DIGITAL IDENTITY – **A SOUTH AFRICAN JOURNEY**

SEPTEMBER 2021
PUBLIC REPORT

pwc

BANKSERVAFRICA

Intended use and disclaimer

It is important for the reader to note that BankservAfrica prepared this report with the intention that the initiative contained herein should be for all the members and not for selected ones only.

None of the information in this report, including all research, opinions or other content, is intended to stand alone as commercial advice. Before making any decision or taking any action, you should seek appropriate advice from a suitably qualified person regarding your circumstances. Although every care was taken to ensure the accuracy of this report, BankservAfrica and/or PricewaterhouseCoopers Inc accepts no responsibility for any loss or damage which may arise from reliance on information contained in it.

243 BOOYSENS ROAD, SELBY, JOHANNESBURG 2001
TEL: +27 11 497 4000 / FAX: +27 11 493 0595

TABLE OF CONTENTS

INTRODUCTION

Digital Identity – A South African Journey is a comprehensive summary of our digital identity journey to date. It evaluates the current environment to the future state of South Africa's digitalised economy in the Fourth Industrial Revolution, draws learnings from existing global Digital ID models and examines South Africa's unique needs to create a successful scheme for the critical mass. The project was a collaborative effort initiated by BankservAfrica with the goal of unpacking our digital identity journey to date.

The initiative involved numerous partners, including a consortium of banks (Absa, Capitec Bank, Standard Bank, FNB, Investec and Old Mutual), FinTechs, regulators and associations, together with PricewaterhouseCoopers Inc. (PwC) as the support partner. Planning started early 2021, with execution running for 6 months from February to July 2021.

FOREWORD

The World Bank defines a digital identity as a set of electronically captured and stored attributes and credentials that can uniquely identify a person.[1] According to their Identification for Development (ID4D) report, there were approximately one billion people globally that did not have any form of recognised identification in 2018.[2] A lack of any form of acceptable identification can limit individuals' ability to access critical services (for example healthcare and education) as well as their participation in formal political life (such as voting) and economic life (such as employment). Some of the challenges South Africa faces in terms of having a secure and inclusive population register originate from the lack of a policy and legislative framework or insufficient attempts at one. Other challenges include outdated and fragmented administrative systems.

Nonetheless, South Africa has implemented different identity programmes to address identity for its citizens. Between 1994 and 2007, the Department of Home Affairs (DHA) rolled out a single national identity system (NIS), which was used to register all South African citizens onto one national population register. Through several initiatives, the DHA extended its services to areas that were previously underserved.

Through the years, the DHA has modernised the identity system, which can facilitate digital identity implementation in South Africa. This is aimed at transforming delivery systems to achieve its strategic objectives of inclusion, national security and improved service delivery, among others. In addition, the DHA's transformation entails the provision of a clear path towards digitisation and attaining a paperless environment.[3] The DHA has identified partnerships with other entities as an enabler in its modernisation journey. The Smart ID card, introduced in 2013, is on par with identity systems in Europe, Asia and America, as it comes with security features that can help prevent identity theft and fraud.

The ever-changing, technology-driven environment is driven by demands from stakeholders within and outside government, with economic activity compelling digital automation. The Fourth Industrial Revolution (4IR) has implications for South Africa in terms of identity management, digital identity development, cybersecurity, the digital economy and other new technology-driven frontiers.[4]

In 2018 BankservAfrica embarked on their Rapid Payments Programme (RPP) to define a mobile-friendly instant payment platform for the industry. The programme aims to address the key needs identified in both the Vision 2025 and Project Future recommendations, which entail increasing financial inclusion, reducing South Africa's dependency on cash, and creating an integrated platform for payments. Digital identity rides on the foundation laid by RPP, with faster payments meaning more reliance on digital identity.

BankservAfrica facilitated discussions with banks, FinTechs and government, engaging and mobilising the digital identity community to explore digital identity and assess the critical elements that should be considered in South Africa's digitalisation journey. This includes actively exploring ways in which financial services can contribute meaningfully to some of the goals set out in the National Development Plan (NDP) 2030, particularly in terms of how science and technology can be leveraged to improve services such as healthcare and education and how to achieve financial inclusion. BankservAfrica, with the support of PwC and the digital identity community, therefore explored the building blocks for a digital identity programme to unpack critical success factors in realising a holistic digital identity programme for South Africa. In this phase, BankservAfrica played a key role in bringing the community together, facilitating these discussions and coordinating the development of the digital identity narrative for South Africa. BankservAfrica appointed PwC as an independent party to conduct research, surveys and interviews, as well as facilitate focus group discussion (FGD) sessions to help craft the South African digital identity story. The summarised outcomes of this process are set out in this document.

This report presents the collective input of our community, comprising banks, FinTechs, regulators and associations, among others. A full list of community members is provided later in the document. The intention of this report is to explore the different aspects of a digital identity programme and identify the potential gains that can be achieved from a successful digital identity programme in South Africa. We trust that this report provides you with valuable insights and look forward to your inputs in supporting South Africa as we embark on a digital identity transformation journey.

Martin Grunewald
Chief Business Officer
BankservAfrica

1 World Bank Group. (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Retrieved from https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf
2 World Bank Group. (2019). Identification for Development (ID4D): Practitioner's Guide, version 1.0. pg.1.
3 Department of Home Affairs. (2020). Draft Identity Management Policy.
4 Department of Home Affairs. (2020). Draft Identity Management Policy.

EXECUTIVE SUMMARY

> Digital Identity is a person's set of attributes that uniquely describes the person engaged in an online transaction under the identity ecosystem.

WHAT IS DIGITAL IDENTITY?

Digital identity is a set of electronically captured and stored attributes and credentials that can uniquely identify a person[5]. Identity attributes can be used to unlock access to banking, government benefits, health, education and other critical services. According to the World Economic Forum, organisations or authorities issue credentials detailing a qualification, competence, or authority for the individual after verifying the individual, and they can attest to the individual's identity claim.

WHAT HAS SOUTH AFRICA'S DIGITAL IDENTITY JOURNEY BEEN AND HOW HAS IT EVOLVED?

South Africa has implemented different identity programmes to address identity for its citizens and residents. The capturing, storing and issuing of identities, with many now using their green ID book or smart ID card as proof of identity, have improved significantly since 1950.

The DHA is the sole authority responsible for providing a means of identity to all South African citizens and residents. In addition, it manages the identity and supporting systems across both government and economic spheres. This has made it possible for registered persons to exercise their rights and access benefits and services in both the public and private domains. The extension of these services by the DHA to marginalised communities has cemented its role as a key enabler in deepening democracy and social justice.[6]

In 2012, the DHA initiated a modernisation programme aimed at transforming its delivery systems to achieve strategic objectives such as inclusion, national security and improved service delivery. [7]Some of the elements that are being rolled out as part of this programme include smart ID cards, fully digital ID and passport processes, online capturing of biometrics at ports of entry and upgrades to movement control and biometric systems.[8]

With technological advancements being witnessed globally and in South Africa, private sector organisations have continued to implement technology-led initiatives to help address challenges such as a lack of financial inclusion and digital skills shortages. In addition, digital footprints have continued to grow as online activities increase across digital platforms, which shows the increasing need for a digital identity programme in South Africa. For example, banking transactions have evolved with the use of smart electronic devices-creating fast methods of accessing financial services.[9]

The DHA has formed key partnerships to improve access by creating new channels for citizens to have better access to their services. An agreement with the major banks has allowed their clients at 14 pilot branches to access a DHA service point.[10] In addition, the DHA has partnered with a visa facilitation service that led to the creation of service points in many countries abroad and in major South African cities. In this case, applications are sent digitally to the DHA, where adjudicators complete the process.[11] Together with local development agencies, the DHA has extended the service to create one-stop centres for local businesses in partnership with government development agencies.

One of the initiatives instituted by private sector organisations was the South African Financial Blockchain Consortium (SAFBC), established in 2016. This initiative aimed to assimilate and demonstrate the transformative potential of blockchain technology for the South African financial industry. The consortium investigated the digital self-sovereign identity (SSI) model as one of its initiatives. Between 2018 and 2019, the consortium launched an SSI platform and reviewed several solution proposals and prototypes put forward. In 2020, it formed an ecosystem with various partnerships and industry collaboration within the financial services community.

5 World Bank Group. (2016). Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Retrieved from https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf
6 Department of Home Affairs. About us: Mandate. Retrieved from http://www.dha.gov.za/index.php/about-us
7 Department of Home Affairs. (2020). White Paper.
8 Department of Home Affairs. (2020). White Paper.
9 Jacobs, D. (2020). Taking Identity Management Seriously — Self Sovereign Identities. LexisNexis. Retrieved from https://www.lexisnexis.co.za/lexis-digest/legal/taking-identity-management-seriously-self-sovereign-identities
10 Department of Home Affairs. (2020). White Paper.
11 Department of Home Affairs. (2020). White Paper.

WHY IS DIGITAL IDENTITY IMPORTANT?

There are approximately one billion people globally that do not have any form of legally recognised identification, especially in many low- and middle-income countries that lack well-functioning civil registration (CR) systems. The identification gap could also be a result of data errors and fraud in countries that still use a paper-based approach when registering citizens.[12] Digital identity can help simplify these processes by minimising human errors, while linking biometrics and other methods of digital verification to one's identity has the potential to significantly reduce fraud such as identity theft. One of the best examples of successful digital identity implementation would be India. By mid-2016, more than one billion residents had been registered on the national identity system, Aadhaar. This is the world's largest biometric database and the first online biometric-based identity system[13].

Furthermore, a digital identity is a way for countries to provide both citizens and residents with access to basic critical government services such as labour markets, government benefits and financial services.[14]

A digital identity can also unlock opportunities for people who have an identity but limited ability to use this in the digital world.[15] In shifting from using a physical identity to a digital identity, there are several advantages to the users, such as efficiency and inclusion. There are also several benefits to those individuals who are already active in the digital world. A good digital identity can facilitate greater user control of data, privacy protection, security for online transactions and decreased resistance in managing online accounts, among others.[16]

A digital identity can therefore unlock and enable economic value creation by fostering increased inclusion, thereby promoting greater access to goods and services. It can also improve formalisation and thereby decrease fraud, protect user rights and increase transparency. Lastly, a digital identity can promote digitalisation which, in turn, drives efficiency and productivity.

12 World Bank Group. (2019). Identification for Development (ID4D): Practitioner's Guide, version 1.0. pg.1.
13 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/gsma-aadhaar-report-270317.pdf
14 The United Nations General Assembly incorporated identification coverage for all by 2030 into the 2015 Sustainable Development Goals.
15 The population with access to the digital world is proxied by active social media users, captured in the We Are Social Global Digital Report 2018.
16 Several bodies of digital ID research have focused on privacy-related requirements and guidelines. These include Identities: New practices in a connected age, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2017; Digital Identity: Issue Analysis, Consult Hyperion, June 2016, identitiesproject.com

WHAT ARE KEY CONSIDERATIONS FOR A DIGITAL IDENTITY PROGRAMME?

Digital identity programmes differ across countries, including the way in which they are established and what frameworks are used. India and Estonia present two very different examples.

In India, the government launched a unique ID number used by citizens to access a variety of public and private services. This ID number is based on a biometric system that captures 10 fingerprints and two irises from everyone, which enables them to issue a 12-digit unique identification number without issuing an identity card.

The Estonian government uses a strong registration system to record digital identity, issuing a chip-based identity card with a photograph, and allowing the user to use a personal identification number (PIN). No biometric information is collected. This model works well in a developed country where the population is highly educated, online services are widely available and the civil registry is well developed.

Another key consideration for a country's digital identity programme is the ecosystem model. Various models – centralised, federated or self-sovereign identity (SSI) – have been adopted by different countries, including Sweden, Norway, Canada, Singapore and Nigeria.

	Sweden – BankID	Norway – BankID	Canada – Securekey Concierge	India – Aadhaar	Estonia – e-Health	Singapore – SingPass
Ecosystem models	Federated model	Federated model	SSI model (pilot phase)	Centralised model	Centralised and SSI model	Centralised model
Adoption rate (approx.)	78%	74%	50%	95%	> 90%	90%
Year launched	2003	2000	2012	2009	2000	2003
Key players	Financial institutions, government	Financial institutions	Financial institutions	Central government	Governent-mandated	Government technology agency
Key use case(s)	Online banking services, payment, online tax services, municipalities, other portal and private services	Financial services, government institutions	Online services from \ financial institutions (i.e., online banking services) and government services (i.e., using familiar online banking sign-in process)	Direct transfer benefits to bank accounts, e-KYC, digital document storae	e-Health record, e-prescription, e-patient, e-ambulance services	Government services (i.e., tax e-filing, housing application, national skills development services, work permit transactions for domestic helpers etc.) and private services (i.e., banking services, insurance services, internet application etc.)

For the purpose of this report, the examples of India, Estonia and Sweden were examined. Lessons learned and considerations from these countries were applied to the South African environment, all of which will help us shape the digital identity story for South Africa. Through the development of a digital identity, we will be able to create new opportunities for South Africans in the realms of, for example, health and education.

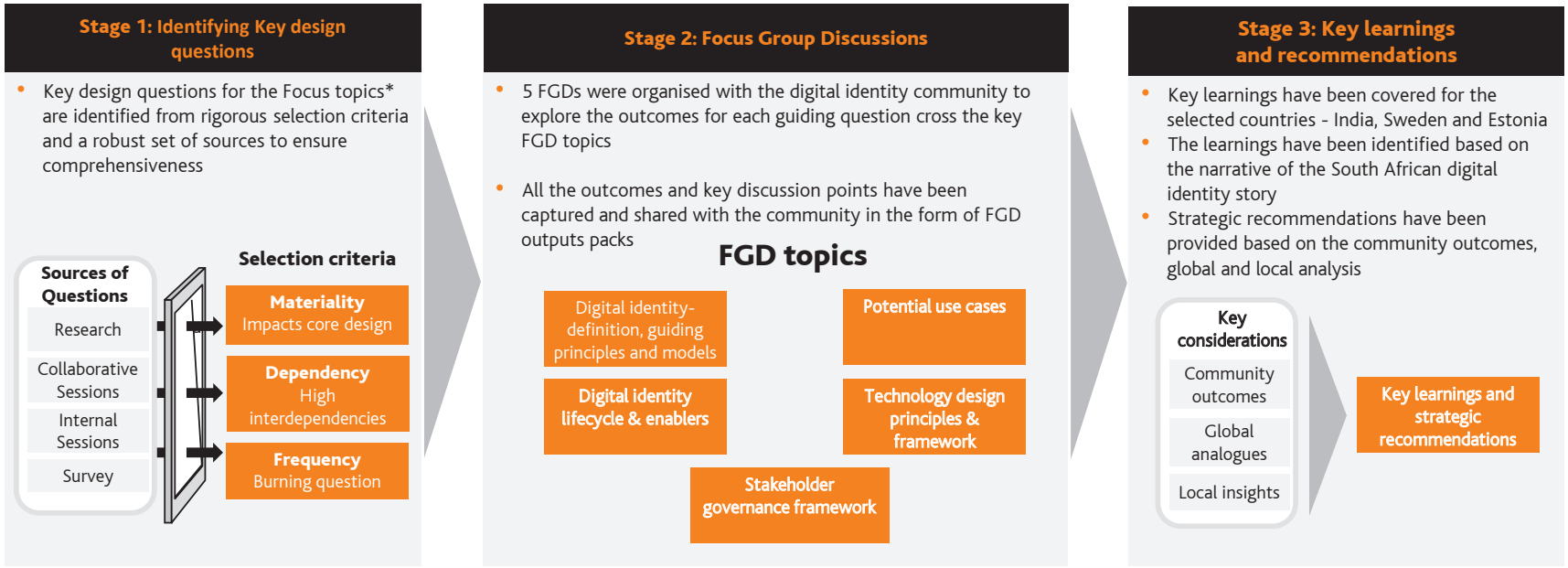
[7]Department of Home Affairs. (2020). Draft Identity Management Policy.
[8]Department of Home Affairs. About us: Mandate. Retrieved from http://www.dha.

South Africa's digital identity programme should be underpinned by clearly defined strategic objectives for the country, which may include the following elements:

- **Focus on inclusion:** Digital identities will help facilitate easy access to a wide range of products and/or services from the healthcare, education and government services sectors.
- **Fit-for-purpose:** The digital identity programme as well as the system design should contribute towards the broad policy and development objectives for South Africa and meet the needs of its people.
- **Simpler FICA processes:** Simpler FICA processes will improve convenience and save time for consumers and service providers.
- **Protection of global financial systems:** Through South Africa's commitment to the Financial Action Task Force (FATF), it contributes to and ensures protection against, for example, money laundering while allowing for alignment with international standards.
- **Focus on reducing identity theft and fraud:** Digitising paper-based applications can help improve the authentication and verification of an individual, which can help minimise identity theft and fraud.
- **Financial sustainability:** The identity management system must be based on a defined model and be cost effective to ensure long-term financial sustainability.
- **Accessible and affordable:** The digital identity must be accessible by all individuals by ensuring that they have the right devices (e.g., smartphones or laptops) to access digital services and/or products.
- **Robust identity systems:** The system must be integrated to enhance and modernise its operations.
- **Privacy and control:** The design of the digital identity system needs to enjoy and engender trust and understanding of its benefits by all individuals.
- **Interoperable platform:** The identification and authentication services should be flexible and scalable and should meet the needs of end-users and relying parties. In addition, there needs to be interoperability between different digital identities to leverage efficiency.
- **Enhanced/Strengthened existing rules and standards:** Digital identity can help enhance and/or strengthen existing legal frameworks around data privacy, information and consumer protection by providing new digital tools that can potentially result in measurable compliance.
- **Trust framework:** A set of business, legal and technical policies will govern the digital identity network. The framework should have specifications and standards that will promote interoperability within the digital identity network.

APPROACH AND METHODOLOGY FOR DEVELOPING SOUTH AFRICA'S DIGITAL IDENTITY STORY

> A digital identity can unlock opportunities for people who have an identity but limited ability to use this in the digital world. In shifting from using a physical identity to a digital identity, there are several advantages to the users, such as efficiency and inclusion.



ASSESSMENT FRAMEWORK BASED ON KEY GUIDING QUESTIONS

Digital identity is emerging within all modern societies and is critical for any country wanting to move towards a digital economy and remain in step with international trendsetters. It is important to develop a robust, secure and comprehensive programme that can meet the country's identity, social, political and economic needs, now and in the future. Designing and implementing a fit-for-purpose digital identity programme is a complex process with several risks and challenges.

Numerous countries have already embraced the 4IR and have embarked on the digital identity journey. Some of these include India, Estonia and Sweden. We examined global best practice as applied in these countries to help South Africa develop a fit-for-purpose digital identity programme. Some of these considerations include the ecosystem adopted, the stakeholders involved, and the regulatory and policy framework implemented

1 **What digital identity ecosystem model was adopted and why?**

There are three main digital ecosystem models - SSI ecosystem, centralised ecosystem and hybrid ecosystem. Each of these models has benefits, key considerations, design frameworks and stakeholders involved. Each country that has implemented a successful digital identity chose a model to fit the country's needs and demands. Through the analysis and interaction with industry players, it will become evident Through the analysis and interaction with industry players, it will become evident which model is best suited for the South African environment.

2 **Who are the stakeholders involved?**

The success of any digital identity programme is demonstrated by the level of adoption among the involved stakeholders. It is very important to address the needs of all the entities involved. For each country there are a number of different stakeholders, each of which have their own roles and responsibilities. The stakeholders are specific to each country's structure and the needs to the associated programme.

3 **What was government's involvement in the digital identity programme?**

There are different roles that government can play, which depends directly on the model that is adopted. The Government can directly be involved as an identity provider; the Government only acts as a regulatory and is not involved as the identity provider; the Government acts as both the regulator and the identity provider. In some countries the Government plays a number of roles. Through the analysis, it will become evident what is best for South Africa.

4 **What technology was used in the development of digital identity?**

The technology framework plays a crucial role in the development of a digital identity. Some of the dimensions that should be considered include capacity, interoperability, usage, security, privacy and long-term viability. Other considerations include the replacement of elements seamlessly without jeopardising the operations of the overall system. Systems should also be based on open standards. An important consideration is also the country's underlying, enabling technology infrastructure.

5 **How long did it take for successful adoption of digital identity?**

The level of adoption refers to multiple objectives that can be achieved: percentage of citizens who have a digital identity to population, number of private and public institutions able to offer services through the use of digital identity, number of accesses to digital services. Due to the different socio-economic and political structures of countries, different countries have different periods for successful adoption.

6 **What regulatory and policy frameworks were adopted?**

In most countries, existing legislation is not really supportive to digital infrastructure. It is imperative that countries set up constitutional acts and policies in order to make the regulatory environment more generic. There are three levels – level 1 is General Law such as Data Privacy Law, Data Sharing Law, GDPR, etc; level 2 captures Generic Identity System Laws; level 3 captures the more specific law that needs to be changed.

7 **What are the accelerators that enabled adoption of the digital identity?**

In some countries concurrent trends, including political willpower, rising global connectivity and emerging technologies, are opportunities to accelerate digital identity. In addition, one of the most important for adoption by individuals and institutions is the trust in the digital identity programme. Individuals tend to trust healthcare providers, financial institutions and government the most with their personal data. However, this varies across different countries.

OVERVIEW OF DIGITAL IDENTITY

> Digital platforms and networks are the backbone for a range of sectors such as banking and financial services, telecommunications, health and education, thus contributing to the overall growth of the digital economy

A person's identity is regarded as the cornerstone of their basic human rights, enabling people to realise their rights, privileges and benefits of citizenship. The South African Constitution confirms that no citizen may be deprived of citizenship (Section 20) and that every child has the right to a name and nationality from birth (Section 28(1)(a)). The mandate of the DHA is to promote and fulfil its constitutional obligation by developing and managing the country's identification system. Only the DHA can affirm a person's official identity, issue a South African identity document and/or passport and register a birth, death or marriage.[17]

Due to the DHA's legal mandate, identity management is an important and pressing issue for it, given the technological advances unfolding globally – particularly in terms of the growth of the digital economy. Innovations and new technologies are sweeping the globe and are rapidly disrupting and changing the way we all behave, live and work. This phenomenon, dubbed the Fourth Industrial Revolution (4IR), also known as the digital revolution, marks a major turning point in our collective local and global development. Identity management in its multiple forms is an integral part of the 4IR era, encompassing the digital economy, e-identity, national security, global threats, and the increasing use of technology by governments to improve the quality of life of their citizens. This ever-changing, technology-driven environment is driven by demands from stakeholders, both within and outside of government, as well as economic activity demanding digitalisation.

Digital platforms and networks are the backbone for a range of sectors such as banking and financial services, telecommunications, health and education, thus contributing to the overall growth of the digital economy. For example, financial institutions in the Nordic countries have been instrumental in forming the digital identity ecosystem, which has helped the businesses evolved while spearheading the financial inclusion agenda in these countries. Central to this is the biometric data of individuals, which now includes fingerprints, iris reading, facial recognition and DNA, and is often integrated with the e-identity, or e-government and e-commerce services. The impact of these technological advances lies in the way the government and the private sector collaborate in facilitating and enabling this widening economic activity.

There are three common elements in defining a digital identity, namely uniqueness, the ability to authenticate the user and the use of a digital or electronic channel. Unlike a paper-based ID such as most driver's licenses and passports, a digital identity can be authenticated remotely over digital channels. It simplifies the authentication process, as a user with digital credentials and a password can remotely log into the websites or portals of multiple entities using an application from their phone or other digital channel.

While it is easy to take identification for granted, particularly in mature economies, close to one billion people in the world lack any form of legally recognised identification, thereby denying them access to critical government and economic services.[18] The rest of the world's population, about 6.6 billion people, either have some form of identification with limited ability to use it in the digital world or are active online yet face difficulty keeping track of their digital footprint securely and efficiently. Digital identification, or "digital ID", could help individuals authenticate their identity through a digital channel and unlock access to the digital world within the economic, social and political realms.

THE FUNDAMENTAL REQUIREMENTS FOR A DIGITAL IDENTITY ECOSYSTEM

To enable a digital identity ecosystem, it is important to understand some of the fundamental requirements for setting up such a cross-country ecosystem. Five of the most important requirements are:

- **Identity management system and existing infrastructure:** The existence of an identity management system in a country can be a major leap forward for a digital identity ecosystem. The existing foundational identity (for example a national ID) can act as a golden source to the digital identity ecosystem.
- **Frameworks and policies:** Established legal and regulatory frameworks may act as enablers in putting forward requirements across data protection and privacy, cybersecurity and anti-money laundering for consideration. Governance of the digital infrastructure can be considered across policy as well as technical levels. The policy frameworks should address digital infrastructure issues and innovative technologies and should factor in consumer protection rights, thus boosting the functioning of the overall digital infrastructure.
- **Digital identity scheme administrator and committed stakeholders:** Behind any successful digital identity programme are entities who act as the scheme administrator and enablers who take ownership of design, development and implementation. A set of involved stakeholders who take part in the process is also a necessary part of the digital identity ecosystem for the rapid adoption and onboarding of relying parties.
- **Government endorsement and participation and the role of the private sector:** The long-term sustainability of a digital identity programme depends on support and backing from the government. This not only instils trust in the system but also boosts adoption by citizens. However, many digital transactions lie within both the government and private sector domains. Therefore, it is important for these parties to collaborate to stimulate adoption.
- **Interoperability:** Standardisation of the identity management infrastructure will improve interoperability, usability and connectivity across different systems within the digital identity ecosystem. Governance of the technical rules and policies should be dynamic to accommodate any changes and improvements. This is one of the critical factors seen in the rapid adoption of payment and national ID schemes across the globe.

17 https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf
18 World Bank: Practitioner's Guide by the Identification for Development (ID4D) Initiative.

IDENTITY SYSTEMS: BASIC CONCEPTS AND TYPES

Identity systems are used by governments and private entities to ascertain the identity of individuals or to prove any claim made by an individual based on valid credentials. Primarily, identity systems can be categorised in two ways:

01

FOUNDATIONAL IDENTITIES:

Foundational identities are mostly used as proof of the legal identity of individuals for a plethora of services and transactions and to enable them to access basic rights and protection. This can range from national population registers to national identifiers.

02

FUNCTIONAL IDENTITY SYSTEMS:

Functional systems are used for authentication and validation for specific sectoral use cases or services only. They can be used for voting, such as a voters identity card, or for travel, such as a passport. In most cases, they have limited scope of usage based on the purpose for which they are made in one sector.

Digital identity systems can fall under both these categories based on the usage and issuance pattern. To understand how the systems are formulated and approached, we need to define the guiding principles for setting up such a system and the different pillars on which these principles rest.

GUIDING PRINCIPLES FOR DEVELOPING THE SOUTH AFRICAN DIGITAL IDENTITY PROGRAMME

The requirements for a robust and efficient digital identity include trust, interoperability, privacy and security, and user consent. It is important to adhere to certain guiding principles as these will give clarity and direction to the programme. These principles are underpinned by ten global principles on identification for sustainable development[19] developed by the World Bank through stakeholder engagements and endorsed by 25 international organisations, associations and development partners. By adhering to these principles, South Africa will be able to ensure that its digital identity ecosystem is inclusive, trusted and useful for its citizens, residents, government and the private sector.

The principles are categorised into the three pillars set out below. These pillars indicate what is most important and what the programme should aim to achieve in the long term.

INCLUSION

Any digital identity must cover all individuals and remove barriers to access and usage in services without discrimination

DESIGN

The digital ID system must be robust, secure, interoperable and sustainable and should use open standards while ensuring vendor and technology neutrality.

GOVERNANCE

The digital ID system must build trust by protecting privacy and user rights while enabling grievance redressal mechanisms and establishing accountability

The principles within each pillar are shown below:

Pillars	Guiding principles based on World Bank report & DHA report
Inclusion	• To ensure universal coverage • To remove barriers to access and usage of information and technology
Design	• To establish a robust, unique and secure programme • To create a platform that is interoperable • To use open standards and ensure technology neutrality • To plan for financial and operational sustainability • To protect user privacy and control
Governance	• To safeguard data privacy, security, and user rights through a comprehensive legal and regulatory framework • To establish clear institutional mandates and accountability • To enforce legal and trust frameworks

19 World Bank: Principles on identification for sustainable development: toward the digital age

CRITICAL SUCCESS FACTORS FOR THE SOUTH AFRICAN DIGITAL IDENTITY PROGRAMME

Developing countries like South Africa face a unique set of challenges when implementing ID systems, especially a digital identity system. The five main universal risks to implementing a new system are exclusion, privacy and security violations, technology lock-in, unsustainable technology and design choices. In addition to these universal risks, many low- and middle-income countries face additional challenges when implementing a digital identity system. These include weak civil registration systems, limited connectivity and infrastructure, low literacy levels, low government capacity and/or trust, poor procurement and insufficient national cybersecurity capacity.

There are several critical success factors associated with the South African digital identity programme, including coordinated governance and sustained stakeholder commitment, a strong operational framework and a well-spread-out distribution network.

WELL DEFINED PROJECT OBJECTIVES AND DESIGN:
Well defined project objectives and KPIs are key to the success of a digital identity programme. The key outcomes should be designed keeping in mind the national goals and user experience.

COORDINATED GOVERNANCE AND SUSTAINED STAKEHOLDER COMMITMENT:
To touch every citizen, clear operational mandates to ID-providing agencies and a sustained political ambience are essential. These projects are ambitious, a significant number of stakeholders, including several public and private players, are involved, which requires good coordination.

STRONG OPERATIONAL FRAMEWORK:
Clear operational guidelines which includes minimum security risks and adequate protection against potential fraud to sensitive data, must be maintained by people with the requisite skill set to execute the programme smoothly.

IDENTIFICATION OF SUITABLE USE CASES FOR ECONOMIC VALUE CREATION:
Classified use cases should be recognised, which will act as economic drivers. Digital identity could create economic value, increased productivity and efficient time and cost savings based on these use cases.

WELL SPREAD-OUT DISTRIBUTION NETWORK:
The success of a digital identity hugely depends on the distribution network. A well-spread-out network can cover even rural areas and make the registration process easy and robust.

> Developing countries like South Africa face a unique set of challenges when implementing ID systems, especially a digital identity system. The five main universal risks to implementing a new system are exclusion, privacy and security violations, technology lock-in, unsustainable technology and design choices.justice.

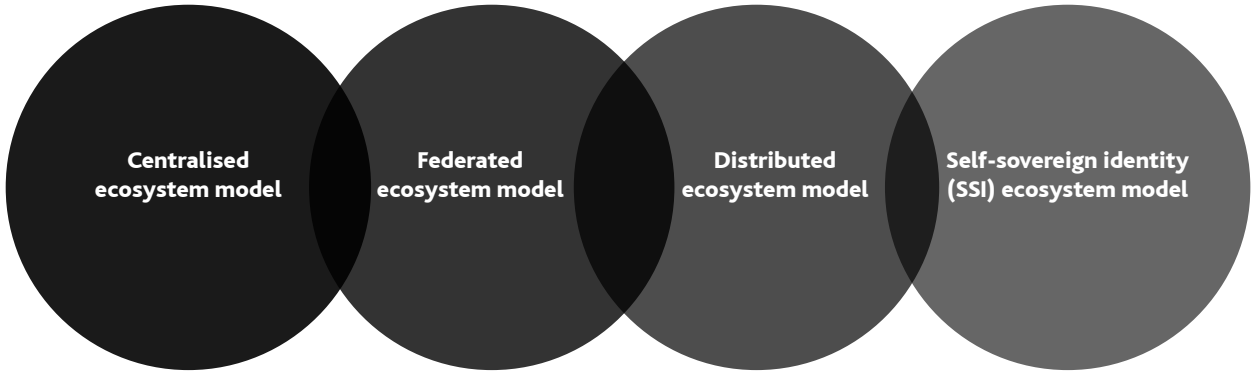
It is also important to understand some of the direct risks and how the critical success factors apply to these in the South African context:

Risks	Critical success factors
• Unclear objectives and lack of well-defined project plan with clear objectives for each phase • Lack of alignment with the existing regulations and user-centric approach to design	**Well defined project objectives and design**
• Absence of coordination between the stakeholders and institutions involved and non-existence of well-detailed governance framework • Non-involvement of stakeholders or no long-term commitment towards the cause	**Coordinated governance and sustained stakeholder commitment**
• Unaddressed potential risks, including data security risks or resourcing risks • Non-existence of proper operating model or clear guidelines	**Strong operational framework**
• Inefficient understanding of the market and choosing unsuitable use cases • Lack of coherence among the stakeholders and defective communication between the parties	**Identification of suitable use cases for economic value creation**
• Lack of adoption by the larger community and residents • Improper branding or messaging and lack of awareness	**Well-spread-out distribution network**

DIGITAL IDENTITY ECOSYSTEM MODELS

There are various ecosystem models that can be examined and adapted when designing and implementing a digital identity ecosystem for South Africa. The distinction between the models rests mainly on the type and role of stakeholders as well as responsibility for the establishment and management of the database.

Different types of ecosystem models have been adopted across the world, namely:



CENTRALISED ECOSYSTEM MODEL

Overview

The centralised model has a single identity provider for a digital identity system which is recognised by the government as providing proof of legal identity. The ID provider is responsible for and has significant control over how authentication is performed and ensures completely consistent ID services and a unified experience for users and requesting parties.

Key features

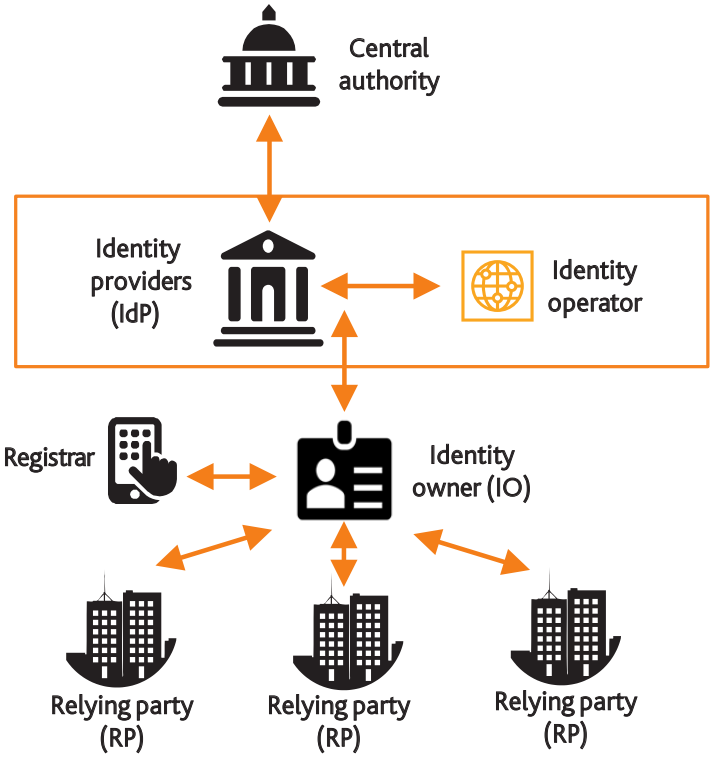
- One central authority which holds all user attributes and owns the identity system.
- The identity provider (IdP) authenticates the user, shares their attributes with relying parties (RP), and transfers either a fixed or a tailored set of attributes to the RP to enable it to complete a transaction on behalf of the user.
- Identity information can be transferred directly through a physical form factor (e.g., a smart card) or through a digital brokerage system.

Benefits

- **Easy integration:** By authenticating from a central database, complex integrations are eliminated.
- **Stronger compliance standards:** The central authority, being a government agency, can ensure strong and better compliance.

Challenges

- **Hindrance to adoption:** Enrolment and registration process are done by third parties and can be time consuming and prone to data leakages.
- **Time complexity:** Processes are handled by public entities, often with intricate governance mechanisms, sometimes leading to increased time complexities.



FEDERATED ECOSYSTEM MODEL

Overview

A federated identity model allows a person's electronic identity and attributes to link to multiple distinct identity management systems or organisations. Federated identity systems are single sign-on (SSO) schemes that allow a user to access multiple separate services by identifying information established in one security domain.

Key features

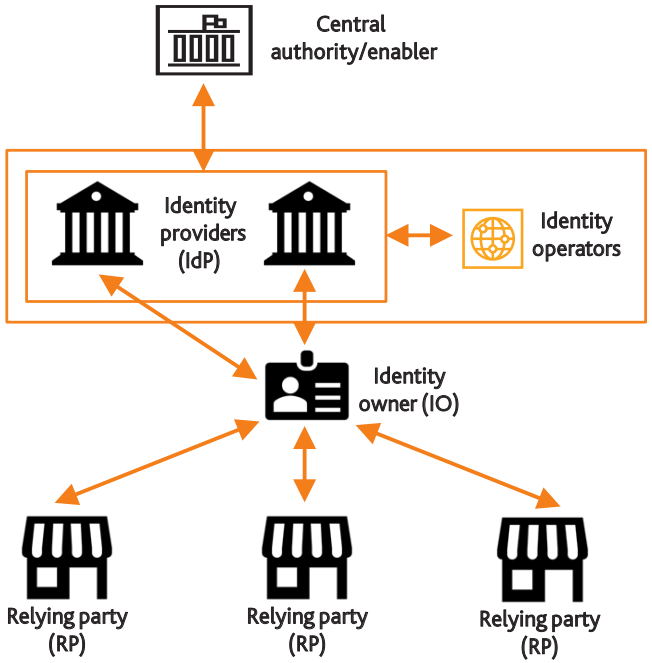
- A limited number of entities store and provide identity information.
- The system has a single IdP that stores user information, while a separate set of IdPs authenticates users who are attempting to transact through RPs. These systems are often government-driven, and the government acts as the centralIdP/central authority.
- Some of the use cases require user consent for attributes to be transferred from IdP to RP.

Benefits

- **High adoption:** Identity providers such as banks enhance trust and drive higher adoption.
- **Interoperability:** Helps improve interoperability through the SSO feature.

Challenges

- **Lack of data control:** Users have no control over their data and enterprises can monetise it without proper regulations in place.
- **Absence of governance:** In cases where there is no central authority or board to set governance standards it is prone to risk.



DISTRIBUTED ECOSYSTEM MODEL

Overview

A distributed identity model comprises multiple regulated and recognised entities issuing electronic identities. These identities, however, only operate based on bilateral agreements with other organisations without a central or trusted framework. Identities can be used for specific purposes as agreed between issuers and acceptors.

Key features

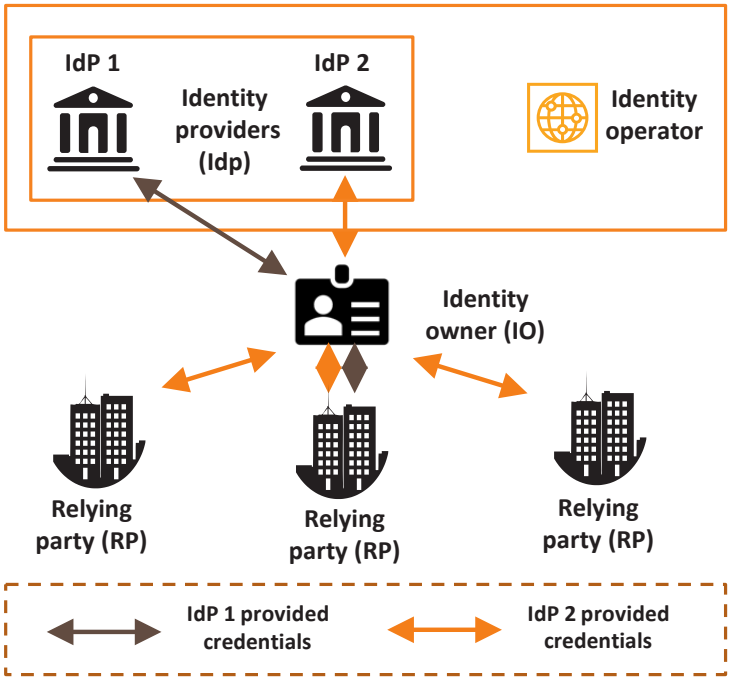
- Multiple issuers of identities; each issuer owns the identity system and holds the user attributes.
- Digital identities can only be used based on bilateral agreement between verifiers and issuers.
- There can be many providers that each maintains a ledger of digital identities issued by multiple issuers.
- There may not be a governance body or a central authority and thus the system relies on common operating standards for interoperability.

Benefits

- **Specificity of identity:** The IDs are used for specific purposes to prevent duplication because of multiple vendors.
- **Faster processing:** The identities are mostly functional and with a limited scope of use, which helps in faster processing for the services or sectors they are designed for.

Challenges

- **Lack of interoperability:** The individual IDs work in silos for specific functions and are only accepted by services for which they are strictly devised.
- **No central trust framework:** The ID providers can have their own rules, resulting in the lack of a centralised trust framework.



SELF-SOVEREIGN IDENTITY ECOSYSTEM MODEL

Overview

The self-sovereign identity (SSI) model allows users to control and own their identity credentials digitally, without intervention from administrative authorities. The user is the single source of truth for their own identity and can give consent to verifiable claims by third parties as required. This model is based on decentralised identifier documents (DIDs), verifiable credentials and distributed ledger technology (or blockchain).

Key features

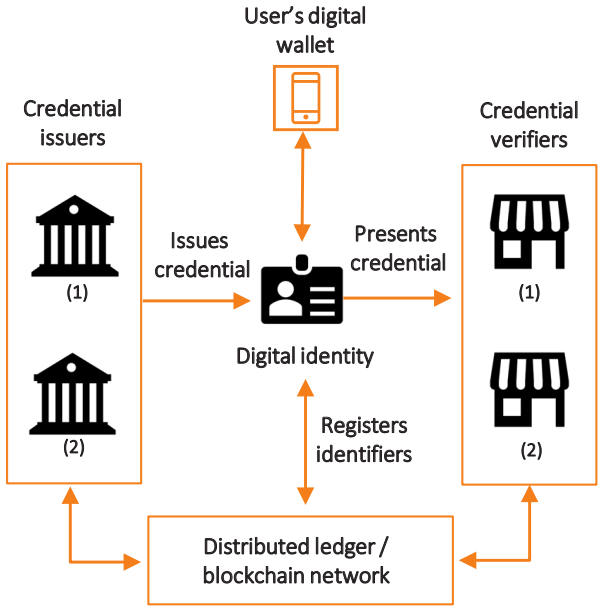
- SSI offers a secure digital identity model with minimum personal data management for organisations (issuers and verifiers).
- Users have control over and access to their own data.
- The model is interoperable and transportable across applications, devices and platforms.
- Sharing of user data and identity may require consent from individuals.
- A trust framework provides policies and guidance across areas such as governance, legal and technology. The trust framework is defined and governed by the trust alliance and regularly shared and updated based on the feedback of the participants.

Benefits

- **Data control and security:** Data control is with the user, making it highly secure from breaches or data leakages.
- **Resilience and robustness:** The distributed architecture lowers the risk of single point of failure (SPOF) and enhances the long-term sustainability of the ecosystem.

Challenges

- **Understanding the concepts:** In most countries, the design and implementation of this ecosystem model are still evolving; therefore, a deeper understanding of the underlying architecture is required, along with technological expertise.

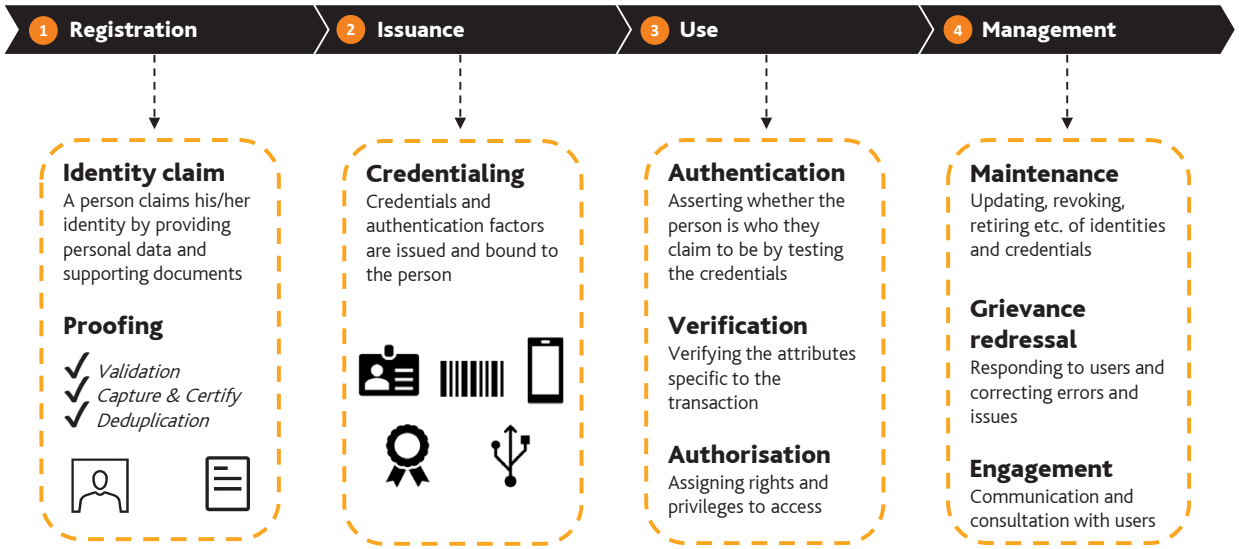


DIGITAL IDENTITY LIFECYCLE IS ESSENTIAL TO CREATE TRUST IN TRANSACTIONS BETWEEN PEOPLE, IDENTITY PROVIDERS, AND PUBLIC AND PRIVATE SECTOR RELYING PARTIES

According to the World Bank,[20] a digital identity lifecycle refers to the process of establishing a person's digital identity and then using this identity in later transactions. A lifecycle is vital to creating trust in a variety of transactions between people, identity providers and relying parties. A digital identity lifecycle generally has four major stages.

Key features

- **Identity claim:** The identity claim stage deals with the onboarding of a user into the ecosystem by validating their proof of identity through existing documents or whatever golden source is considered for the process. The user generally uses a digital platform to onboard by submitting the required proof.
- **Credentialing:** The digital credentials are issued to the user who has onboarded, which they can store in their applications. The credentials are issued by entities who are verified as credential issuers by the authority and adhere to the trust framework set up by the authority.
- **Authentication/Verification/Validation:** This stage helps a user access any service that is provided by the relying parties who have onboarded within the ecosystem and integrated their services to use digital identity as a tool for authentication or verification of user credentials.
- **Management/Grievance redress:** The updating of personal data or credentials and revoking access to the system is all part of management of the digital identity ecosystem and carried out by the authority in coherence with the stakeholders to provide a seamless experience.



The lifecycle is not a one-time event but rather a process that starts when a person first registers and their identity is created. The process continues with authentication of that identity and any updates to the attributes and credentials over time. The process ends when the identity record is retired or invalidated after death, for example. The lifecycle may be completed by a single stakeholder or may be split between multiple public and/or private sector stakeholders. Therefore, this process can be applied irrespective of the model adopted by a country.

20 Source: World Bank Practitioner's Guide by the Identification for Development (ID4D) Initiative.

GLOBAL ANALOGUES AND KEY LEARNINGS

> There are several countries across the world that have set up and implemented a successful digital identity structure.

Digital identity is an important infrastructure for any modern society and a country wanting to move towards a digital economy. Therefore, it is important to develop a robust, secure and comprehensive programme that can meet the country's identity, social, political and economic needs, now and in the future. Designing and implementing a fit-for-purpose digital identity programme is a complex process with several risks and challenges.

There are several countries across the world that have set up and implemented a successful digital identity structure. In developing South Africa's digital identity journey, we applied some of the global best practices that have been followed across countries such as India, Estonia and Sweden.

India adopted the centralised digital identity ecosystem model and it has proven to be one of the most successful digital identity programmes in terms of adoption and use. With almost 18% of the world population, India required its government to implement an all-inclusive identity management system which would not only serve as a unique identifier but was also accepted by its citizens. Aadhaar, India's unique digital identity, serves as a single identifier across all major service sectors of the country. Aadhaar-enabled use cases have been widely adopted in both public and private sectors, benefiting both businesses and individuals. These use cases impact key areas such as e-KYC, government aid, social welfare schemes and direct benefit transfers (DBT).

Estonia is one of the most digitally advanced countries in the world with almost 99% of its population having access to their SSI based e-ID. This penetration rate helped Estonia to launch the Estonian National Health Information System, which provides a nationwide system that integrates all healthcare providers and medical institutions. Any patient can thus access all their records from multiple places through a single portal. The system also allows healthcare professionals to access all records at a single place, which results in the sector being able to better serve the community.

The Nordic region is home to one of the largest economies in the world. As one of the first movers and innovators in the payment market, Nordic banks decided to collaborate and introduce a bank ID to ease the payment system for citizens. Similarly, most of the major banks in Sweden formed a consortium with the aim to develop a general infrastructure for e-IDs. It not only met the requirements of authorities and banks and became acceptable to both the public and companies but also simplified the taxation/mortgage application system across the country. Lessons learned and considerations from these countries were applied to the South African environment, which has helped craft the digital identity story for South Africa.

Source: https://www.ibef.org/economy/indian-economy-overview
Source: International Monetary Fund's World Economic Outlook database (April 2021)

THE INDIAN ECONOMY IS A MIDDLE-INCOME DEVELOPING ECONOMY

Backed by its democratic nature and strong strategic alliances, India is expected to become one of the top three economic powers in the next 10 to 15 years.[21] It is currently among the world's 10 biggest economies.[22]

INDIA'S SOCIO-ECONOMIC LANDSCAPE

Despite India's exposure to global trade and strategic alliances with multiple countries, it saw a decline in growth in several sectors in the 2020 financial year. Like the rest of the world, India was left reeling from the impact of COVID-19, with its Gross Domestic Product (GDP) growth rate falling to an all-time low of -7.9% in the 2020 fiscal year.[23]

During 2020, India's main economic sectors as a percentage of gross value added (GVA) included the service sector (58%), manufacturing (19%), agriculture (18%) and other sectors (9%).[24] Although agriculture has been one of India's economic pillars for many years, recent government policies such as 'Make in India' have enabled services and manufacturing to become two of the major sectors in the current Indian economy.

Internet penetration among adults in the country is relatively low, with only 34.5% of adults having internet access. However, India provides one of the lowest rates globally per gigabyte of data at $0.68 per GB.[26] Furthermore, the country's banking population has risen to over 80% after several financial inclusion schemes were introduced by the Indian government.

INDIA'S ECONOMY - 2020

Real economic growth rate: **-7.9%**

9.46/25 (Accelerator)
Global Digital Readiness Index Score

6.3%
Consumer price inflation rate

1.3 billion
Total population size

7.11%
Unemployment rate

35.7
Income Gini (Gini-Coefficient)

Largest sectors in India (as a % of GVA)

Services	Manufacturing	Agriculture	Others
58%	19%	18%	9%

Global competitiveness

49.4/100
Public institutions & governance ranking

57.3/100
Competition & anti-trust frameworks ranking

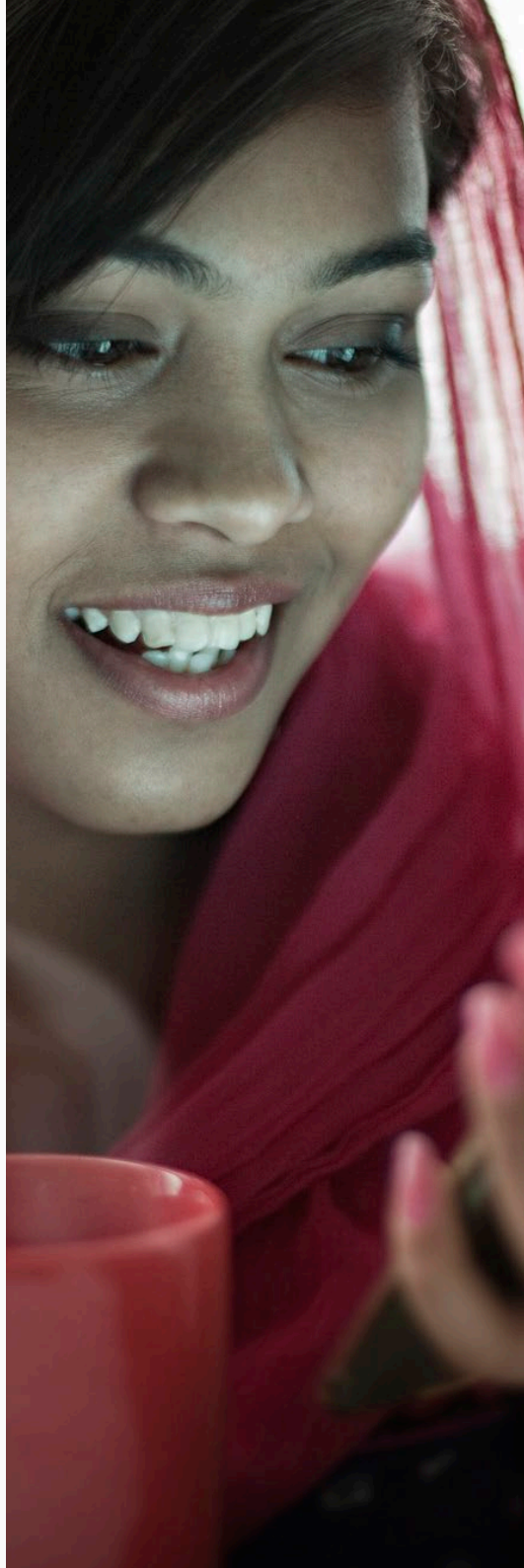
32.1/100
ICT adoption

Digital inclusion

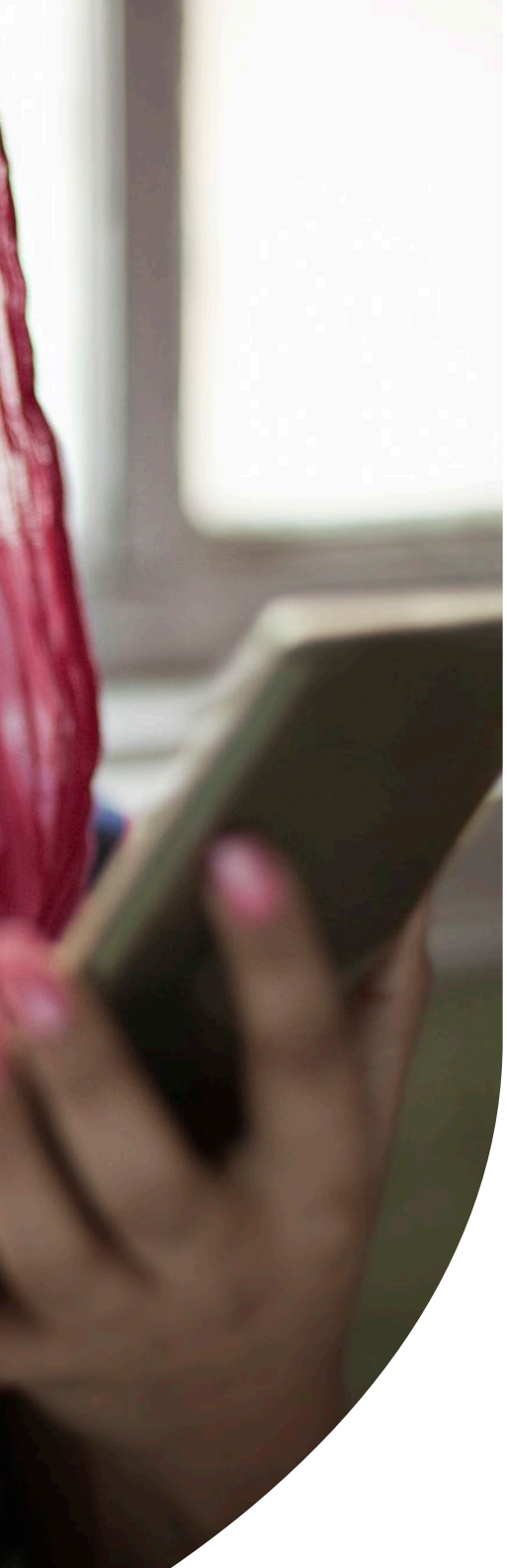
34.5%
Internet users (% of adult population)

US$0.68
Cost of 1GB data

80%
Percentage of banked population



21 Source: https://www.ibef.org/economy/indian-economy-overview
22 Source: International Monetary Fund's World Economic Outlook database (April 2021)
23 Source: https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/IND?year=2021
24 Source: https://www.ibef.org/economy/economic-survey-2020-21
25 Source:http://reports.weforum.org/social-mobility-report-2020/social-mobility-rankings/#series=NETUSERPCT
26 Source: https://www.cable.co.uk/mobiles/worldwide-data-pricing/



EVOLUTION OF INDIA'S ID SYSTEM

The project started in 2002 when a group of ministers devised the idea of having a multipurpose national identity card. In 2006, the Department of Information Technology, the Ministry of Communications and Information Technology, and the government of India approved the creation of what they named a unique identification for below-poverty-level families.

Based on a **Strategic Vision Unique Identification of Residents** paper by the committee, an empowered group of ministers (EGoM) was set up on 4 December 2006 to collate a national population register and lead the unique identification number project.

> In developing South Africa's digital identity journey, we applied some of the global best practices that have been followed across countries such as India, Estonia, and Sweden.

THE EVOLUTION OF INDIA'S IDENTITY SYSTEM

2002

- India always had a fragmented market in terms of identity cards
- Considered a need for a common identity
- A group of ministers introduced the concept of a "multipurpose national identity card" to serve as a record of citizenship

2006 - 2008

- The concept of a unique identity for all was finally conceived
- Planning commission of India created Unique Identification Authority of India (UIDAI)
- Ministry of IT approves the unique identity

2009 - 2010

- UIDAI was elevated to cabinet committee - level post
- Organisational structure was created
- The Aadhaar programme was launched in February 2009
- 1st Aadhaar was issued on 29 September 2010

2011 - 2016

- 2011: Number of Aadhaar holder exceeds 100 million
- 2015: A horizon of schemes being introduced and included into the scope of Aadhaar
- 2016: Aadhaar bill is passed as money bill

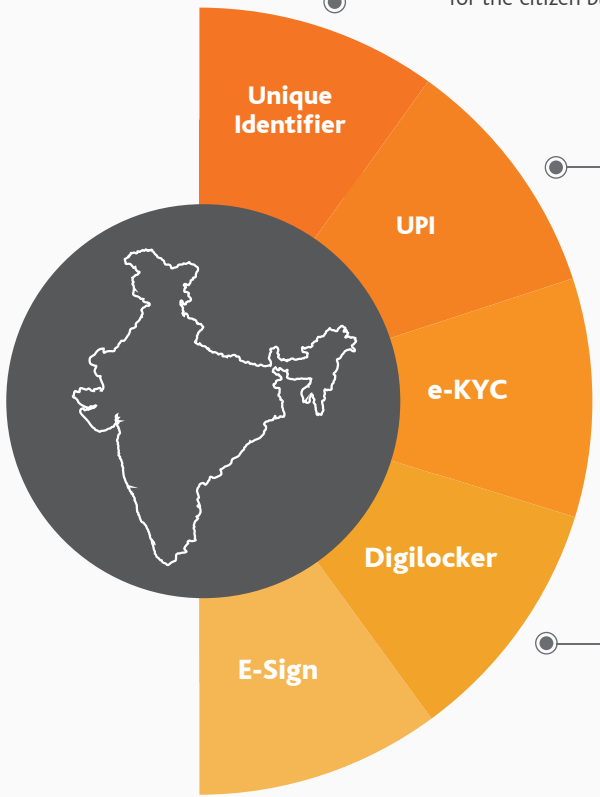
2017 – Present

- 2017: several ministries make Aadhaar mandatory for social welfare schemes
- The centre proposes to make the Aadhaar card mandatory to file Income Tax Returns
- 2018: QR - based offline Aadhaar enrolment introduced
- Present: Almost 1.3 billion Aadhaar cards generated

AADHAAR: INDIA'S UNIQUE DIGITAL IDENTITY

Aadhaar was launched with a view to bringing all citizens under one umbrella digital identity, thus eliminating the inconvenience of multiple identities for multiple services. The Aadhaar unique 12-digit identity, with the help of government investment, addressed different problem areas, which resulted in better digital adoption across the country.

Figure 1: Public digital platforms using Aadhaar[27]



1.3 Bn Enrollment

Aadhaar Enrolment: 12 digit unique identification number for the citizen based on biometric and demegraphic data.

22.3 Bn Transactions

Enables all bank account holders to send and receive money instantly using smartphones, without using bank information.

9.5 Bn Transactions

Paperless KYC process veryifying subscribers' identity and address electronically through Aadaar.

67.06 Mn Users

Platform for issuing and verifying documents digitally using cloud storage linked to Aadaar.

8.7 Mn Transactions

Replaces manual paper based signatures by allowing Aadhaar holders to electronically sign documents.

27 Source: NPCI, UIDAI Dashboard, DigiLocker Dashboard)

IDENTIFYING AN AADHAAR-BASED USE CASE: DIRECT BENEFIT TRANSFER (DBT)

The government of India provides subsidies to its citizens in different sectors of services. These subsidies are one of the major economic driving forces, contributing almost 4% to the country's GDP. The subsidies were previously manually transferred to citizens via multiple intermediaries across the country. The lack of a well-defined and transparent public distribution system led to increased revenue leakages and fraudulent transactions. To address these problems, Aadhaar-based DBT was launched in 2013, promising to transform service delivery in India by transferring government subsidies directly to the citizens.

CHALLENGES IN DISTRIBUTION OF SOCIAL WELFARE BENEFITS BEFORE THE INTRODUCTION OF AADHAAR

There were multiple challenges in providing subsidies to citizens:

- Lower-income families in India spend almost 56% of their income on fuel and electricity, education, food and health. Before the introduction of Aadhaar, the absence of a trusted and proven national identity resulted in huge financial leakages in social welfare benefits. An estimated 70% to 85%[28] of all government subsidies were not reaching the intended beneficiaries. This meant a heavy expenditure loss to the social sector.
- Due to the absence of a proper identity-based public distribution system, intermediaries were largely involved in distributing social welfare benefits. This resulted in increased structural expenditure and operational risks in the public distribution system.
- Lengthy manual subsidy disbursement processes resulted in delayed aid disbursements to beneficiaries.

> Aadhaar-enabled use cases have been widely adopted in both public and private sectors, benefiting both businesses and individuals. These use cases impact key areas such as e-KYC, government aid, social welfare schemes and direct benefit transfers (DBT).

28 GSMA Aadhaar Report

BENEFITS TO INDIA OF INTRODUCING DBT

The DBT scheme was launched to improve the public distribution system and make it more systematic. Before the launch of DBT, the government subsidy distribution system was tedious, with everything being done by hand. The government and citizens alike depended heavily on intermediaries for rolling out government aid. Maintaining such a huge manual system incurred huge cost to the government, while citizens were not getting their subsidies on time.

Citizens:	• Citizens receive the government aid directly into their account in almost real time, which not only saves them time but also builds trust in the government. • The government usually bears the cost of the goods to be distributed amongst the people targeted. • This PDS ensures citizens get these essential goods for a very low price or some times for free. • Also, as DBT is directly linked with the Aadhaar card, it authenticates any beneficiary via biometrics hence, duplication is eliminated which, ensures that aid reaches the intended beneficiaries.
Government:	• DBT eliminated all the intermediaries who were previously involved in the public distribution service. this helped the government to reduce the operational cost of disbursement of money. • Aadhaar - based DBT also eliminated ghost beneficiaries, which in turn saved the government a good amount of money. • DBT also reaffirmed public trust in the government.
Economy:	• As citizens receive their aids in real time, public buying capacity increases, which is good for the country's economy. • Money started to flow in the market and the buying capacity of people increased as a timely infusion of money made life a little easier for them. • This was a good sign for the economy and overall market as flow of goods became normal again.

KEY LEARNINGS FROM INDIA FOR SOUTH AFRICA

Despite being a highly populated country, India was able to achieve a high adoption rate. Aadhaar has changed the Indian socio-economic and demographic landscape, not only for the citizens but also for the Government. It has impacted the lives of citizens by valuing privacy, shaping up public policies and harnessing technology.

India's experience with the Aadhaar journey could provide some insights to other countries that are developing and implementing a digital identity system:

- **Inclusivity:** Aadhaar played a significant role in increasing the number of banked customers and enhancing the public distribution system. With the help of Aadhaar-based eKYC, it was easier for people to open a bank account in their name, and the Aadhaar-based DBT system ensured digital distribution of social welfare aid to the intended beneficiaries' accounts. The Aadhaar system propagated an all-inclusive cashless economy, which can be a model to follow for many countries. Over 27.5 million ghost or non-existent records were eliminated in the food distribution programme[29], for example.
- **Making data privacy a true priority:** Despite being the world's largest biometric identity programme, the Aadhaar system works with a minimum set of personal information of citizens to ensure better management of the data as well as prioritise maintaining the privacy of the data (personal information is treated as being very sensitive).
- **Building a robust and cost-efficient identity infrastructure:** The Aadhaar programme costs US$1.16 per enrolment, making it one of the lowest-cost identification programmes in the world. Aadhaar's low cost is achieved through the absence of a smart card, as a country like India with relatively weak connectivity in rural areasmakes it difficult to enroll and authenticate people virtually. To address this concern, UIDAI introduced QR-based offline verification in 2018, which not only expedited the registration process but also reduced the overall cost.

29 Source:https://documents1.worldbank.org/curated/en/745871522848339938/Public-Sector-Savings-and-Revenue-from-Identification-Systems-Opportunities-and-Constraints.pdf

KEY GUIDING QUESTIONS TO ASSESS THE SUCCESSFUL IMPLEMENTATION OF THE AADHAAR IDENTITY SYSTEM

The implementation of Aadhaar resulted in significant savings for the government. In 2017/18, the government of India saved over US$14 billion through the Aadhaar-based DBT scheme.
India's experience with the Aadhaar journey could provide some insights to other countries that are developing and implementing a digital identity system:

1

What digital identity ecosystem model was adopted and why?

- India has adopted the centralised model as their digital identity ecosystem model.
- an all-encompassing identity was required.
- This should also be digital due to the limitations of other available identities and involve direct government intervention.
- Low digital literacy and lesser banked adult population during the planning phase led to a centralised solution to deliver government services.

2

Who are the stakeholders involved?

- Central authority
- Identity provider
- Identity operator
- Relying parties
- Enablers

3

What was government's involvement in the digital identity programme?

- Introduction of Aadhaar Cards was one of the flagship programmes under Digital India Plan of Government India.
- The GOI patronized the Aadhaar programme, monitored the issuance of the cards, introduced several social welfare schemes around Aadhaar and managed data privacy & security closely.

4

What technology was used in the development of digital identity?

- Biometric deduplication is the core of the Aadhaar technology.
- UIDAI has 3 Automatic Biometric Identification System (ABIS) providers that are competing against each other for work.
- Aadhaar data is encrypted using two of the most robust public key cryptography encryptions in PKI-208 and AES-256.

5

How long did it take for successful adoption of digital identity?

- Aadhaar was conceptualized in 2006.
- UIDAI was formed in 2009.
- 1st Aadhaar was issued in 2010.
- Currently almost 1.3 billion Aadhaar cards generated.

6

What regulatory and policy frameworks were adopted?

- Aadhaar is one of the major game changes in the Indian Economic landscape.
- Government of India has clear and strict data protection policies assigned to Aadhaar.

7

What are the accelerators that enabled adoption of the digital identity?

- India being a vast country it was important to have a National Public register to provide an identity to each citizen. Also, it was essential to remove multiple identities for multiple services and an umbrella identity introduction was required to bring all the services under that card. A digital identity was also required for better financial inclusion and a better pub lic distribution system. Aadhaar became one of the major contributor to the economy while acting as a single identifier for the citizens.

ESTONIA IS ONE OF THE WORLD'S MOST DIGITISED ECONOMIES

Estonia is a developed country on the list of high-income economies. It has experienced robust economic growth in the last few years (excluding 2020) with a growth rate of around 5% in 2019[30], higher than other developed countries. It is also ranked high on the Human Development Index (HDI) (around 0.892)[31].

ESTONIA'S SOCIO-ECONOMIC LANDSCAPE

The past year has been a little slower in terms of economic growth for Estonia and has seen the real GDP growth decline to -2.9%[2], which is lower than that of many countries. The decline in growth has severely impacted unemployment in the country, which increased to 53.6%[32].

As of 2020, Estonia's main economic sectors as a percentage of GVA included trade (12%), real estate (12%), transport (8%) and public administration (8%). Its trade and public administration are almost completely digitised, making them two of the top-earning sectors in the country. Internet penetration is very high in the country at around 89.5%[6], making it easier to digitise the economy for its citizens. Additionally, the price of data is low, giving people more access to online data. The country implemented online banking in1996 and has a banked population of almost 98%.

ESTONIA'S ECONOMY - 2020

Real economic growth rate: -2.93%

17/180 — Corruption perception index score

3.6% — Consumer price inflation rate

1.3 million — Total population size

7.4% — Unemployment rate

32.7 — Income Gini (Gini-Coefficient)

Largest sectors in Estonia (as a % of GVA)

Trade	Real estate	Transport	Administration
12%	12%	8%	8%

Global competitiveness

66.5/100 — Public institutions & governance ranking

66.9/100 — Competition & anti-trust frameworks ranking

78.8/100 — ICT adoption ranking

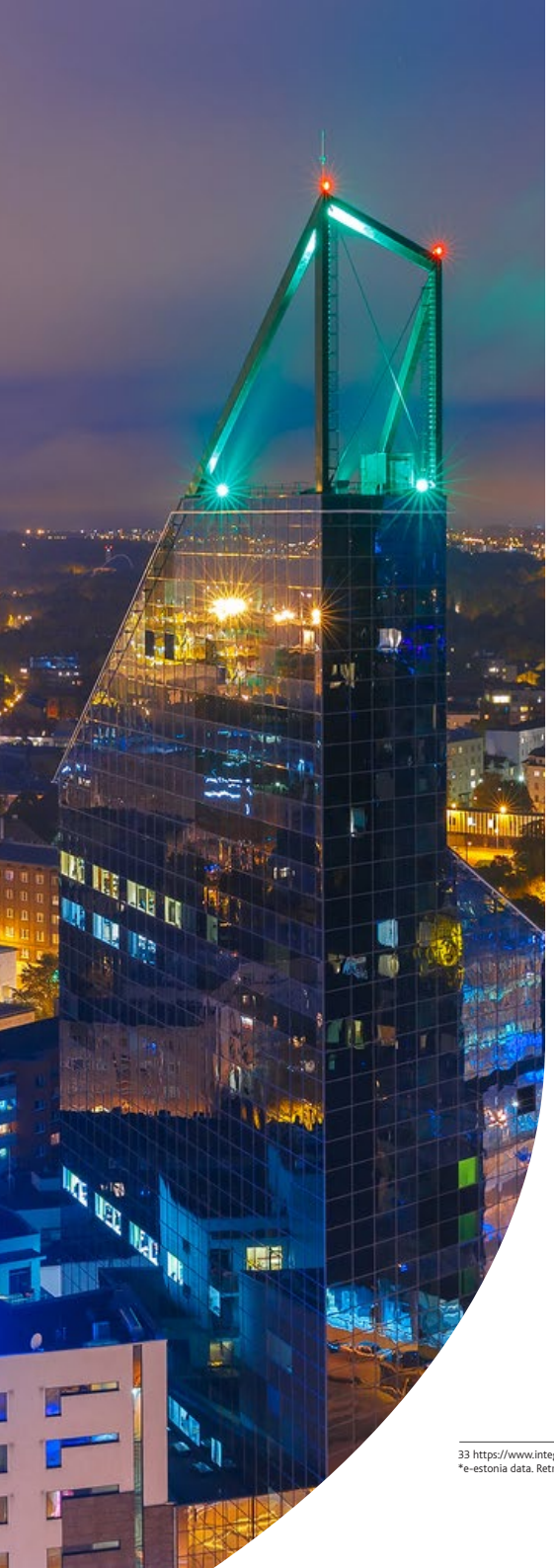
Digital inclusion

89.5% — Internet users (% of adult population)

US$1.39 — Cost of 1GB data

97.7% — Percentage of banked population

30 Eurostat
31 http://hdr.undp.org/sites/default/files/hdr2020.pdf
32 Statistics Estonia, Fitch Solutions



EVOLUTION OF ESTONIA'S ID SYSTEM

The Estonian e-ID system was launched a year after independence in 1992[33]. The Government sector made a political commitment to develop an information society. The first services were in the banking and financial services sectors, which started in 1996. In 1998, the Principles of Estonian Information Policy was approved, which paved the way for a digital society. Next, e-health services started in 2000, when legislation was passed requiring healthcare providers to have access to a computer with internet access.

By 2019, 99%* of the Estonian population had an e-ID card, with 17%* using mobile IDs and another 35%* using the smart ID application. More than 2 600[34] services are on the X-Road platform, which include 99% of the government's services.

> Estonia is one of the most digitally advanced countries in the world with almost 99% of its population having access to their SSI based e-ID.

THE EVOLUTION OF ESTONIA'S IDENTITY SYSTEM

1991
- Estonia got independence
- The landline phone coverage was <50% of the population

1996
- Internet banking was introduced in the country
- Banks created digital authentication services for the account holders and it was also used by the Income Tax Authority

2002
- The issuance of first e-ID card
- Digital signature was implemented using Cybernetica's X-Road (A peer-to-peer data exchange platform with high security)

2006
- The total number of e-ID cards exceeded 1 million
- Total coverage of the e-ID went past 90% of the total population

2007
- Mobile ID was introduced which let the users validate their identity using their mobile phones
- Private keys were stored in SIM cards, so people no longer required the smart card

2014
- E-residency programme was introduced for foreign nationals to apply for digital residency
- Approximately1/3rd of the overall votes in the parliamentary elections were cast digitally

2017
- A mobile based authentication solution 'Smart-ID' was launched which started using SplitKey technology
- SplitKey provided a method of digital signing documents and authentication for online banks

2019
- The users of Smart-Id applications exceeded 2.5 million including Latvia and Lithuania
- Total transactions per month exceeded 50 million and 44% of votes were casted digitally that year

33 https://www.integratedcare4people.org/media/files/CaseProfileEstonia.pdf
*e-estonia data. Retrieved from https://e-estonia.com/

ESTONIA'S E-HEALTH SYSTEM

The e-ID, followed by subsequent innovations such as the SIM-card-based mobile ID and the smart ID application, based on SplitKey technology, represent some of the most advanced digital identity systems in the world. Its identity ecosystem is so robust that it has helped Estonia turn into a digital society with seamless access to services.

One of the problems that Estonia tried to solve prior to 2008 was the availability of health records in emergency circumstances and to track the overall health profile of a patient when admitted for any critical surgery.

Estonia launched X-Road in 2002, which is a peer-to-peer data exchange platform that is highly secured through encryption. It acts as a backbone for private and public entities to provide e-services in sync with each other. Based on this underlying architecture, they decided to launch the **Estonian National Health Information System in 2008**. As part of it, e-health record, e-prescription and e-ambulance applications were also introduced.

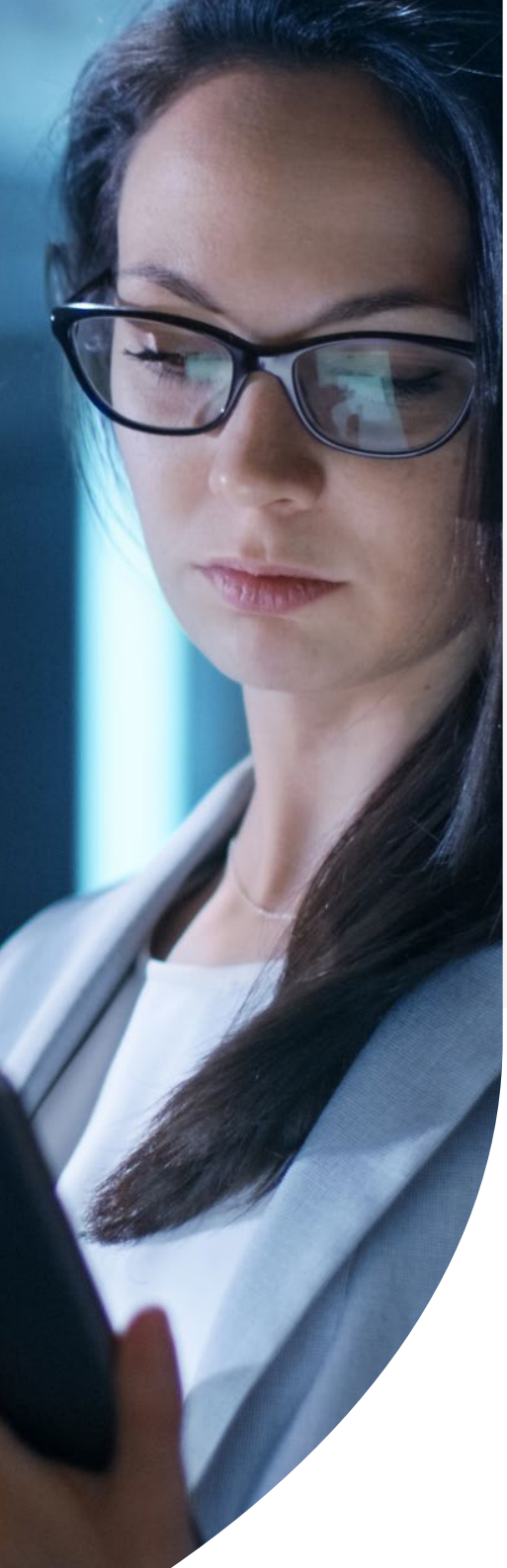
- **E-Health Record** is a nation-wide system that integrates all healthcare providers and medical institutions so that patients can access all their records from multiple places/sources through a single portal. It also helps the healthcare professionals to access all records in one place, which can be lifesaving. Since 2015, 95%[35] of data generated by medical institutions has been digitised and stored in the system. Currently, it manages over 1.8 million[36] patient queries every month and almost 99%[9] of the patients in the country have their digital record in the system.
- **E-Prescription** is a digitised and paperless way for issuing and storing prescriptions. Currently, over 99%* of the prescriptions issued to patients are through this system.
- **E-Ambulance** is a system that detects an emergency and initiates a phone call for an ambulance within 30 seconds and sends the ambulance to the desired location as fast as possible, saving lives. The doctor can use the patient's ID code to check their records in such emergencies through the e-patient portal.

CHALLENGES BEFORE THE INTRODUCTION OF E-HEALTH

In the late 1990s, Estonia faced the problem of fragmented information held by healthcare professionals and institutions at different levels. This resulted in an overdependence on the patient's store of records or hard copies every time someone had a medical appointment. As the rates of circulatory diseases increased from 2 337[37] per 100 000 in 1990 to 3 175 per 100 000 in 2000, it was imperative for the government to find a solution for patients with chronic illness. This way, treatment could be started as soon as the patient was admitted.

> Estonia launched X-Road in 2002, which is a peer-to-peer data exchange platform that is highly secured through encryption.

35 https://na.eventscloud.com/file_uploads/c5da2a5e465f932e6debe55020e70899_E-health-factsheet.pdf
36 https://e-estonia.com/solutions/healthcare/e-health-record
37 https://www.integratedcare4people.org/media/files/CaseProfileEstonia.pdf
*e-estonia data. Retrieved from https://e-estonia.com/



BENEFITS TO ESTONIA OF THE INTRODUCTION OF E-HEALTH

The implementation of E-Health Record and similar services has immensely helped citizens. The national health information system has changed the whole medical ecosystem of the country and made it easier to track trends and allocate resources usefully. Some of the major benefits for the three major parties involved in this ecosystem are:

Citizens:	• The patients can access their records directly from the e-patient portal and they don't have to carry the hard copies anymore. The chance of old reports getting lost has gone to zero. • Parents can access records of their underaged children and of others who have given them their access. • The e-ID or Mobile-ID is enough to login the e-patient portal without any hassles. • The access to prescriptions can be done online and one can review the past doctor visits as and when required. • In an emergency they can have access to Ambulance within 30 seconds due to e-Ambulance.
Government:	• The whole system has become more secure due to the KSI Blockchain being used as the underlying architecture. • The immutable and unremovable trail of records has ensured maximum transparency in governance over the medical sector. • Monitoring of the actions of private medical entities from both a governance and technical perspective has become easier. • Currently it has more than 20 million health documents and another 30 million* events. More than 50%* of the doctors are referred digitally, and 99%* of the prescriptions are issued digitally. • The ministry can also measure health trends based on the information collected and track epidemics.
Economy:	• Health professionals can now access the records of their patients, who have given them their access, directly from their homes. • In emergency situations hospitals can access urgent past reports before moving on for time critical surgeries. • The prescriptions can be issued by doctors online and they don't have to carry any paper-based materials.

*Republic of Estonia, Ministry of Affairs, (2017). Factsheet: E-Health in Estonia.

KEY LEARNINGS FROM ESTONIA FOR SOUTH AFRICA

Estonia has been spearheading digital identity innovations for the past decade and a half, and it has provided several learnings and insights. Some of those key insights are:

- **Privacy and trust:** Estonia has always kept the trust of people as a pillar for their digital society and it has given special attention to privacy since the advent of e-IDs. The introduction of a keyless signature infrastructure (KSI) blockchain after 2007 and giving citizens ownership of their personal data are prime examples of how an information society should work.
- **Interoperability and interconnectivity:** The existence of silos decreases the efficiency of the whole digital identity ecosystem. The Estonian government ensured that all sectors and private entities were onboard the X-Road system. This ensured that all public and private services could be integrated.
- **Digital society:** Estonia showed that the goal was to create a digital society. To achieve this, Estonia has developed connectivity and technology infrastructure at a country level to support this ambition.
- **Resilience**: Since 2002, starting with e-ID, the country has faced multiple challenges, from cyber-attacks (2007) to European Union General Data Protection Regulation (GDPR) violations by some pharma companies in areas of privacy. Nevertheless, Estonia continues to drive innovation and improve the regulatory landscape.
- **Potential for commerce:** With programmes like e-Residency, Estonia demonstrates that digital identity is not only a change agent but can also act as a tool for alternate revenue generation for the government. E-Residency lets people in other countries set up businesses in Estonia for which they pay taxes, and some charge for accessing the services.

KEY GUIDING QUESTIONS TO ASSESS THE SUCCESSFUL IMPLEMENTATION OF E-HEALTH SERVICES

Estonia has the most highly developed national ID card system in the world. The mandatory national card also provides digital access to all of Estonia's secure e-services.

1

What digital identity ecosystem model was adopted and why?

- Estonia adopted a **self-sovereign identity model** which has a centralized blockchain maintained by the government. It was adopted as it gave the citizens data privacy and security while maintaining ownership.

2

Who are the stakeholders involved?

- **Central authority & ID operator:** Information System Authority (RIA)
- **ID providers:** Police and Border Guard, Ministry of Foreign Affairs
- **Enablers:** E-Estonia briefing centre, SK ID Solutions etc.

3

What was government's involvement in the digital identity programme?

- The whole system is driven by the **Information System Authority** as an oversight body which is part of the Estonian government and major IDs are issued by government bodies like the police and border guard.

4

What technology was used in the development of digital identity?

- The underlying architecture is a **KSI Blockchain**; since 2007, they have been using SplitKey technology in Smart-ID application to maximize security.

5

How long did it take for successful adoption of digital identity?

- The e-ID was first issued along with a digital signature in 2002. Later, a Mobile-ID and Smart-ID platform was launched. **It took 15+ years to onboard multiple e-services**.

6

What regulatory and policy frameworks were adopted?

- The country as part of EU **follows all GDPR measures** and they have strict policies against misuse of personal data and access to data by entities.

7

What are the accelerators that enabled adoption of the digital identity?

- **Smartphone penetration:** The smartphone penetration based on the monthly active users in Estonia is pegged at 63.13% of the population, which helped adoption of Mobile-ID.
- **Banks leading the adoption:** The two largest banks in Estonia, Swedbank and SEB, were the firsts to implement Mobile-ID for their services which helped their customers onboard to the system.

SWEDEN IS A STRONG KNOWLEDGE-BASED ECONOMY WITH WELL-INTEGRATED GLOBAL VALUE CHAINS

Sweden is a country that ensures high standards of living, well-being, income and gender equality as well as a high environmental quality for its inhabitants (around 0.892). There has been widely spread growth over the past five years, with consumption, investment and exports all contributing significantly.

SWEDEN'S SOCIO-ECONOMIC LANDSCAPE

Despite Sweden's exposure to global trade dynamics, COVID-19 has had a rather limited impact on its economy compared with other European countries. The country experienced softer preventative restrictions against COVID-19 earlier in the year and a strong recovery in the third quarter contained the GDP contraction to 2.8% in 2020[38].

While Sweden is a country with low inequality (0.29 Gini coefficient value) and unemployment, the COVID-19 crisis has exacerbated difficulties for some and risks scarring youth working prospects. With only a few individuals lacking access to the internet and high information and communication technology adoption in the country, the government was able to implement measures that could help reduce the digital divide.

Sweden's BankID programme has unlocked a few benefits and opportunities within the economy. These include an increased customer base for the banking sector; a streamlined administrative process, saving people time and money; and reduced service channel costs for banks. Other benefits include ease of adoption and financial inclusion.

SWEDEN'S ECONOMY - 2020

Real economic growth rate: **-2.8%**

3/180 Corruption perception index score

2.1% Consumer price inflation rate

10.40 million Total population size

9.8% Unemployment rate

29.2 Income Gini (Gini-Coefficient)

Largest sectors in Sweden (as a % of GVA)

Manufacturing	Other services	Human health	Trade
15%	14%	11%	10%

Global competitiveness

70.3/100 Public institutions & governance ranking

70.7/100 Competition & anti-trust frameworks ranking

89.7/100 ICT adoption ranking

Digital inclusion

92.1% Internet users (% of adult population)

US$1.45 Average cost of 1GB data

99.7% Percentage of banked population

38 https://www.nordeatrade.com/dk/explore-new-market/sweden/economical-context

EVOLUTION OF SWEDEN'S ID SYSTEM

Sweden recognises BankID as a legal form of identification. In 2001, European Union (EU) law changed to recognise an electronic signature as equal to a physical signature. The Swedish government quickly followed suit; BankID, based on the Swedish personal identity number registered in the national population register, was first issued in 2003.

In 2005, BankID became available on debit and credit cards issued by the Swedish banks. A growth in self-service offerings from governmental institutions and private companies was recorded, with about 500 000 users by 2006. This number has significantly grown to eight million users in 2018.[39]

EVOLUTION OF SWEDEN'S BANKID

BankID is a personal and easy way to secure electronic identification and sign onto the Internet[40].

Individuals with a Swedish national identification number can obtain the Swedish BankID through their bank[41]. BankID has the same value across all banks as it is used the same way, irrespective of the bank that initially issued it. In addition, BankID is typically issued to persons over 18 years, although many banks allow persons under 18 years to get BankID.[42]

BankID was first issued in 2003, when it was available only as a certificate issued by the banks. Despite some reluctance from banks, BankID soon became popular. In 2005 it became available on card, embedded in the debit or credit cards issued by the Swedish banks.

In 2011, BankID introduced a software-based app solution enabling anyone with a smartphone and a BankID to use "Mobile BankID" independently of both their phone and SIM-card provider. From 2013 onwards, BankID's use rapidly increased, with especially Mobile BankID quickly outrunning the other solutions.

The objective of BankID in Sweden was to enable digital authentication and signature with limited data sharing, for use by public- and private-sector institutions through smart cards or digital devices (mobile or computer).

39 Signicat. (n.d.). Federated e-IDs as a value driver in the banking sector based on experience from Nordic Market. An Arkwright report.
40 https://developer.signicat.com/enterprise/identity-methods/swedish-bankid.html#authentication
41 https://developer.signicat.com/enterprise/identity-methods/swedish-bankid.html#authentication
42 https://developer.signicat.com/enterprise/identity-methods/swedish-bankid.html#authentication

THE EVOLUTION OF SWEDEN'S IDENTITY SYSTEM

1999
The Swedish e-ID has relied on e-IDs issued by the private sector since 1999

2001
A consortium involving the major Swedish banks was formed with the purpose to develop a general e-ID usable for all kinds of e-services

2003
The first BankID was issued

2004
The second framework contract procurement process was established in 2004 to increase availability of e-IDs and increase use

2005
In November, the e-IDs became available on cards (earlier versions were only available as files downloadable to the users' computers)

2006
More and more self-service services came from private companies as well as municipalities and county councils

2007
Transactions linked to internet banking or insurance have substantially increased which has consequently increased the Government's dependence on banks

2008
The design of the next major carrier of BankID - BankID for mobile phones is underway

2009
BankID is by far the most widely used e-ID with a reported 1.5 million users in early 2009, and 2 million in November - it is provided by nine banks

2010
On April 14, 2010 BankID in mobile is launched

2011
Mobile BankID is used as a security method, rapidly climbing in popularity and just a year later all connected banks issue Mobile BankID

2014
In order to increase the number of e-ID service providers within the federation, the e-ID Board opened service concession in early March 2014

2015
The billion barrier was broken, with more than one billion transactions made with BankID

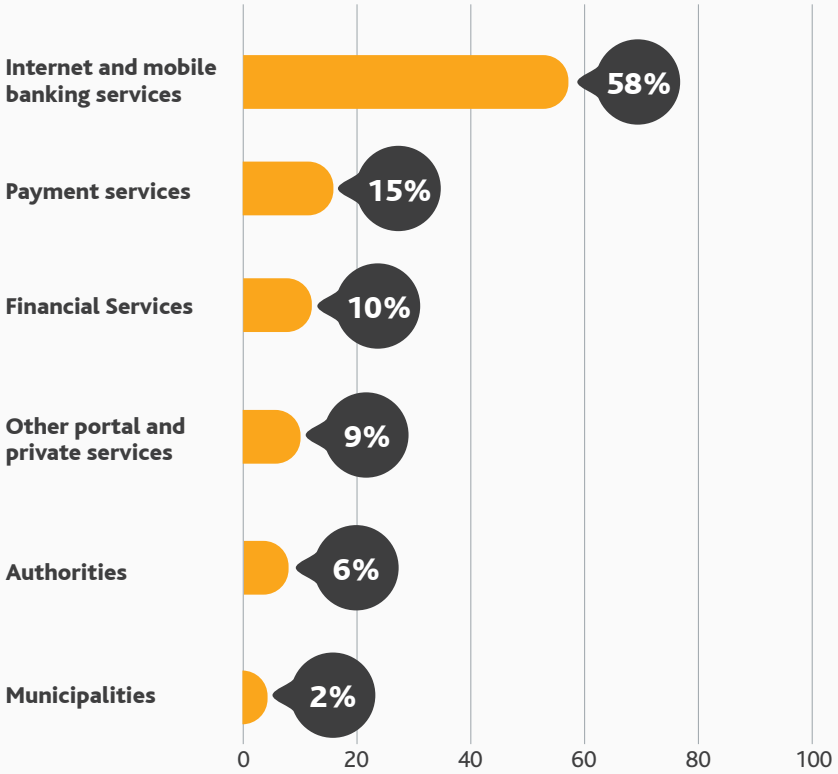
2019
The BankID was averaging four billion identifications and signings by eight million users yearly in Sweden

Today
Most internet and mobile banks, financial companies and payment solutions as well as state and municipal e-services are users of BankID and today we have 8 million users

IDENTIFYING A USE CASE: BANKID

BankID, a private-led partnership with the government, is recognised by the Swedish government as a legal form of identification that uses the identities established through banks.[43] Both government authorities and individuals use the digital BankID application for multiple public and private services, as shown in the diagram below.

Figure 1: Percentage split of Sweden's BankID use cases



Source: Signicat and Arkwright (n.d.), Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets

BankID is used by 80% of the population (almost 100% for people between 21 and 60 years old).

CHALLENGES BEFORE THE INTRODUCTION OF BANKID

Identifying the country's entire population and issuing citizens with e-IDs was both time-consuming and expensive. This was due to the long administrative processes and turnaround times for the government, citizens and businesses in accessing and/or providing various services.

BENEFITS TO SWEDEN AFTER THE INTRODUCTION OF BANKID

BankID has made it easier for users to use various banking services conveniently efficiently and securely, which has in turn benefitted the Government, the banks and the economy.

> BankID is a personal and easy way to secure electronic identification and sign onto the Internet.

43 http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Some of the major benefits for the three main parties involved in this ecosystem are:

Citizens:	• The use of the BankID services has provided benefits to Swedish citizens, as they are able to efficiently and securely complete application processes from their mobile devices.
Government:	• The collaboration by different players contributed to the success of the BankID system. This is because banks have the initial infra structure and customer base, and they are the only players who have already authenticated the majority of a country's citizens and transferred them to an online solution – online banking. This has saved government time and money that could be spent in investing in new infrastructure and in ensuring user adoption since users are hesitant to have government access and/or share their personal data online.
Economy:	• The commercial benefits associated with this application for banks is an increased customer base. In addition, the processing of applications in a paperless form results in an efficient administrative process, which can save users and the bank administrators both time and money.

KEY LEARNINGS FROM SWEDEN FOR SOUTH AFRICA

The digitisation of Sweden's banking sector has accelerated since the introduction of BankID, with an adoption rate of about 78% in 2018. The successful implementation of BankID was dependent on some of the key aspects highlighted below.

- **Collaboration among key stakeholders:** Sweden's BankID was a partnership model based on collaboration among various strategic partners, including the government. This enabled digitalisation and successful implementation in the banking sector.
- **Infrastructure investment and cost sharing:** Infrastructure investments, operational costs as well as research and development, previously covered by each bank independently, could now be split with other banks and the government.
- **Improved customer experience through provision of new services:** BankID enabled smaller banks unable to offer e-signature to provide new services to their customers. Banks were more user-friendly after removing the necessity for several e-credentials.
- **Fear of being left behind:** As more and more banks migrated to BankID and became part of the consortium, those who were not part of BankID joined the trend.
- **Enhanced security features and trust:** The successful collaboration between the banks to form an e-ID system has allowed them to establish trust among each other and customers.
- **Convenience:** The mobile BankID can be downloaded on multiple devices, especially in instances where users get a new mobile device and/or may need to block a BankID.[44]
- **Compliance with laws and regulations:** Government and the providers of the digital identity products/services ensure that the necessary laws and regulations are complied with, especially from a privacy and security perspective, to build user trust.

44 https://www.bankid.com/en/privat/om-bankid

KEY GUIDING QUESTIONS TO ASSESS THE SUCCESSFUL IMPLEMENTATION OF BANKID

Sweden's federated model allowed for various stakeholders to play a key role in ensuring the successful implementation of BankID. The government's involvement from an oversight perspective and the various banks' ability to provide excellent secure infrastructure as well as innovative services have resulted in an increasing adoption rate since inception.

1

What digital identity ecosystem model was adopted and why?

- An all-encompassing National Id was already present; there was a drive to create a digital identity derived from the National Id Collaboration amongst banks to create a digital identity in a federated model with trust framework from Central Authority.

2

Who are the stakeholders involved?

- **Identity Authority:** Finansiell ID-Teknik BID AB.
- **Issuer/ID Provider:** 10 Major Banks.
- **Identity Operator:** Private Operators (like Signicat).
- **Relying Parties:** Tax Dept.(Skatteverket), e-comm firms etc.
- **Enablers:** Signicat, Private Providers.

3

What was government's involvement in the digital identity programme?

- Government plays a central role in defining and regulating the identity framework and endorsing providers. BankID is used not only for payments but also for online contact with public authorities such as the Tax Agency, the public healthcare system, and the municipal school system.

4

What technology was used in the development of digital identity?

- Federated digital ID architecture with SSO schemes that allow a user to access multiple separate services by identifying information established in one security domain. The release of the state-of-the art technology, Mobile BankID, drove transaction rates to several billion a year as the solution can be accessed at any time and from any place.

5

How long did it take for successful adoption of digital identity?

- It started in 2001, when the EU law changed to recognise an electronical signature as equal to a physical signature. From 2013 onwards, BankID's use rapidly increased, with especically Mobile BankID quickly outrunning the other solutions. BankID reached 1.5 billion transactions in 2016, and grew to 2.5 billion in 2017. In 2018, the 8 million users' threshold was achieved.

6

What regulatory and policy frameworks were adopted?

- A consortium between Swedish's major banks was formed in 2001 and a second framework contract procurement was established in 2004.

7

What are the accelerators that enabled adoption of the digital identity?

- The bank's collaboration in terms of developing the BankID solution has given them an ad vantage over governmental and third-party solutions as they are the only players who have authenticated the majority of their citizens and transferred them to an online solution (i.e. online banking). Also, the digitisation of the banking sector is accelerating and has resulted in an increase in e-banking customers and in turn, trust in high-security e-banking systems.


Personal Data
Name
Home Address
Business Address
Identity Card No
Passport No
Driving License
Income Tax No
Car Registration
Other
[Identify Person]
Confidential Data

SOUTH AFRICA IS AN UPPER-MIDDLE-INCOME, EMERGING MARKET ECONOMY

South Africa is the continent's third-largest economy, after Nigeria and Egypt.[45] South Africa's economy is the most industrialised on the continent and is a gateway for businesses into the rest of Africa, thereby functioning as a hub for diverse mining and other activities, services and associated consumables.

SOUTH AFRICA'S SOCIO-ECONOMIC LANDSCAPE

South Africa is an upper-middle-income,[46] emerging market economy with an abundant supply of natural resources. Real GDP growth has been weak over the last several years, averaging just 0.7% over the period 2016–2019. This slowdown, according to the International Monetary Fund (IMF), was due to stalled implementation of structural reforms, inefficiencies in public enterprises, weaker sovereign ratings, increasing domestic political uncertainty, lower commodity prices and drought conditions.[47]

The global COVID-19 pandemic saw South Africa implement a country-wide lockdown at midnight on 26 March 2020, with a phased return-to-work approach starting from 1 May. The lockdown measures, both in South Africa and worldwide, have caused major disruptions along all supply and demand chains in the economy, severely impacting economic growth. This trend of low economic growth continued throughout 2020, with the economy contracting by about 7%.[48]

Due to the country's slow rate of economic growth over the past years, job creation has failed to keep pace with population growth, with unemployment increasing by 0.1% from the previous quarter to 32.6% (Q1:2021).[49] The COVID-19 pandemic has had negative impacts on various sectors, which has in turn affected South African households, which are highly dependent on salaries as their main source of income (54.8%, 2019 General Household Survey).

The COVID-19 lockdown has forced South Africans to use digital platforms more than before. This has led to an increased need for digitalisation and the roll-out of a digital identity system, due to individuals' need to do more online rather than face-to-face transactions.

The potential economic value and benefits of the introduction of a digital identity could see it unlock opportunities within the economy. In addition, it could increase access to financial services as well as to employment opportunities while increasing productivity.

From a social perspective, South Africa's socio-economic profile is characterised by high levels of poverty and unemployment as well as unequal access to services such as healthcare, education, water and electricity. Although South Africa has sought to address poverty and inequality with a wide range of initiatives that include the use of fiscal policy to support redistributive measures, it remains a dual economy with one of the highest and most persistent inequality rates in the world, with a consumption expenditure Gini coefficient of 0.63.

The introduction of a digital identity has the potential to open new opportunities for the unemployed, vulnerable and/or elderly. A digital identity would assist them to verify a secure identity and include them in the economy, which in turn would give them easier access to, for instance, employment, social benefits and government services.

SOUTH AFRICA'S ECONOMY - 2020

Real economic growth rate: 4,6%

69/180 Corruption perception index

5.2% Consumer price inflation rate

59.6 million Total population size

32.6% Unemployment rate

63.0 Income Gini (Gini-Coefficient)

Largest sectors in South Africa (as a % of GVA)

Finance & real estate	Public admin, edu. & health	Trade, accomm. & food	Manufacturing
21%	17%	16%	14%

Global competitiveness

53.9/100 Public institutions & governance ranking

58.3/100 Competition & anti-trust frameworks ranking

49.7/100 ICT adoption ranking

Digital inclusion

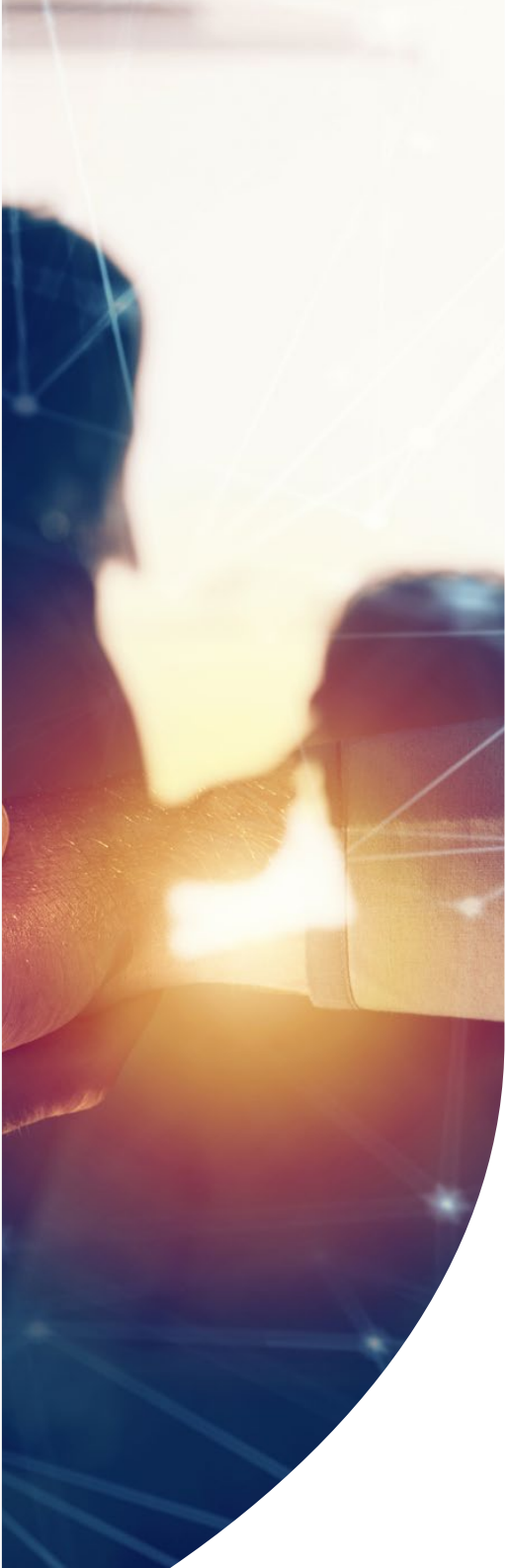
56.2% Internet users (% of adult population)

R39.47 Average cost of 1GB data

69.22% Percentage of banked population

Sources: Fitch Solutions, WEF, Statistics South Africa, Transparency International, World Bank

45 World Population Review. (2021). Richest African Countries.
46 World Bank, 2020. Doing business. https://www.doingbusiness.org/en/data/exploreeconomies/south-africa
47 PwC, 2018. Investment decisions: Why South Africa, and why now? https://www.pwc.co.za/en/assets/pdf/investment-decision-why-sa.pdf
48 Fitch Solutions, 2021.
49 Statistics South Africa. (2021). Quarterly Labour Force Survey, first quarter 2021.



EVOLUTION OF SOUTH AFRICA'S ID SYSTEM

Different approaches have been employed to develop South African national identities.

Post-apartheid, the green bar-coded ID book was introduced and issued to all South Africans. Having a common form of official identity and citizenship was a key part of building a new national identity.[50] During this period, the DHA's goal was to build a national system connecting the offices of the DHA to the National Population Register (NPR).

The 2007–09 turnaround programme saw a significant investment in governance (management and processes), systems, service culture, security and training. The strategic objective of this programme was to update the DHA's operating model and revise its operating profile to provide citizens with predictable and acceptable turnaround times for identity documents and passports and to restore confidence in the department.[51]

In 2011, an agreement was signed with the banking sector that allowed them to improve security, reduce fraud and speed up services by checking the identity of their clients using fingerprint scanners that interface with the DHA's live verification system. The DHA later connected many other institutions, both public (e.g., Department of Labour and Post Office) and private, to their live verification system.[52]

THE EVOLUTION OF SOUTH AFRICA'S IDENTITY SYSTEM

1950
Population Registration Act of 1950

1953
The Bewysburo (Bureau of Proof) starts process of issuing books

1960
The Bureau of Proof becomes one of the first South African government agencies to deploy electronic computers

1966
10 million sets of fingerprints captured, making it the second - largest collection in the world

1977
The Bureau of Proof and the CSIR investigate computerising the search and classification of fingerprints

1980
The National population register is designed. Issues around inconsistent or missing data abound

1984
The Bureau of Proof along with its population registry are transferred into the Department of Home Affairs (DHA)

1986
Separate population registers were merged into a single "integrated" database. Green bar code ID issued

2013
The DHA begins issuance of the National Smart ID card to South African citizens

2018
SABRIC and the DHA collaborated to enable the verification of customers' identities by matching their fingerprints directly against the DHA's biometric HANIS database

50 Department of Home Affairs. (2019). White Paper.
51 Department of Home Affairs. (2019). White Paper.
52 Department of Home Affairs. (2019). White Paper.

In 2012, the DHA initiated a modernisation programme aimed at transforming its delivery systems to achieve strategic objectives such as inclusion, national security and improved service delivery.[53] Some of the elements that are being rolled out as part of this programme are the smart ID card, fully digital ID and passport processes, online capturing of biometrics at ports of entry and upgrades to the movement control and biometric systems.[54]

The DHA has formed key partnerships to improve access by creating new channels for citizens to have better access to their services. An agreement with the major banks has allowed their clients at 14 pilot branches to access a DHA service point.[55] In addition, the DHA has partnered with a visa facilitation service that led to the creation of service points in many countries abroad and in major South African cities. In this case, applications are sent digitally to the DHA, where adjudicators complete the process.[56] Together with local development agencies, the DHA has extended the service to create one-stop centres for local businesses in partnership with government development agencies.

At present, the Smart ID card, issued in 2013, is on par with identity systems in Europe, Asia and America as it comes with security features that can help prevent identity theft and fraud.

APPROACH TO IDENTIFYING SOUTH AFRICAN FOCUS AREAS, USE CASES AND THE DIGITAL IDENTITY JOURNEY THROUGH A CONSULTATIVE PROCESS

To plan the way forward, we took a consultative process which involved a survey, interviews and focus group discussions to understand what is required to successfully implement a digital identity programme.

The first step was to understand the key considerations for a digital identity programme. This involved analysing successful programmes around the world and identifying learnings for South Africa. Consultations with the community were also done through a survey and interviews.

The next step was to facilitate focus group discussions, which served as knowledge-sharing and alignment sessions. In these sessions, participants explored several design topics, and the outputs were documented and shared with the community.

The community constituted both public and private entities across different sectors. A snapshot of the major participants is presented below:

PASA	SABRIC	Secure Citizen	BASA
SARB	Investec	SAFPS	SSI Consortium
FSCA	Old Mutual	PBSA	SABRIC
FIC	Signiflow	ABSA	Consumer Profile Bureau
Direct Transact	Astute	One Vault	National Treasury
Capitec	Bidvest	Government technical advisory centre	Standard Bank
FNB			

> The introduction of a digital identity has the potential to open new opportunities for the unemployed, vulnerable and/or elderly.

53 Department of Home Affairs. (2020). White Paper.
54 Department of Home Affairs. (2020). White Paper.
55 Department of Home Affairs. (2020). White Paper.
56 Department of Home Affairs. (2020). White Paper.

As part of the ongoing analysis, we identified the challenges associated with digital identity implementation that are generally experienced by low- and middle-income countries.[57][58]

Weak civil registration systems

Lower literacy levels

Poor procurement processes

Limited connectivity infrastructure

Low government capacity/trust

Insufficient national cybersecurity capacity

Accessibility and inclusion

Interoperability

Data sharing, user consent and control

Data protection, privacy and security

Cybercrime and cybersecurity

Identity authority & governance structure

Some of the challenges identified in the South African context align to the overall global challenges, especially with regard to data privacy and security, standardised rules and the trust framework, and governance and regulation. In addition, community members identified challenges unique to South Africa in the focus group discussions.

- **Internet access:** Many South Africans still have limited access to online services. There are also concerns around the affordability of data as well as ICT infrastructure in some townships and rural areas.
- **Data privacy and security:** There is some user concern around the protection of their personal data and the handling of the data by private companies and especially government.
- **Fraud:** Fraudulent activities such as identity fraud and credit cloning are still prevalent in South Africa.
- **Standardised rules and the trust framework:** Many citizens still lack trust in the online system and are uncomfortable with sharing personal information on online platforms due to fraud. This is because they do not trust the government to have the capacity and ability to protect their personal information.
- **Government regulations:** The country's regulatory development around data security and privacy has been weak, which may impact the trust framework.
- **Digital literacy:** Many South African are still digitally illiterate; the adoption of a cashless and internet-driven environment would be challenging for them.

Over and above these challenges, a further twelve focus areas were recognised: government administration, financial services, telecommunications, immigration, social protection, education, healthcare, transport-related industries, mining, sport, retail and SMMEs.

57 World Bank Group. (2019). Identification for Development: Practitioner's Guide version, 1.0.
58 Department of Home Affairs. (2020). White Paper.

To shortlist the focus areas, we worked with the community using parameters such as inclusion, reach of users, ease of implementation and existing infrastructure. The shortlisted focus areas were financial services, healthcare, social protection and government services. Their significance to the South African environment is highlighted in the table below.

Focus area	Role in enabling digital identity	Benefits of digital identity
Financial Services	Financial institutions facilitate the allocation of about R15 trillion + of assets; therefore, they play the role of a trusted advisor.	• Compliance with local regulations • Improve risk management for insurance and credit products • Improved individual customer experience • Enhanced administrative efficiency and productivity
Healthcare	With 84% of the population being dependent on the public healthcare sector, the sector can play a key role in collecting and storing data of the unbanked and vulnerable population.	• Enable sharing of medical records • Improve the collection, storage and protection of personal data • Accessibility of personal health information can improve the quality of care
Social Protection	At the end of 2020, the unemployment rate sat at 32.5% with about 31% of the population relying on social grants due to COVID-19-related grants and economic decline.	• Digital identity can prevent, manage, and overcome situations that adversely affect people's well-being, e.g., administration of social grants • Eliminate human error
Government Administration	The Department of Public Service and Administration has a budget allocation for 2020/21 of R566 bn. Administration currently accounts for the largest portion (45%) of the budget. This is because it acts as a supportive function housing many units, human resources, finance and general audit etc.	• Improve government efficiency by providing citizens with the option of voting digitally • Empower citizens, build trust and awareness • Improve citizens' daily lives by enabling a more connected society • Enhanced customer experience

Based on the key challenges and focus areas for South Africa's digital identity programme, we determined the most relevant use cases along with their priority.

DIGITAL IDENTITY: A USER JOURNEY CONSIDERING SOUTH AFRICA'S DEMOGRAPHICS

Each focus area plays a key role in the South African environment and can effectively enable the successful implementation of a digital identity programme in the country. In showing the significance of each focus area, we developed potential use cases applicable to the South African context. In addition, we developed four personas to provide a realistic representation of the potential users of South Africa's digital identity programme and the benefits of this programme to the users thereof.

The development of the personas helped us to understand the application of a digital identity in the South African environment while enabling the practical application of the concept to South Africa, making it fit for the digital identity story.

The persona journey highlights three key aspects for each individual: the persona's background, the current process before digital identity, and the process once digital identity is introduced, as well as the relevant benefits.

We outline two personas' backgrounds which resonate with those of a typical South African. Persona identification is important because it shows our understanding of the user's needs, experiences, behaviours and goals. Different users have different needs and expectations; it is critical to recognise this to develop a product/service that is fit for purpose.

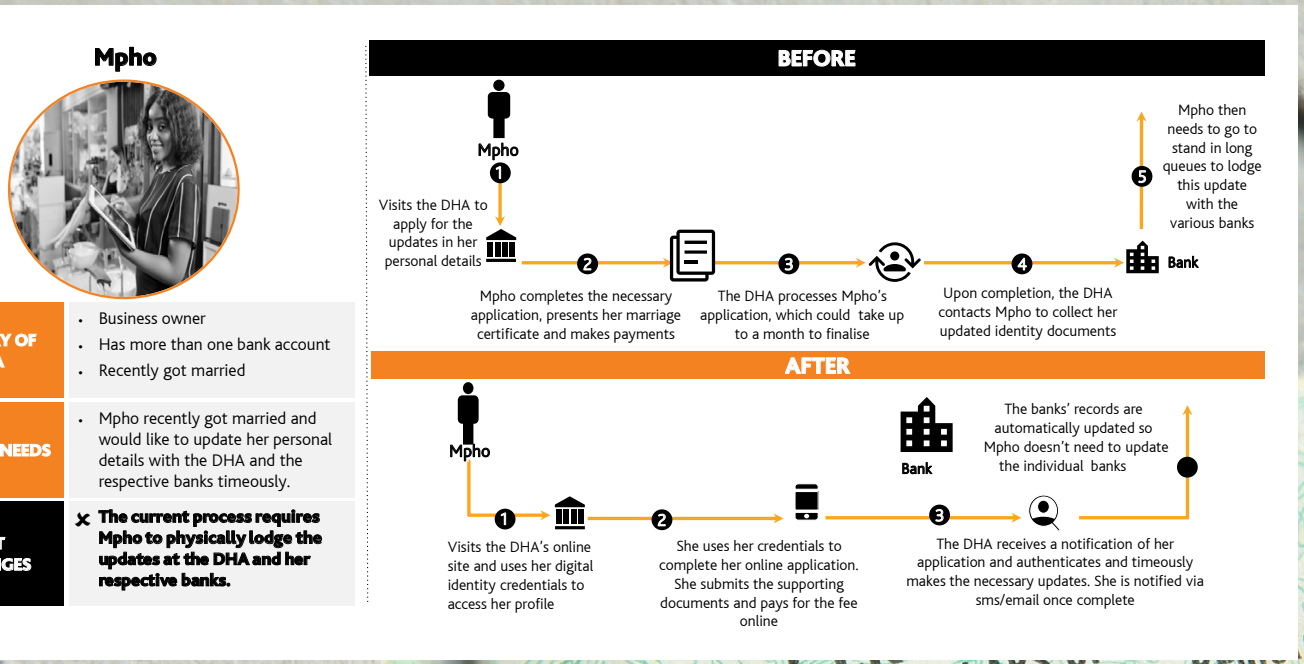
	Mpho	Lerato
		
SUMMARY OF PERSONA	• Business owner. • Has more than one bank account. • Recently got married.	• Single mother. • Dependent on social welfare. • Not digitally literate.
SPECIFIC NEEDS	• Mpho would like to update her personal details with the DHA and the respective banks simultaneously.	• Lerato just turned 60 years old and she would like to apply for her SASSA grant conveniently.
CURRENT CHALLENGES	✖ The current process requires Mpho to **physically** lodge the **updates at the DHA** and her **respective banks.**	✖ Lerato needs to **physically** go to the SASSA offices to kick-start her application process and can **expect feedback in 3 months.**
THE NEED FOR DIGITAL IDENTITY	• Convenience. • Streamlined administration. • Cross-application.	• Streamlined administration. • Convenience.

We looked at the common challenges experienced by a typical user of a product/service under each focus area, which helped us identify a use case that can benefit the users through the implementation of the digital identity programme. In the following section, we provide an analysis of how digital identity can benefit South Africa based on each user journey.

FINANCIAL SERVICES: MPHO'S DIGITAL IDENTITY JOURNEY

Mpho is an entrepreneur who owns cleaning and logistics services businesses. She has two bank accounts for different services within her businesses and prefers transacting via her online banking app. She recently got married and would like to update her personal details with the DHA and the respective banks. She is faced with administrative inefficiencies, long queues and long turnaround times to process this update.

Digital identity can benefit users of financial services by saving them time and money spent on tedious administration and paperwork. The provision of online services has the potential to increase the banking sector's customer base, drive efficiency, lead to cost savings and increase profitability. As seen in the Sweden BankID programme, the introduction of mobile banking services and allowing users to sign contracts/documents digitally increased the adoption rate.



BusinessTech. (2021). How many South Africans now rely on social grants: 1996 vs 2020. Retrieved from https://businesstech.co.za/news/government/459186/how-many-south-africans-now-rely-on-social-grants-1996-vs-2020/

SOCIAL PROTECTION: LERATO'S DIGITAL IDENTITY JOURNEY

South Africa introduced social grants for the purpose of improving citizens' standard of living and redistributing wealth to create a more equitable society. Since inception, the percentage of the population dependent on government's social grants has increased from 7% in 1996/97 to 31% in 2019/20.[59]

However, the key challenge for most of those dependent on this social relief programme is the process it takes to access the funds. These individuals are required to stand in long queues, complete paper-based application forms and wait as long as three months before accessing these funds.

Lerato is a single mother who is highly dependent on subsistence farming activities and social grant payments for her three kids to help her feed her family. She has recently turned 60 years old, qualifying her for the South African Social Security's (SASSA) older person's grant. Given her socio-economic status, Lerato has experienced some social, economic and financial challenges accessing various services that could improve her standard of living.

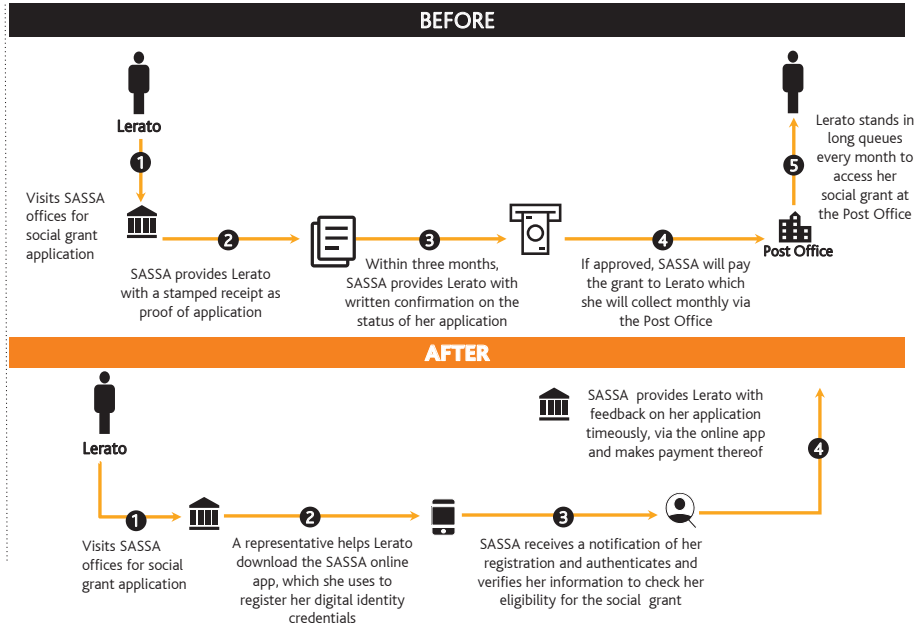
In terms of social protection services, digital identity can improve SASSA's ability to administer social relief payments to unbanked individuals who face challenges applying for and receiving payments. As noted in India's Aadhaar programme, the implementation of a digital identity programme can help streamline the administrative processes and facilitate payments.

In summary, citizens face the challenge of much paperwork, lengthy time-consuming processes and long wait times before receiving any form of feedback when accessing services. As a result, countries have implemented digital identity to address some of these challenges and improve access.

59 BusinessTech. (2021). How many South Africans now rely on social grants: 1996 vs 2020. Retrieved from https://businesstech.co.za/news/government/459186/how-many-south-africans-now-rely-on-social-grants-1996-vs-2020/

Lerato

SUMMARY OF PERSONA	• Single mother • Dependent on social welfare • Not digitally literate
SPECIFIC NEEDS	• Lerato just turned 60 years old and she would like to apply for her SASSA grant conveniently.
CURRENT CHALLENGES	✕ **Lerato needs to physically go to the SASSA offices to kick-start her application process and can expect feedback in 3 months.**



Overall, collaboration between various stakeholders across the public and private sectors is required for digital identity implementation to be a success. Areas of collaboration range from infrastructure investment to standard setting and regulatory oversight, necessary for establishing a trust framework. It is important to ensure that the services are inclusive and convenient to the user to improve adoption and use.

POTENTIAL BENEFITS OF DIGITAL IDENTITY TO SOUTH AFRICA

In the table below, we outline the potential benefits for the citizens, government and economy:

Citizens:	• Simpler, more convenient FICA process that will save time. • Improved quality of service provision, reduced fraud and a better user experience.
Government:	• Reduced government expenditure due to improved administrative processes across its departments. • In addition, increased tax revenue collection and a boost to digital eCom, SME, financial services and health.
Economy:	• The commercial benefits associated with this application for banks is an increased customer base. • In addition, the processing of applications in a paperless form results in an efficient administrative process, which can save users and the service providers both time and money. • Integrated services across G2P and G2B as well as an increased transparency and accountability.

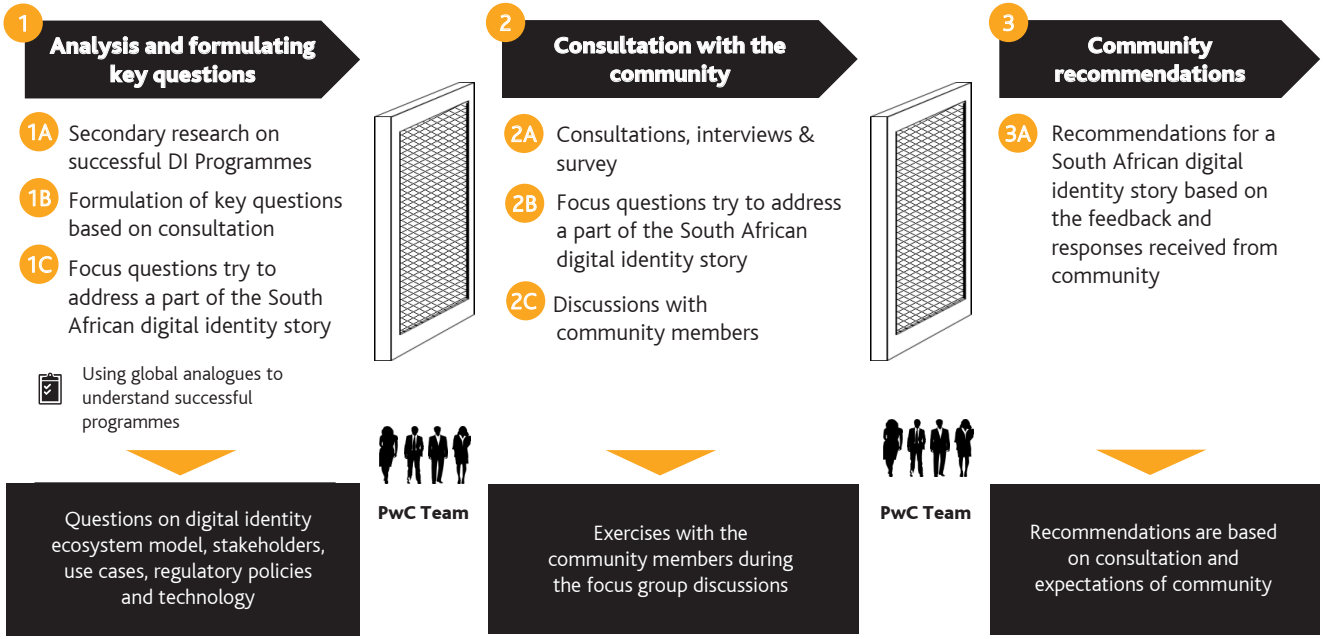
JOURNEY TOWARDS A SOUTH AFRICAN DIGITAL IDENTITY

> Some of the challenges identified in the South African context align to the overall global challenges, especially regarding data privacy and security, standardised rules and the trust framework, and governance and regulation.

JOURNEY TOWARDS A SOUTH AFRICAN DIGITAL IDENTITY

In the sections above, we examined the need and opportunities for digital identity in South Africa, explored some key learnings from global analogues, unpacked the potential risks and identified the critical success factors that could potentially mitigate those risks and ensure the successful implementation of a digital identity programme.

Through the consultations and outcomes, some key questions were also identified to develop the South African digital identity story. The answers to these questions make up the strategic recommendations and key considerations for the digital identity story.



> The mobile access penetration of South Africa was about 95% in 2018, which makes it easy for people to onboard a mobile friendly ecosystem.

To ensure the robustness of this story, there was extensive consultation with the community. Some of the considerations for the stakeholders can be summarised as follows:

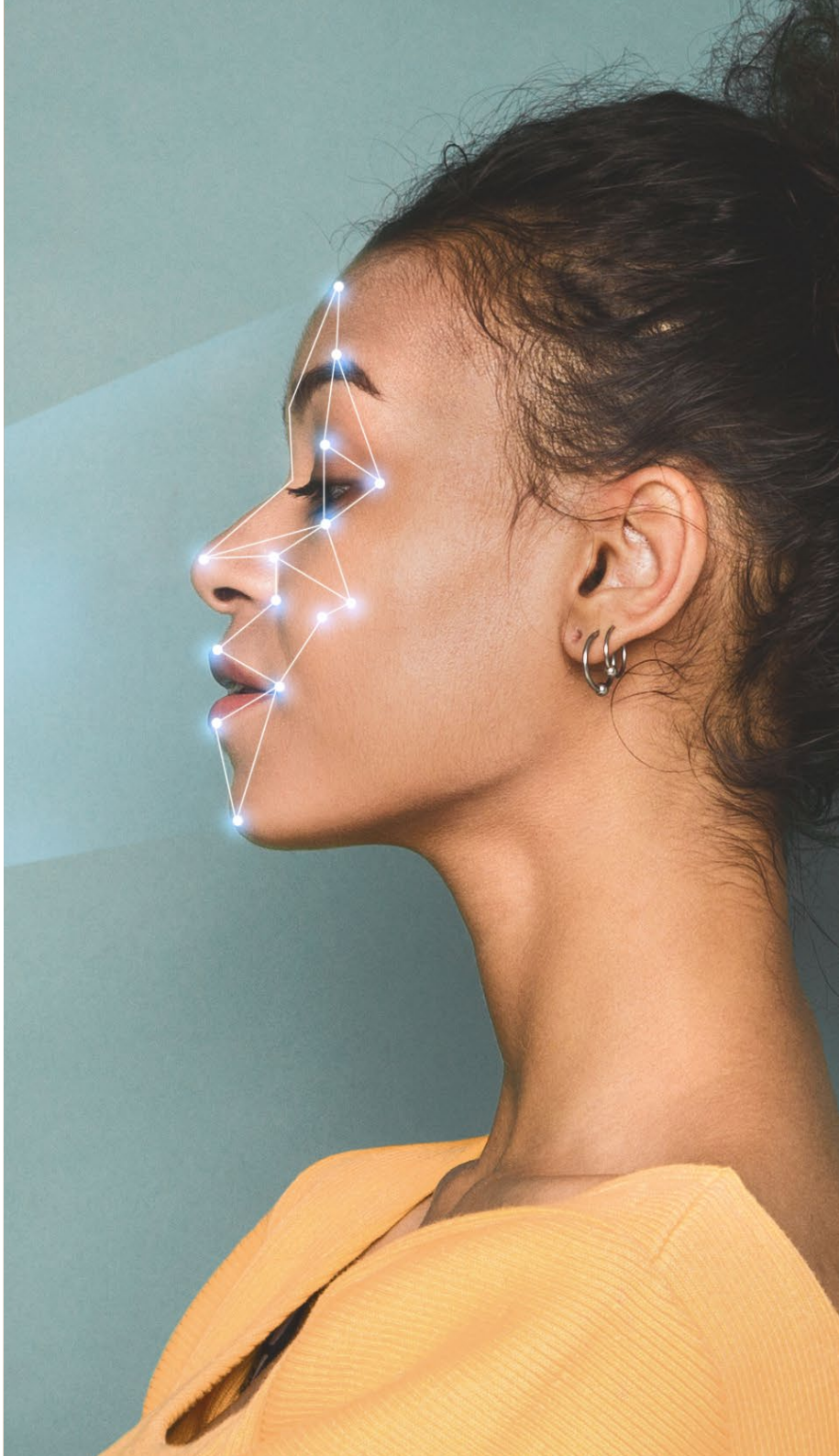
- The inputs were drawn from a consultative process, and are collective inputs based on discussions with and ideas shared by the community members.
- The recommendations are based on the global analogues and community outcomes to create a common narrative. More work and collaboration are required to further unpack and implement these recommendations.

KEY QUESTIONS FOR THE SOUTH AFRICAN DIGITAL IDENTITY STORY

We have identified some key questions to guide the South African digital identity story.

Topic	Guiding question
Digital identity ecosystem model	What should be the proposed digital identity ecosystem model for South Africa?
Stakeholders and roles	Who should be the key stakeholders in the South African digital identity ecosystem and what will be their respective roles?
Key use cases	What should the key use cases be for a South African digital identity?
Regulatory policy changes	What needs to change in the regulatory landscape to support the setup of a digital identity ecosystem?
Technology framework	What should be the overall technology framework considerations for the South African digital identity ecosystem ?

The following sections explore these questions and provide rationales for the recommendations.



Guiding question 1: What should be the proposed digital identity ecosystem model for South Africa?

We identified key parameters to analyse the three ecosystem models which provided the basis for recommending an appropriate model for South Africa. The ecosystem models were evaluated based on the following parameters that are relevant for the South African market:

- **Ease of onboarding**, which is the process of integrating a new user into the digital identity ecosystem. The mobile access penetration of South Africa was about 95% in 2018, which makes it easy for people to onboard a mobile friendly ecosystem. The literacy rate of South Africa was about 87%[60] in February 2020, which makes it easier to educate and inform people of the onboarding process.

- **Ease of adoption**, which refers to the process of users familiarising themselves with the digital identity by making it their own. With about 16.6% of the South African population living below the poverty line as of 2020 and a substantial proportion living in remote areas, many face barriers to adoption like the cost of a smartphone or internet access (56.3% as of 2020). These barriers will need to be addressed by the ecosystem model so that a higher adoption rate can be achieved.

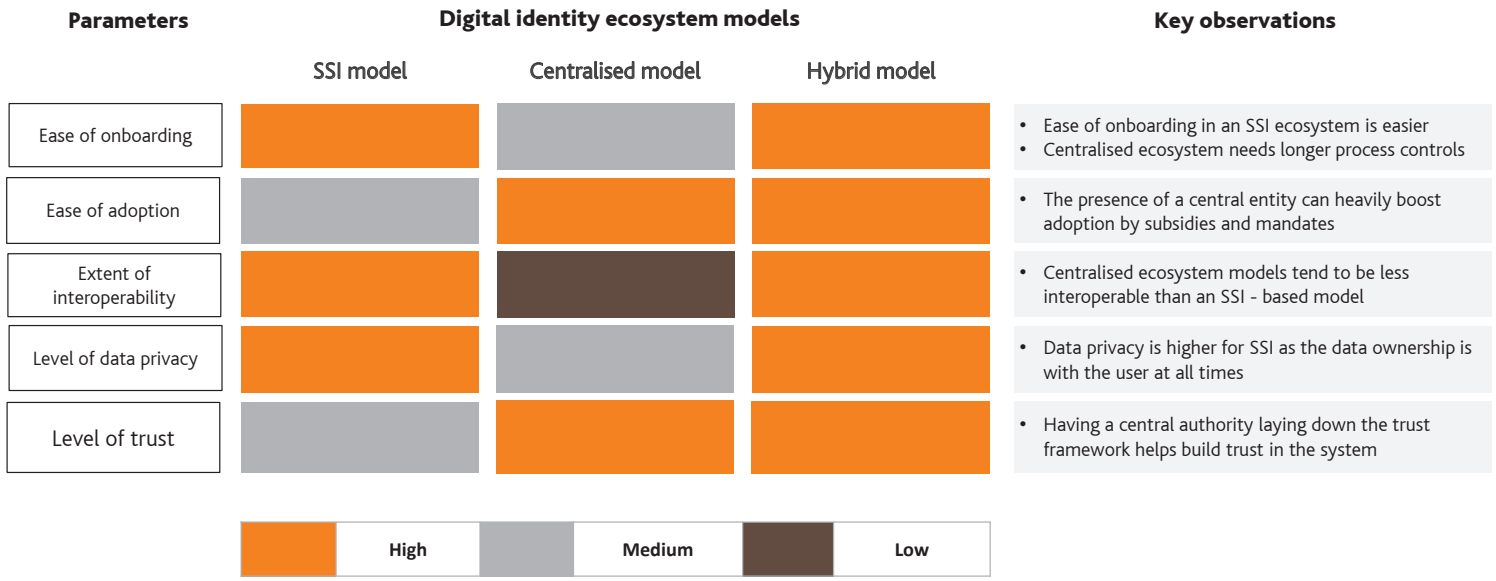
- **Extent of interoperability** relates to the ability of various digital identity systems to readily connect and exchange information with one another. The interconnectedness of the South African economy makes interoperability critical. It should also be compliant with global standards to be compatible and interoperable across geographies and within organisations for accessing multiple services. According to the DHA, the South African identity system does not have standards-based technical interoperability; therefore, it does not allow different components and devices to communicate with each other and work together.[61]

- **Level of data privacy** defines how private and secure one's personal data is from undesired access or breach by an external party. The use of personal data should be secure, and ownership should be with the individual or a guardian. Data breaches across services and industries must be addressed by digital identity as that will be important for the global adoption of such an identity. On 1 July 2021, the Protection of Personal Information Act (POPI) came into force in South Africa. The purpose of the Act is to protect personal information in order to strike a balance between the right to privacy and the need for the free flow of and access to information as well as to regulate how personal information is processed.[62]

- **Level of trust** refers to the extent to which the parties within the ecosystem can be trusted. The concept of a digital society cannot be conceived without a trust framework. The involvement of the banking and financial sectors makes it more important for people to trust the ecosystem. A centralised body governing such a trust framework can engender trust in the ecosystem by the public. In South Africa, the DHA is a single, dedicated entity for identity management; however, in its policy white paper, the DHA states that it is not well equipped with sufficient and capable human, financial and technological resources to efficiently carry out its mandate around identity management. Thus, private sector involvement is key in gaining user trust as they are already managing some of the citizen's personal information.

60 https://www.indexmundi.com/south_africa/literacy.html
61 Department of Home Affairs. (2020). White Paper.
62 Department of Home Affairs. (2020). White Paper.

An analysis that cuts across these parameters shows that a hybrid model would be the best fit for South Africa.



What are the key takeaways from the community?

Three ecosystem models were explored, and the following takeaways were gleaned from the exercises and discussions.

SSI ecosystem	Centralised ecosystem	Hybrid ecosystem
• Concerns include cross-industry vertical adoption with support from participants, and financial sustainability. • Existing infrastructure can be leveraged and administrative costs reduced by implementing holistic end-to-end use cases.	• May be suitable in the short term to address financial inclusion but may not address many digital identity requirements in the long run. • A central entity can help drive adoption and implement digital identity faster and it can help create mandates more easily, which would speed up the mandate process.	• A hybrid model could address the shortcomings of both ecosystems by making use of an SSI-based digital identity governed by a central authority. • The model based on SSI would improve onboarding while safeguarding data privacy, and an existing central trust authority would boost trust in the ecosystem.

- A hybrid model with the key features of both centralised and self sovereign identity would engender trust, and an SSI-based digital identity would ensure data privacy, faster access to services and interoperability.
- The existing national identity infrastructure could be leveraged as a foundational source to build a digital identity platform.
- A trust framework could be defined with a common set of principles, goals and policies to ensure trust within the ecosystem. The framework should promote interoperability and enable a better user experience.

Department of Home Affairs. (2020). White Paper.

Guiding question 2: Who should be the key stakeholders in the South African digital identity ecosystem and what will be their respective roles?

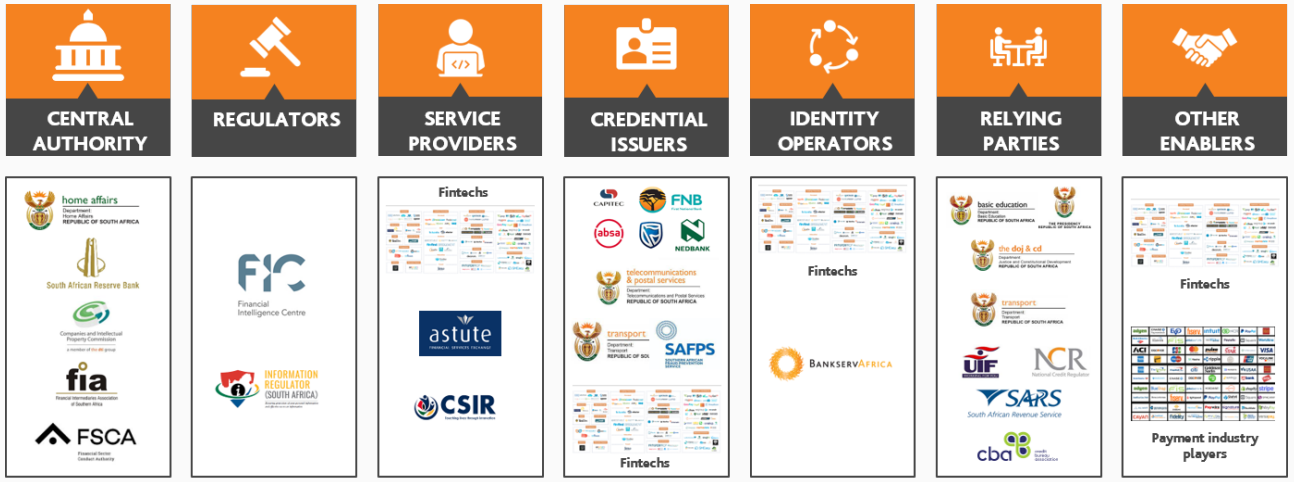
Within any identity ecosystem, several primary stakeholders play varying roles across the value chain. In general, individuals (citizens or clients) are the primary end-users in the system, while government bodies and private firms are the primary providers of digital identity credentials, authentication and other services. Other key stakeholders are public actors responsible for regulation, and actors responsible for setting standards and building trust.

A governance framework of the digital identity model is key in outlining the roles and responsibilities of each stakeholder in the digital identity ecosystem model. A good governance structure is one which consists of various stakeholders and is developed in a way that allows for proper information access and collaboration among these stakeholders to improve efficiency.

What are the key takeaways from the community?

As shown below, the key stakeholders/enablers in the digital identity ecosystem were identified. These stakeholders include government bodies, regulators, service providers, public entities and the private sector.

A summary of the main stakeholders and the potential role(s) they could play in the digital identity ecosystem is provided below:



The roles of each identified stakeholder group will be determined by the model adopted in South Africa. Currently, the DHA is a single dedicated entity for identity management in the country and the community is of the view that the DHA will remain the golden source of identity for South Africa. This will in turn help formulate the necessary governance structure fit for a South African digital identity ecosystem, guided by existing and new regulations.

Community recommendations

- Based on the type of ecosystem model, there will be multiple credential providers. Due to the strong distribution network and large customer base, banks, financial institutions, telecommunications and service providers could be the potential credential providers.
- Government entities will be key in enabling interoperability within the digital identity network.
- The network should be leveraging the existing identity infrastructure to support the development and implementation of different use cases.
- The scheme operator or administrator would be responsible for the overall governance of the system and defining an overarching trust framework.
- The identity platform will be managed and governed within the trust framework. Mostly, the technology service providers will be responsible for providing the ledger and the wallet platforms.
- FinTechs will play an important role in the expansion of the digital identity ecosystem, with the help of emerging technologies and security controls.

Guiding question 3: What should the key use cases be for a South African digital identity?

Due to the versatility of digital identity, there are many use cases to consider for South Africa. Based on the focus area and level of impact, some use cases were identified for further analysis.

What are the key takeaways from the community?

Based on the shortlisted focus areas, the following list of use cases for each focus area was identified:

Financial Services

- KYC
- Multi-model biometric authentication
- Person-to-person payments
- Proof of bank account, income, ID, address etc.
- Digital onboarding
- Debicheck authorisation
- Digital FOREX
- Digital signature/bank ID
- Payment authentication

Healthcare

- Vaccine passport
- Medical records
- Proof of medical aid
- Touchless medical information sharing
- Prevention of medical aid fraud
- Electronic scripts and notes

Social Protection

- Corporation for deposit insurance
- Access to education
- SASSA fraud prevention
- Parent/child digital protection
- Digital birth & death certificates
- Anonymous info (whistleblowing)
- Early childhood development (ECD)

Gov. Administration

- Title deeds
- Proof of life for social grants
- Biometric updating
- DHA ID
- Government ID number
- SARS tax fraud prevention
- Drivers license
- Verification of DHA info
- True unemployment rates
- IFWG
- Singpass/Corpass

Social grant use case was identified as having a major impact in South Africa. In addition, several challenges were identified which may affect the implementation of these use cases. These challenges include digital illiteracy; lack of an established regulatory and governance framework; lack of ICT infrastructure; high number of people who remain unbanked; and inequality. Thus, implementing digital identity in the current South African environment would still leave some citizens excluded and the benefits would only be experienced by those with access to the digital world.

Community recommendations

KYC, digital onboarding and digital signatures (BankID) were recommended as the use cases to explore further. The choice of these use cases is supported by the fact that it would save time and effort and in turn increase the adoption rate. Digital onboarding, for example, can decrease time-consuming paper-based manual processes, thereby increasing productivity and creating a more convenient experience for the user.

Guiding question 4: What needs to change in the regulatory landscape to support the setup of a digital identity ecosystem?

The DHA is the established legal institution within the South African government mandated to take charge of identity management. The DHA's core functions are a fundamental part of all human societies. Throughout history, managing identity and status has been essential for societies to organise work, distribute resources and ensure that people's rights and identities are protected.

However, current legislation and systems will need to be updated to support the digital identity ecosystem. These legislations will help address challenges such as the following:

- **Accessibility and barriers to inclusion:** The vulnerable face economic and social barriers to enrolling in or using the identity system.
- **Interoperability and integration of identity systems:** The data of a person is stored across multiple systems and captured differently.
- **Data protection for privacy:** Key legislation that regulates how the DHA manages personal data needs to be updated to align with the Constitution and the POPI Act. In addition, the information regulator is not suffiently functional to manage its legal obligations
- **Data security, data sharing and user consent:** The information regulator is not sufficiently functional to manage its legal obligations.

The identity management policy drafted by the DHA establishes the vision, goals and objectives, and approach of the DHA towards establishing a modern and secure NIS. The NIS is expected to become the backbone for systems, networks and platforms to facilitate providing goods and services to citizens and other legal persons, in the government-wide consolidation of processes and systems to enhance national security and in the contribution to economic development and growth.

What are the key takeaways from the community?

It is imperative to review the existing regulatory landscape and identify changes required to support digital identity in South Africa. Emerging legislations would be on open data or open finance that will support innovative digital identity use cases.

Community recommendations

As part of the development of a robust digital identity system for South Africa, a regulatory framework needs to be developed that will support digital identity adoption based on the identified use cases.

Guiding question 5: What should be the overall technology framework considerations for the South African digital identity ecosystem?

A robust technology framework underpins a successful digital identity ecosystem. The major technology design considerations include:

- **Simplicity and scalability of network infrastructure:**
  - Adaptability: For the technology to be scaled as needed, it needs to be able to adapt to an increase or decrease in the volumes of data being processed or the number of people in the system.
  - Scalability: In addition, the system architects need to be able to easily procure and install the necessary hardware and software as well as establish data transfer channels.
- **Security against unauthorised access and usage:**
  - Circumvention resistance: The technology should protect against hackers and other attacks like DDoS, Brute-Force etc.
  - Resilience: The technology should be able to quickly recover from a technology attack and/or breach.
  - Transmission security: The technology should support secure and impenetrable information exchange channels.
- **Technology performance:**
  - Throughput: The technology should be able to process a high number of identity service requests per unit of time.
  - Response time: The response time of the system to an individual request should be fast enough for practical use.
  - Accuracy: The technology should be trusted to provide accurate information and matching.
  - Stability: The technology should be able to withstand significant changes in terms of external forces (e.g., age, development pace, etc.).
- **Integration and user acceptance of the technology:**
  - Integration of the technology with legacy and future systems should be easy and fast.
  - Ease of use: The system should be easy to learn, use and navigate.
  - User interface simplicity in terms of the technology's interfaces is important for the users and relying parties to onboard.
  - Ability of the user to have control over their data and where it can be used is essential to increase trust in the system.
- **Economic and financial viability of the technology:**
  - Affordability and economic viability: The technology needs to be affordable and economically viable. In addition, the technology must be sustainable.
  - Cost-effectiveness: The technology also needs to be cost-effective.

What are the key takeaways from the community?

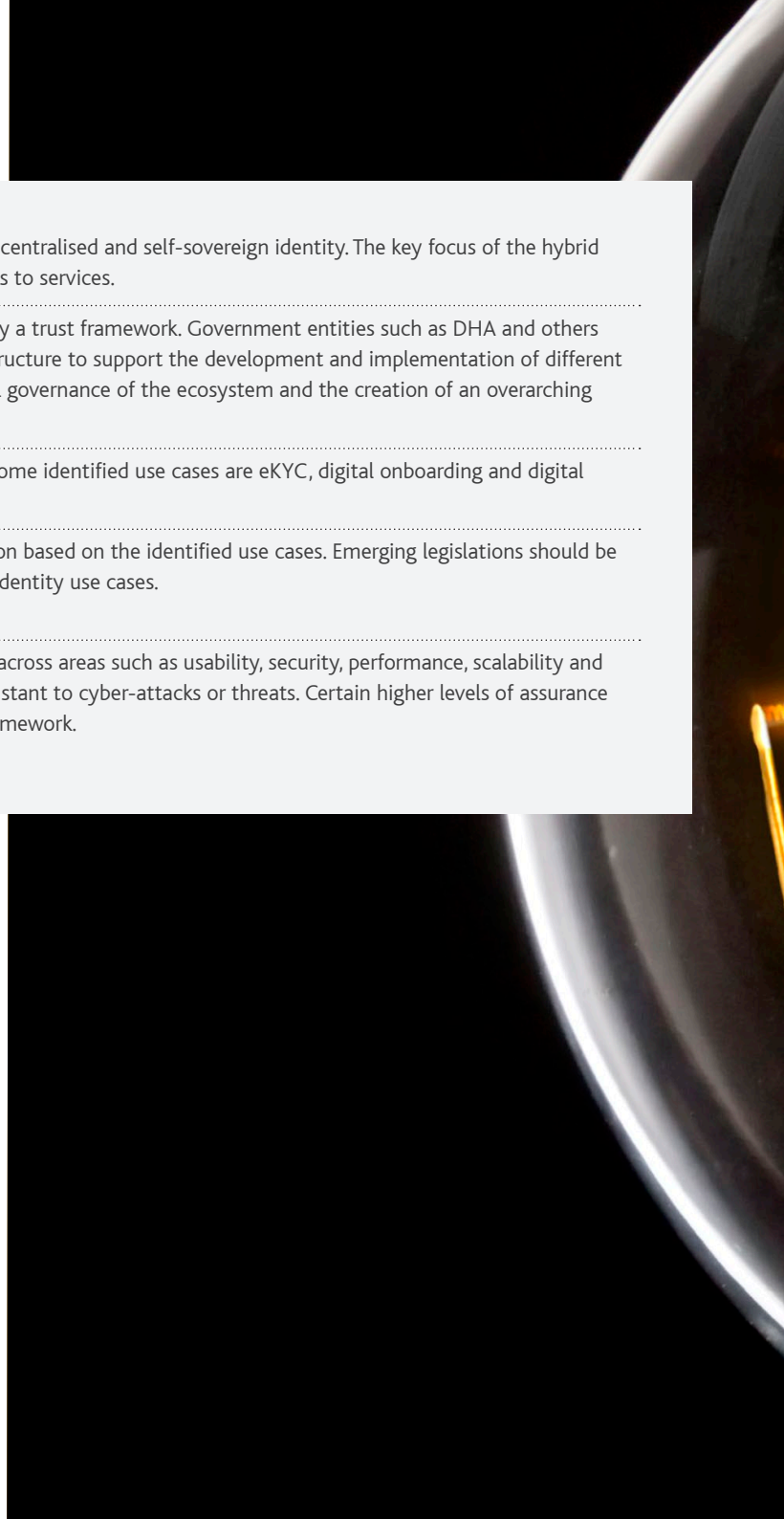
Some of the technologies explored can be used throughout the South African digital identity lifecycle, in alignment with the design principles. These include credential and support technologies and mobile technologies that help enable the ecosystem. The level of assurance was examined, which is an important metric that defines how robust and secure the digital identity is and how user friendly it can be at the same time. The three individual levels of identity assurance, authentication assurance and federation assurance can help us gain insight into the functioning of a digital identity within a set framework of security procedures and measures

Community recommendations

A distributed ledger technology (DLT) which is scalable, fast and secure is required. Certain higher levels of assurance (LOA) should be used in the authentication process and defined in the trust framework. The chosen technology should be tamper-proof and should be able to avoid cyber-attacks or threats.

The table below summarises the community recommendations:

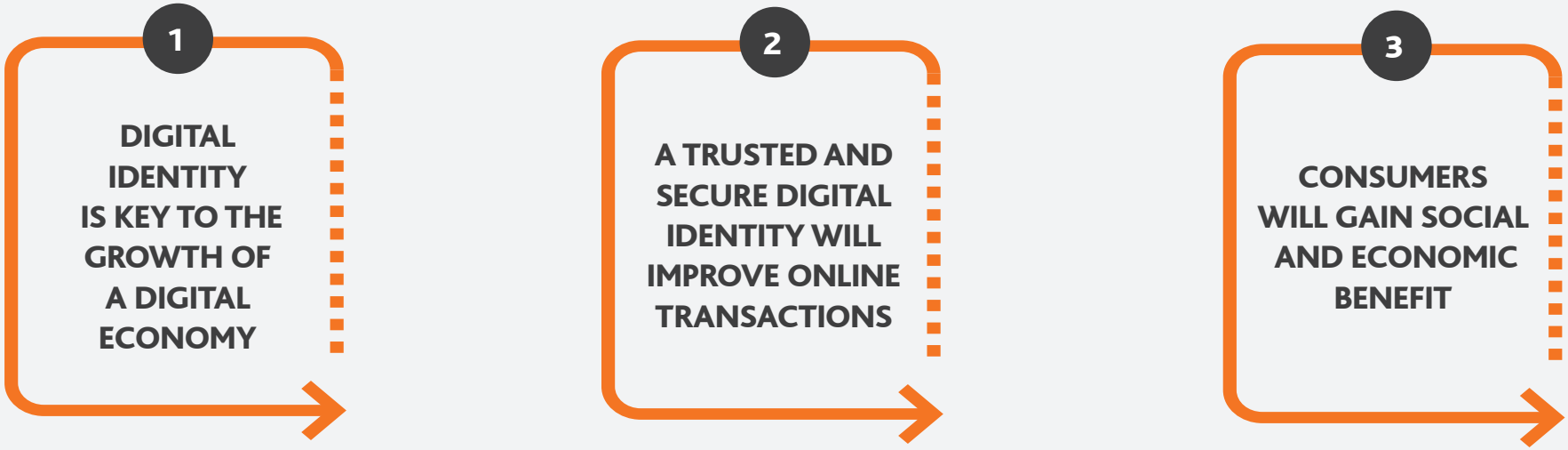
Recommendation 1: Proposed **digital identity model** for South Africa	A hybrid model would address the shortcomings of both ecosystems — centralised and self-sovereign identity. The key focus of the hybrid model should be to ensure data privacy, interoperability and faster access to services.
Recommendation 2: Key stakeholders in the South African digital identity ecosystem and their **respective roles**	There should be multiple credential providers, supported and governed by a trust framework. Government entities such as DHA and others can act as the identity provider and leverage the existing identity infrastructure to support the development and implementation of different use cases. The scheme administrator would be responsible for the overall governance of the ecosystem and the creation of an overarching trust framework.
Recommendation 3: Key focus areas and use cases for a South African digital identity	Key focus areas are financial services, healthcare and social protection. Some identified use cases are eKYC, digital onboarding and digital signature (BankID).
Recommendation 4: Proposed changes to the regulatory frameworks in South Africa for setting up a digital identity ecosystem	Develop a regulatory framework that will support digital identity adoption based on the identified use cases. Emerging legislations should be based on open data or open finance that will support innovative digital Identity use cases.
Recommendation 5: Proposed overall technology framework and considerations suitable for the South African digital identity ecosystem	The technology framework design should consider key design principles across areas such as usability, security, performance, scalability and economic value. The chosen technology should be tamper-proof and resistant to cyber-attacks or threats. Certain higher levels of assurance should be used in the authentication process and defined in the trust framework.



DIGITAL IDENTITY: A CATALYST FOR CHANGE IN SOUTH AFRICA

> A successful digital identity has the potential to benefit those South Africans who are already digitally literate by facilitating greater use and control of data, secure online transactions and reduced fraudulent transactions on online accounts.

A successful digital identity programme can help drive economic value by helping the government curb leakages in areas like social benefits. India is a prime example, with its government saving around US$4.93 billion in FY20. Non-economic value includes the unlocking of major benefits for the people through inclusion, rights protection and transparency. It can facilitate economic transactions, social interactions and political involvement. It becomes a catalyst for change.



A trusted and secure digital identity would improve online transactions and in turn make for a more productive, innovative and competitive economy. A successful digital identity has the potential to benefit those South Africans who are already digitally literate by facilitating greater use and control of data, secure online transactions and reduced fraudulent transactions on online accounts. If the cost of technological devices could be made more affordable and access to internet infrastructure improved, then there would be a larger shift to online services. Digital identity could then be used securely, thereby facilitating more economic transactions, social interaction and political participation.

Consumers will also gain socially and economically. There are a lot of tedious daily activities that can be managed efficiently with a digital identity. In an inefficient environment, the consumer spends a lot of time either creating new identity sources or using existing ones to prove who they are.

By implementing a digital identity, these processes could be streamlined, resulting in time and cost savings for the individual. In addition, the streamlined process and improved experience could potentially increase the buying of new goods and services.

There could also be broader economic benefits, including the growth of online businesses and services; improved security; economies of scale; increased administrative efficiencies; and reduced cost. For small, medium and micro enterprises (SMMEs), digital identity could improve business processes, which in turn could lead to increased production, employment opportunities and revenue.

NEED FOR SHARED UNDERSTANDING AND COORDINATED ACTIONS FOR ACHIEVING A SUCCESSFUL DIGITAL IDENTITY PROGRAMME

The implementation of a digital identity programme involves many critical elements, including support from the community and collaboration between stakeholders. An understanding of these critical elements can set us up for the successful implementation of the digital identity ecosystem.

Active involvement of stakeholders and commitment to the digital identity programme

The digital identity ecosystem can benefit from active involvement of the stakeholders in the design and implementation phases. The complexity of such a programme demands inputs from all stakeholders as well as the larger community. The commitment of resources in the digital identity space is another important factor in the success of digital identity in the long run.

Ambassadors for driving change within the digital identity community

Ambassadors are individuals from the community who will be responsible for driving the thought process of what digital identity does and how it can have positive implications, within their respective organisations. They will create a platform to discuss and promote digital identity within their organisations. They will also be responsible for exploring use cases within their organisations.

Ambassadors will also support decision-making around resource allocation and use case testing and product roll-out to ensure alignment with the strategic outcomes of their organisations and the larger community.

Business case to show commercial viability

The long-term financial sustainability on an initiative like this depends on whether there are commercially viable digital identity business cases that can be identified. Without identifying a clear revenue generation stream and self-sustaining ecosystem, it will be difficult to get buy-in from some critical stakeholders and progress at a rapid pace.

PRINCIPLES FOR FINANCIALLY SUSTAINABLE GROWTH AND ADOPTION OF DIGITAL IDENTITY

- **Essential services:** In some countries, essential or time-critical public services are usually given free of charge or at a low cost to enable access by citizens. Thailand and Kenya are good examples where access to biographic data for essential public services like healthcare is free.
- **User-based pricing:** Some countries have adopted a service pricing model essentially built around the type of user and the type of service being accessed. Typically, utility services are offered at lower prices while perceived luxury services like real estate or personal vehicle registration are offered at a higher price. Tanzania has different price points for citizens and legal residents.
- **Basic services:** Most countries try to offer some basic services such as birth registration for free to help boost adoption by citizens. These services are typically free but attract a fee for subsequent or multiple requests by the same individual. India offers all its public services free of charge.
- **Phased approach:** This model prescribes onboarding users for free or at a low cost in the beginning, and subsequently increasing the fees as demand increases for the services. In India, UIDAI kept the initial services free until 2019 for the relying parties.
- **Discounted pricing for bulk services:** Discounted pricing for bulk services generally involves charging lower if a relying party uses all the services, ranging from authentication to digital signature etc., while providing access to their services. This can help adoption as well as generate revenue for a long-term sustainable digital identity ecosystem. The discounting can be based on the type of request being made, like in Malaysia, or it can be based on online or POS-based services, like in Ecuador.

COMMERCIAL VIABILITY AND REVENUE MODELS OF DIGITAL IDENTITY ECOSYSTEMS FOUND GLOBALLY

Digital identity ecosystems have the potential to generate revenue in addition to saving costs. There are two major ways[63] in which countries around the world try to generate revenue and make the digital identity ecosystem self-sustainable in the long run.

Generating revenue through pay-per-use model

- Charging the relying parties or private entities for the services used, specifically the authentication and verification services.
- Charging individual customers for advance or luxury services or for the more expedited processing of any request.

63 https://id4d.worldbank.org/guide/business-models

Generating revenue through public/private partnerships

- Having service agreements with different government agencies to provide such authentication or support services.
- Operating certain processes in the digital identity lifecycle for the government entity for a fixed period.

India as an example of how digital identity can reduce costs and thus maximise profits

In January 2013, the Indian government proposed a new mechanism for transferring subsidies to cut costs, reduce leakage, and bring higher levels of transparency to the disbursement process called the Direct Benefit Transfer (DBT) scheme. This allowed the government to transfer the benefits or subsidies directly to an individual's bank account. There are now thirty-six government schemes linked under DBT.

Previously, there was ample evidence that subsidies towards the poor were negatively impacted because of 'ghost' public distribution cards. 70-85% of total subsidy spending was not reaching the actual households. After the introduction of Aadhaar-linked DBT, this was reduced drastically. In addition to this, early evidence suggests that by linking PMJDY accounts to Aadhaar, liquefied petroleum gas (LPG) subsidies sent via DBT have seen a 24 per cent reduction in financial leakage. The DBT scheme had seen the percentage of adults with access to an account increase from 35-53%, which means that almost 175 million Indian citizens now have access to banking systems, making the distribution system of the government more robust.

Digital identity was critical in the development of the Canadian digital economy

It is an instrumental tool in making digital services safe, secure, efficient and accessible. For the Canadian digital economy to reach its potential, it is critical that Canadians and businesses have a trusted digital identity to access digital services efficiently.

As per Digital Identification and Authentication Council of Canada (DIACC) report, a conservative estimate of the potential value of trusted digital identity to the Canadian economy is at least 1% of GDP, or CAD 15 billion.[64] Small businesses account for about 30% of Canada's overall GDP (CAD 450 billion). Assuming, the average small business could be just 1% more efficient with access to trusted digital identity, this could potentially add CAD 4.5 billion to the country[65].

The Canadian e-commerce market saw an increase in sales figures from CAD 21.7 billion in 2015 to CAD 28.34 billion in 2018[66]. Trusted digital identity is key to enabling the continued growth of the sector. From e-commerce to the sharing economy, a robust, trusted digital identity establishes trust, provides security and mitigates fraud. A win for citizens and businesses.

64 The Economic impact of digital identity in Canada: Understanding the potential for considerable economic benefits and the cost of inaction
65 The Economic impact of digital identity in Canada: Understanding the potential for considerable economic benefits and the cost of inaction
66 The Economic impact of digital identity in Canada: Understanding the potential for considerable economic benefits and the cost of inaction

In the Nordic countries, digital verifications have taken on the form of a service in which the citizens can use their identity number and a pin code to identify themselves.

- By 2018, about seven million people in Sweden (almost the entire adult population) had digital BankIDs. It is used for payments as well as online contact with public authorities such as the tax agency, the public healthcare system and the municipal school system. It has facilitated the development of the digital government service at both central and local levels. This has led to faster processing of cases and savings in time and money. BankID and other services have resulted in a decline of physical cash in Sweden. During 2016, about EUR 8 billion of cash was in circulation and the country is on track to become cashless by 2025.
- The Government of Denmark has saved about US $300 million annual in self-service efficiencies and aims to unlock a further US$8 billion in benefits.[67]
- Major banks that have instituted e-IDs have seen improvements on existing processes, making them more efficient and less costly. It increases margins for the banks, as well as attracts and retains customers. E-IDs have enabled banks to automate and digitalise their processes through online authentication and e-signature. Estimations by Nets Norway reveal that one paper-based application in the banking sector costs roughly EUR180 in processing and shipping costs. If all signatures in Norwegian banking were electronic, the gains are estimated at EUR150 million annually, with EUR10 million in savings for the Norwegian mortgage market.[68]

It has been observed globally, digital identity has great potential in bringing economic value for countries that have identified the appropriate use cases and used digital identity to solve the underlying problems. There are multiple opportunities for South Africa to realise the economic value of digital identity. There is a need for commercial case for change that will support successful implementation of digital identity in South Africa. It is important to assess the commercial viability of the use cases while building a sustainable ecosystem.

67 Citibank. (n.d.). The Age of Consent: The Case for Federated Bank ID. Retrieved from https://www.citibank.com/tts/sa/flippingbook/2019/the-age-of-consent/gra30727_TTS_age_of_consent/
68 Signicat and Arkwright (n.d.), Federated e-IDs as a value driver in the banking sector based on experience from Nordic markets

CONCLUSION

> The time has come for consumers, investors and the private and public sectors to work collectively to achieve the common goal of enabling a robust, secure and trusted digital identity for South Africa.

Based on the benefits for the economy and society, digital identity needs to be high on the agenda of policymakers, politicians and business leaders. Collaboration by all parties and stakeholders involved is fundamental to the success of a digital identity roll-out in South Africa. With society demanding more from businesses and stakeholders, there is a greater need for the public and private sectors to work together to put the customer first, thereby giving the customer control of their own identity. It is no longer enough for each organisation to go its own way.

Due to identity management's critical role in the 4IR, there is a growing need for the roll-out of a digital identity programme in South Africa. For the benefits to be realised and the impact to the economy to take full effect, the digital identity policy at government level and the development of integrated solutions by businesses need to be a high priority for all stakeholders.

The time has come for consumers, investors and the private and public sectors to work collectively to achieve the common goal of enabling a robust, secure and trusted digital identity for South Africa. It has the potential to generate economic value as well as resolve challenges such as inclusion.

It is important that all parties unite while ensuring a distinctly South African approach so as to safeguard their collective digital futures, ensure that privacy and choice are maintained, and strive to protect the most vulnerable citizens. Digital identity has the potential to meet the evolving needs of South Africans and contribute indirectly towards addressing the high unemployment rate, low savings rates, income inequalities and structural deficiencies faced by the country. In addition, it is aligned to the economic development goals contained in the National Development Plan (NDP) and could help to achieve broader societal objectives such as financial inclusion.

WAY FORWARD

> To embark on this digital identity journey, there needs to be strong partnerships among the custodians of identity, the DHA, as well as the larger digital identity community.

There is an opportunity for the digital identity community to come together and accelerate the digital identity programme to achieve tangible outcomes for South Africa. The community has contributed to the South African narrative learnt on this journey and realised it is time to come together in a truly South African manner.

To make this real, there needs to be a focus on the three core areas of business, technology and governance.

THE NEXT STEPS FOR THE SOUTH AFRICAN DIGITAL IDENTITY STORY

1) **Planning stage**
   - Alignment with the community for finalising the key members and entities who will be part of the ongoing digital identity programme
   - Identification and finalisation of the use cases for developing the business case and infrastructure to run PoCs
2) **Initiation and set-up stage**
   - Setting up of the governance model, including the roles and responsibilities of an advisory board, scheme owner and other stakeholders
   - Preparation of the business cases for the identified use case
   - Setting up an innovation lab that will serve as a platform to test the digital identity solutions be fore the final roll-out

The planning and initiation stages will be critical in shaping the design principles and policies for the identified use cases. There are certain key success factors that need to be considered to ensure the programme meets its strategic objectives and goals. An estimated timeframe for these stages will be four to six months (approximately) and will be dependent on the active involvement of stakeholders as well as support from the community.

A digital identity story is a national story and is only as good as the sum of its parts. There are some key critical success factors that are fundamental to making the story real.

This is a South African narrative to be pursued with active members of the community. As BankservAfrica we are committed to leadership, support and collaboration in this process. We recognise this is not our process but that of the digital community. We are committed to delivering the desired outcomes and making sure the stakeholders are equally involved and engaged in the process.

The success of such a programme is highly dependent on the adoption of digital identity by the industry and the residents of South Africa, which includes citizens and permanent residents. To address this need for adoption at scale, it is imperative to have a 'customer first' ideology entrenched within the design and to analyse customer insights while taking all major decisions on the build and design of the digital identity ecosystem. This needs to be fit for purpose for South Africa.

To embark on this digital identity journey, there needs to be strong partnerships among the custodians of identity, the DHA, as well as the larger digital identity community. This requires continuous involvement, engagement and partnerships among us as the community members. Narrating this story as the base for the South African digital identity story is a good start to making this real.

BankservAfrica would like to recognise and acknowledge the digital identity community for their support in the process of developing the South African digital identity case for change.

ABBREVIATIONS

DBT	Direct Benefit Transfer (India)
DHA	Department Of Home Affairs (South Africa)
DIDs	Decentralised Identifier Documents
DPSA	Department Of Public Services And Administration (South Africa)
eKYC	Electronic Know-Your-Customer
EU	European Union
GDP	Gross Domestic Product
GDPR	General Data Protection Regulations (Eu)
GVA	Gross Value Add
HDI	Human Development Index
ICT	Information And Communication Technology
IdP	Identity Provider
IO	Identity Owner
KSI	Keyless Signature Infrastructure
NIS	National Identity System (South Africa)
PIN	Personal Identification Number
PMJDY	Pradhan Mantri Jan Dhan Yonja (India)
R&D	Research And Development
RP	Relying Parties
SAFBC	South African Financial Blockchain Consortium
SASSA	The South African Social Security Agency
SMMEs	Small, Medium And Micro Enterprises
SSI	Self-Sovereign Identity
SSO	Single-Sign-On
UIDAI	Unique Identification Authority Of India

GLOSSARY

Attributes	The pieces of information that can together help identify a person digitally can be termed as "attributes" of that digital identity. This could include disclosing details from the government — such as your legal name, date of birth, and right to reside, work, or study — as well as details from other organisations, such as your professional qualifications or employment history. The types of attributes include: • **Name:** A combination of letters that can be used to identify a person as given in their birth certificate • **Mobile number:** A unique set of numbers assigned to a mobile phone registered with a network provider • **National ID:** A unique number assigned to a citizen and permanent and temporary residents by the local government • **Date of birth:** A set of numbers signifying the date of birth provided in the birth registration certificate • **Address:** A unique set of characters that signify the permanent address of the user within the country • **Photograph:** A photograph of the user that is stored digitally and helps identity the individual • **Digital signature:** A digital signature is a mathematical scheme like a cryptographic key which is used to validate authenticity • **Biometrics:** Any unique physical identifier that was obtained by birth, like fingerprints or iris • **Gender:** A set of letters defining the gender by birth of the person
Attribute Provider	Offers additional attributes that are not collected by the identity provider during registration, such as government agency, state-affiliated company (e.g., post office) or private company (e.g., teleco).
Authentication	The process of asserting an identity that has been previously established during identification. The individual must demonstrate their ownership of the digital identity.
Authorisation	The process of determining the actions that may be performed or services that can be accessed based on the asserted or authenticated ID.
Enrollers	An entity that helps to verify the identity of new customers during the online onboarding process.
Identification	The process of establishing information about an individual. Successful identification results in the creation of a digital identity.
Identity Authority	An entity that is responsible for overseeing the collection, verification, storage and sharing of personal identity data. They are also responsible for public engagement and grievance redressal.
Identity Operator/ Broker	An entity that helps manage multiple digital identities and passwords and helps integrate with different services through single sign-on systems, e.g., private firms or commercial operators. They play the role of intermediating the data flow between the identity provider and the relying party, for example, an infrastructure provider.
Identity Owner	Owner and controller of a digital identity. Uses their digital identity to identify themselves conveniently and securely in digital transactions. For example, natural person (John, Alex etc.)
Registrars	An entity that helps collect data related to identity attributes for the ID authority or issuer/provider.
Relying Party	An entity that relies upon the credentials or authentication systems provided by an ID system to provide services or grant access to information.
Service Provider	Offers electronic trust services such as digital signatures. Electronic trust services allow providers to enhance and expand the interactions and services within the ecosystem.

APPENDIX: STAKEHOLDERS

STAKEHOLDER	MANDATE
Companies and Intellectual Property Commission	Mandate encompasses companies, close corporations, co-operatives, trademarks, patents, designs, aspects of copyright legislation and enforcement of rules and regulations in most of these areas of law.
Department of Home Affairs (DHA)	The DHA is custodian, protector and verifier of the identity and status of citizens and other residents in South Africa.
Financial Intermediaries Association of South Africa	Financial Intermediaries Association of South Africa.
Financial Sector Conduct Authority	To protect financial customers by promoting their fair treatment by financial institutions, providing financial education programmes and promoting financial literacy, among other things.
South African Reserve Bank (SARB)	To protect the value of the currency in the interest of balanced and sustainable economic growth. Also, the SARB has a statutory mandate to enhance and protect financial stability in South Africa.

In the table below, stakeholders can potentially provide support from a **regulatory and oversight perspective** to ensure consistent identity management and data protection and privacy as well as security and user trust.

STAKEHOLDER	MANDATE
Financial Intelligence Centre	To assist in identifying the proceeds of crime and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.
Information Regulator	Its objective is to ensure respect for and to protect, enforce and fulfil the right to privacy and the right of access to information.
South African Reserve Bank (SARB)	To protect the value of the currency in the interest of balanced and sustainable economic growth. Also, SARB has a statutory mandate to enhance and protect financial stability in South Africa.

The stakeholders below can act as **service providers** in the digital identity architecture for South Africa to ensure effective and efficient service provision as well as security and user trust and fraud reduction.

STAKEHOLDER	MANDATE
Astute	Astute FSE is an industry-owned and -managed body responsible for ensuring that consumer financial information is protected and only shared with authorised bodies.
CSIR	The objective of the CSIR is to undertake directed, multidisciplinary research and technological innovation that contributes to the improved quality of life of South Africans.
FinTechs	The objective of FinTechs is to make financial services more accessible to the greater public. These services include traditional financial transactions (i.e. saving, investing, and loan processing). In addition, the services also encompass revolutionary financial technologies like blockchain and cryptocurrency.

The stakeholders listed below can potentially be **credential issuers** in the digital identity ecosystem to ensure effective and efficient service provision as well as security and user trust and fraud reduction.

STAKEHOLDER	MANDATE
Department of Transport	The DoT is responsible for the legislation and policies for rail, pipelines, roads, airports, ports and the intermodal operations of public transport and freight.
FinTechs	The objective of FinTechs is to make financial services more accessible to the greater public. These services include traditional financial transactions (i.e. saving, investing, and loan processing). In addition, the services also encompass revolutionary financial technologies like blockchain and cryptocurrency.
Major banks	Banks play a key role in the economic development of South Africa. Some of the banks' role(s) include capital mobilisation and financing the local industry, trade, agricultural activities, consumer activities and employment activities as well as assisting with the country's monetary policy.
Southern African Fraud Prevention Service	Objective is to reduce the impact of financial crime on society and the economy.
Telecommunications and postal services	To develop ICT policies and to ensure the development of robust, reliable, secure and affordable ICT infrastructure.

The stakeholders listed below can potentially provide support as **identity operators** to help establish trust among digital identity ecosystem stakeholders as well as to support client government goals and capacity building.

STAKEHOLDER	MANDATE
BankservAfrica	BankservAfrica provides interbank switching, clearing and settlement of low value retail transactions (below R5 million) to the South African banking sector. The group facilitates transactions in a properly regulated system that is compliant with international banking best practice and standards, while reducing risk and complexity in the industry.
FinTechs	The objective of FinTechs is to make financial services more accessible to the greater public. These services include traditional financial transactions (i.e. saving, investing, and loan processing). In addition, the services also encompass revolutionary financial technologies like blockchain and cryptocurrency.

Relying parties and other enablers can help establish trust among digital identity ecosystem stakeholders as well as support client government goals and capacity building. In addition, they can help build open, scalable, interoperable and robust identity solutions.

STAKEHOLDER	MANDATE
Credit Bureau Association	To provide a framework of standards and policies to protect consumer credit information in South Africa to ensure fair and good practice within the consumer credit industry.
Department of Education	Objective is to monitor the standards of education provision, delivery and performance across South Africa to assess compliance with the provisions of the Constitution of the Republic of South Africa of 1996 and national education policy.
Department of Justice	To uphold and protect the Constitution and the rule of law. The department's responsibility lies in overseeing the administration of justice in the interests of a safer and more secure South Africa.
Ministry of Transport	The DoT is responsible for the legislation and policies for rail, pipelines, roads, airports, ports and the intermodal operations of public transport and freight.
National Credit Regulator (NCR)	To promote and support the development of a fair, transparent, competitive, sustainable, responsible, efficient and effective consumer credit market.
Office of the Presidency	The Presidency's key role lies in its responsibility to organise governance. In this regard, a key aim is the facilitation of an integrated and coordinated approach to governance. This is being achieved through creative, cross-sectoral thinking on policy issues and the enhancement of the alignment of sectoral priorities with the national strategic policy framework and other government priorities.
Payment industry players	To offer payment solutions and to innovate.
South African Revenue Services (SARS)	To collect all revenues due, ensure optimal compliance with tax and customs legislation, and provide a customs and excise service that will facilitate legitimate trade as well as protect the economy and society.
Unemployment Insurance Fund (UIF)	To contribute to the alleviation of poverty in South Africa by providing effective short-term unemployment insurance to all workers who qualify for unemployment insurance and other related benefits.

ACKNOWLEDGEMENTS

As we embark on the South African Digital Identity Roadmap, we would like to reiterate our gratitude to all our participants for partnering with us on this initiative and committing your expertise, knowledge and time to reach this point. We look forward to even more rewarding discussions to eventually deliver a uniquely South African Digital Identity solution as a collective.

BankservAfrica
Dana Jedrisko
Jan Pilbauer
Kelello Keetse
Lean Robbertse
Martin Grunewald
Max Sokolich
Runveer Singh
Wendy du Preez

PricewaterhouseCoopers
Aritra Sengupta
Chantal Maritz
Jeaunes Viljoen
Lucia Okafor
Mihir Gandhi
Monindro Saha
Portia Moutlwatsi
Riaan Singh
Salome Ntsibande
Sanelisiwe Hlongwane
Shamik Bandyopadhyay
Zubin Tafti

ABSA
Allen Ramaboli
Sean Mouton

Bidvest
Dijon Smit
Idalina Marthinho
Johan Prinsloo
Kyle Hoffman-Barrett
Muhammed Nathie
Nivindra Naidoo
Rakesh Rama

Capitec Bank
Francois Dempers
Louis Steyn

Consumer Profile Bureau
Marina Short
Nic Meyer

Direct Transact
Mark Heymann

Financial Intelligence Centre
Christopher Malan
Kamla Govender
Pieter Smit

Financial Sector Conduct Authority
Awelani Rahulani
Dino Lazaridis
Jurgen Boyd

Astute
Charl Theron
Jacques Rossouws
Sanet Kotze

Banking Association South Africa
Benjamin April
Billie-Jean Joseph
Kumaran Selvarajalu
Mark Brits
Natasha Malandji

Government Technical Advisory Centre
Kathy Nicalaou-Manias

Illustrious
Robert Dersley

Investec
Camilla Swart
Richard Williams

National Treasury
Paul Esquino
Varsha Gokool

Old Mutual
Brian Robertson
Imraan Ahmed
Lehlohonolo Sehloho
Mohammed Vadee
Siyanda Cibane

Pitney Bowes South Africa
Eugene smit
Leon van der Merwe

Payments Association of South Africa
Jason Wang
Maurits Pretorius
Vinu Thomas

Secure Citizen
Dalene Deale
Katherine Gibson
Onkaetse Bosiu
Shreelin Naicker
Udesh Naicker

South African Reserve Bank
Adri Potgieter
Alicia Potgieter
Annah Masoga
Ayn DuBazane
Freddie Buys
Gerhard van Deventer
Herco Steyn
Hilda Botes
Karel Viljoen
Louis Baloyi
Natalie Roux
Pasca Moale
Pearl Malumane
Peter Makgetsi
Pheto Moabela
Philip Csapler
Pregasen Moodley
Susan Potgieter

SAFBC
Anushka Soma-Patel

Standard Bank of South Africa
Muhammed Omarjee
Stanton Naidoo

SSI Consortium
Lohan Spies

South African Banking Risk Information Centre
Juan Globlaar

South African Fraud Prevention Service
Manie van Schalkwyk

Logos as shared and agreed by the digital identity community for public sharing

CONTACT US

Switchboard: +27 11 497 4000

Email: info@bankservafrica.com

Web: www.bankservafrica.com

Twitter: @bankservafrica

LinkedIn: BankservAfrica