driver | Strengthen KYC and enhance fraud reduction capability in the banking sector |
| Scheme provider | NIBSS (on behalf of central bank + all licensed banks) |
| Identification/ verification | Banks enrol their existing and prospective account holders by verifying ID to breeder docs and capturing finger biometrics |
| Unique number issued? | Yes |
| Token issued? | No |
| Biometrics captured? | Yes |
| Who pays? | Banks (through central utility which manages the scheme NIBSS) |
| Authentication & authorization | Banks |
| Legal requirement? | Yes—existing account holders must enrol or else accounts are frozen |
| Use cases | New bank account opening<br>Future: biometric authentication at ATMs or POS |
| Reference | https://nibss-plc.com.ng/bvn/ |

## 2. Bank ID, Sweden

| **Started** | **2003** |
|---|---|
| No. individuals enrolled | 7.5m (2016) |
| Main driver | Initially, banks need to offer secure translatability online |
| Scheme provider | Financial ID Technology BID AB (Bank owned utility company) |
| Identification/ verification | Participating banks enrol customers for the scheme |
| Unique number issued? | Yes |
| Token issued? | Yes—smart card, soft token on App. |
| Biometrics captured? | No |
| Who pays? | Banks, customers |
| Authentication & authorization | Yes—for online banking and for many government applications such as filing taxes |
| Legal requirement | Yes—under ID board |
| *Reference* | https://www.bankid.com/en/ |


### 3. Mobile Connect (global scheme managed by GSMA, the trade body for MNOs)

| **Started** | **2012** |
|---|---|
| No. individuals enrolled | Not reported at overall level |
| Main driver | Convenience and security for online commerce |
| Scheme provider | MNOs, connected via API Exchange operated by |
| Identification/ verification | Done as part of applying for subscription |
| Unique number issued? | Mobile number |
| Token issued? | No |
| Biometrics captured? | No |
| Who pays? | GSMA set up; MNOs pay their own costs |
| Authentication & authorization | Yes—for secure log into websites (e.g. SKT case) |
| Legal requirement | No |
| *Reference* | https://www.gsma.com/identity/mobile-connect |

## 4. eID, Estonia

| **Started** | **2002 /e-residency 2014** |
|---|---|
| No. individuals enrolled | 1.2m (98% of residents)<br>e-residents: 27,000 applicants to date |
| Main driver | Leveraging core competence to provide ID as an export service for access to Europe |
| Scheme provider | Government for eID card; Private for Mobile and Smart ID (outsourced private providers SK for digital certificates) |
| Identification/ verification | e-residency: Apply online; card is issued at Estonian consulate when biometrics are also captured |
| Unique number issued? | Yes |
| Token issued? | Yes—card (needs reader to use on computer) |
| Biometrics captured? | Yes—e-residents |
| Who pays? | Citizens for card<br>E-residency: Eu100 |
| Authentication & authorization | Government sites; banks use for remote onboarding |
| Legal requirement | Yes, for Estonians |
| *Reference* | https://e-estonia.com/solutions/e-identity/id-card/ |


## 5. Aadhaar, India

| **Started** | **2009** |
|---|---|
| No. individuals enrolled | 1.14 billion Aadhaar numbers assigned as at August 2017 |
| Main driver | Inclusion; visibility for state; access to state programs |
| Scheme provider | The Unique ID Authority of India, a Union agency |
| Identification/ verification | Yes—via physical enrolment via agents in which biometrics are captured |
| Unique number issued? | Yes |
| Token issued? | No |
| Biometrics captured? | Yes—fingerprints and IRIS |
| Who pays? | Government of India funds UIDAI (cumulatively $1.4 billion up to 2017) which does not charge individuals for issuance but pays registrars per ID. |
| Authentication & authorization | eKYC service can be used as part of account opening to authenticate for mobile phone subscriptions and certain categories of bank account |
| Legal requirement | For government benefit schemes, yes |
| *Reference* | https://uidai.gov.in/ |

## 6. GlobalID

| Started | 2017 |
|---|---|
| No. individuals enrolled | Not disclosed |
| Main driver | (for profit) Creation of a self-sovereign ID framework |
| Scheme provider | Global ID INC, a fintech startup |
| Identification/ verification | Uses authentication via code text to mobile phone number to verify name |
| Unique number issued? | Yes—private key used to identify name uniquely on blockchain |
| Physical token issued? | No—soft token via app |
| Biometrics captured? | No—although these could presumably be added to the ID container |
| Who pays? | User seeking attestation; users for more than 1 userID |
| Authentication & authorization | Yes for online |
| Legal requirement | No |
| *Reference* | https://www.globalid.net/ |

## REFERENCES

### A. General landscape of ID issues


| Author | Year | Title |
|---|---|---|
| Ian Brougham (Consult Hyperion) | 2016 | *ID & authentication systems in digital financial services* – available here |
| Center for Digital Development (USAID) | 2017 | *Identity in a digital age: Infrastructure for inclusive development* – available here |
| Nyquist, Carly et al (Consult Hyperion) | 2016 | *Digital Identity—Issue Analysis* – available here |
| Pon, Bryan et al (Caribou Digital) | 2016 | *Private sector identity in emerging markets* – available here |
| World Economic Forum | 2016 | A Blueprint for Digital ID – available here |
| World Bank Group (WBG) & GSMA | 2016 | *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation* – available here |
| GSMA | 2016 | *Regulatory & Policy trends Impacting Digital ID and role of Mobile* – available here |
| WBG & CGD | 2017 | *Principles on Identification for Sustainable Development: Towards the Digital Age* – available here |
| WBG ID4D | 2017 | *The State of Identification Systems in Africa: Country Briefs* – available here |
| WBG ID4D | 2017 | *The State of Identification Systems in Africa: A Synthesis of Country Assessments* – available here |
| WBG ID4D | 2017 | *Building an Identification Ecosystem for Africa: The WorldBank's Sub-Regional Identification for Development Projects* – available here |
| WBG ID4D | 2017 | ID4D Africa Business Plan IDA 18 (FY18-20) – available here |

## B. Sources of ID data

World Bank ID4D Database: https://data.worldbank.org/data-catalog/id4d-dataset

## C. SADC specific references

| Author | Year | Title |
|---|---|---|
| Aurora Bila & Kim Dancy | 2017 | "SADC Needs a Regionally-Accepted Digital Financial ID—and It Is Feasible to Contemplate" CFI Accion blog available here |
| World Bank ID4D | 2016 | Namibia Identity Management System Analysis Report – available here |
| World Bank ID4D | 2016 | Zambia Identity Management System Analysis Report – available here |
| World Bank ID4D | 2015 | Botswana Identity Management System Analysis Report – available here |
| FinMark Trust | 2015 | Anti-Money laundering and CFT in SADC countries – available here |
| FinMark Trust | 2017 | Cross-Border Remittance Pricing – available here |
| FinMark Trust | 2016 | An Excluded Society? Financial Inclusion in SADC through the FinScope Lenses – available here |
| FinMark Trust | 2014 | The Legal and Regulatory Framework for Payments in 14 SADC Member States – available here |
| SADC Bankers Assoc. & Glenbrook | 2017 | Regional Payments Integration, Financial Inclusion, and Remittances in the Southern African Development Community (SADC): Reflections on a Work in Progress – available here |
| Migrating for Work Research Consortium (MiWORC) | 2015 | Adoption of SADC labour migration policy framework – available here |
| Tralac | 2016 | Moving money across borders in the SADC region – available here |

| | | |
|---|---|---|
| SADC | 2017 | Implementation of the Tripartite Transport and Transit Facilitation Programme Eastern and Southern Africa (TTTFP) – available here |
| SADC | 2015 | TTTFP Mandates from the SADC Transport and Communication Protocols – available here |