GSMA Intelligence

gsmaintelligence.com @GSMAi

SSA Identity Summit

Leveraging the identity gap

The commercial case for mobile-enabled digital identity solutions in Sub-Saharan Africa

DATE

March 2019

Contents

GSMA Intelligence

Executive summary

1. Government agencies are working for growth of the digital economy

Government agencies, both regional and national, recognise the benefits of online digital identity for the SSA. Benefits include acceleration of digital economic activity, enhanced livelihoods, security of personal rights & credentials, enhanced efficiency of government services, and trust in digital infrastructure and services. Government influence can 'move' the identity market but to leverage this operators need to acquire the ICT resources for single sign-on (SSO) authentication and sophisticated database management to cope with increasingly complex datasets. Partnerships with both government and ICT vendors will be needed to create the identity tools that attract active consumer and SME demand.

2. With operator help, SSA is ready for expansion of identity services

Although mobile internet coverage is currently low in Sub-Saharan Africa, at just 24% of the population, it is expected to reach 40% by 2025[1] creating a market of almost 0.5 billion mobile internet connections. Combining connectivity growth with 495 million Sub-Saharans without foundational identity and the rising cost of cybercrime (estimated at $3.5 billion[2]) creates a formula for massive latent demand for online digital identity. Turning this demand into active consumption of identity services requires the right tools. Operators in the region have a fundamental opportunity to contribute to the delivery of these tools, strengthening their position in the mobile ecosystem at the same time.

3. Operators can target identity, fraud and credit sectors

Recognition that operators have the resources and capability to help deliver online digital identity is growing. Operators have an expanding set of rich customer data and high-use consumer channels such as mobile money, enabling them to assume different roles in the digital identity ecosystem. Leveraging these resources and targeting the region's identity gap could earn operators a stake in the identity and attribute services market, estimated to be worth $4 billion by 2025.[3] To do this, operators will target use cases within three key sectors: identity and authentication; fraud detection and prevention; and credit referencing. Use cases will include linking with national ID to authenticate users online, combatting telecoms and financial fraud, and providing sought-after alternative credit reference data for financial services.

4. Operators should select deployment strategies that scale fast

Operators should choose the deployment strategies that scale value the fastest, which can differ between countries. If governments want to extend national ID online, then basic SSO authentication could be the first move, deployed on high-use services such as mobile money to grow SSO users fast. If the banking sector shows interest in alternative credit data or anti-fraud products, Know-Your-Customer (KYC) attribute products could be the first identity service deployed. Lessons can be learnt from previous national deployments, such as India's Aadhaar identity system; specifically, build security in by design from the start, consider authenticator options carefully, train on privacy, and plan for data breaches.

[1] GSMA Intelligence, 2019
[2] Serianu, 2017
[3] GSMA Intelligence, 2019

GSMA Intelligence

Context: the identity market in Sub Saharan Africa

Types of paper and digital identity

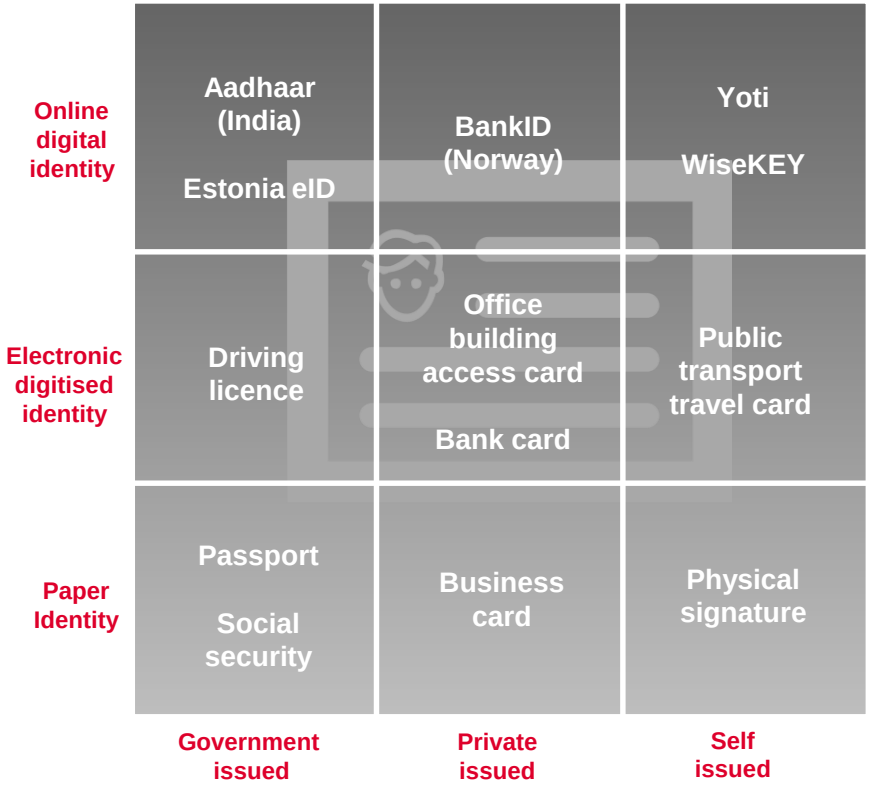
Online digital identity enables people to participate in the digital economy, facilitating online access to e-commerce, digital payments, money transfers, government benefits and cross-border authentication.[1]

An online digital identity is the online version of a person's real-life identity, which potentially includes all personally identifiable digital information such as contact details, electronic digitised identity documents, purchasing preferences, financial data and media activity.

Identities can be issued by government agencies or private organisations, or even self-issued by individuals. They have three main stages: paper, electronic digitised and online digital. Electronic-digitised identity works only in physical space, whereas online digital Identity can support internet authentication.

Online digital identity can evolve from government-issued identities (e.g. Aadhaar in India and eID or Mobile-ID in Estonia). Government-issued identity is often categorised as 'foundational identity' (but can also be 'functional identity' as in a voter ID), and is built with the objective of bolstering national development by creating a general-purpose identification for use across sectors.[2]

Functional identity is defined as evolving from a single use case, such as voter ID, health records or bank cards, and has the potential for use across the private sector. Identity solutions can be categorised by format and issuance, as shown with examples in the table.



[1] McKinsey, 'Digital Identification: A key to inclusive growth' 2019
[2] GSMA M4D Digital Identity, World Bank

Source: GSMA Intelligence

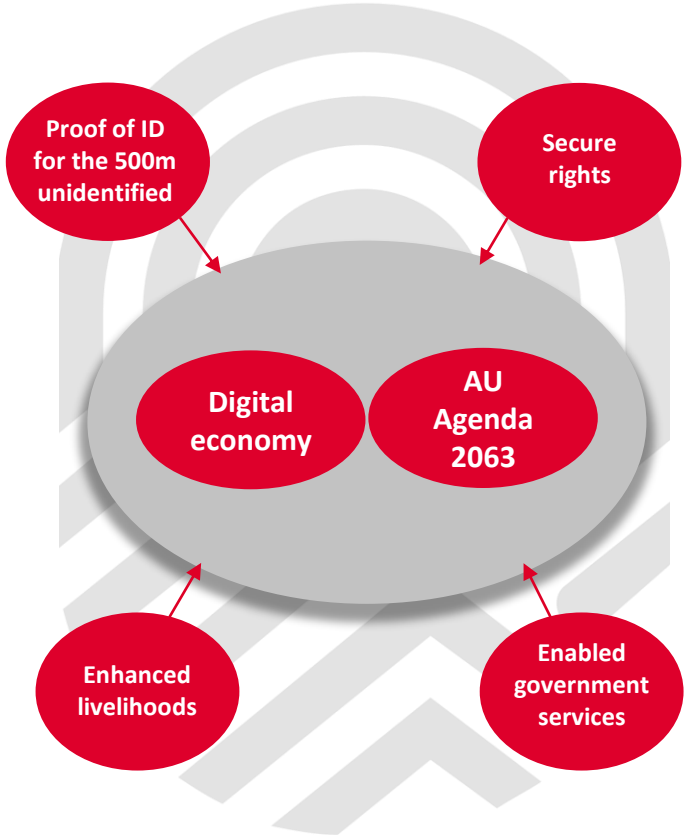
Digital identity is a critical enabler of benefits

Africa's digital economy as a whole is expected to grow to more than $300 billion by 2025 [1]. Digital identity is seen by the African Union (AU) and United Nations Economic Commission for Africa (UNECA) as a critical enabler for the digital economy and for the AU's Agenda 2063, which has ambitious targets on poverty, education and technology. Regional policy targets are expected to encourage investment in infrastructure and innovation that can deliver important benefits for the people of SSA, including:

- **Proof of identity** for around 500 million Sub-Saharan Africans who do not have a foundational form of ID, accelerating their access to and participation in the digital economy[2]
- **Enhanced livelihoods**, through access to employment, education, health, technology, financial services and social protection
- **Secure rights** to land, property, nationality and benefits
- **Enabled government services** – efficient delivery of government-to-person (G2P) payments and international funds linked to an individual's identity.

With the success of mobile money services in SSA, mobile operators have already proven their ability to create digital services that put them at the centre of the digital economy. Contributing to the delivery of benefits illustrated here will open a new phase of opportunity for operators to build new mobile services, with digital identity as the critical enabler.

Benefits enabled by digital identity:



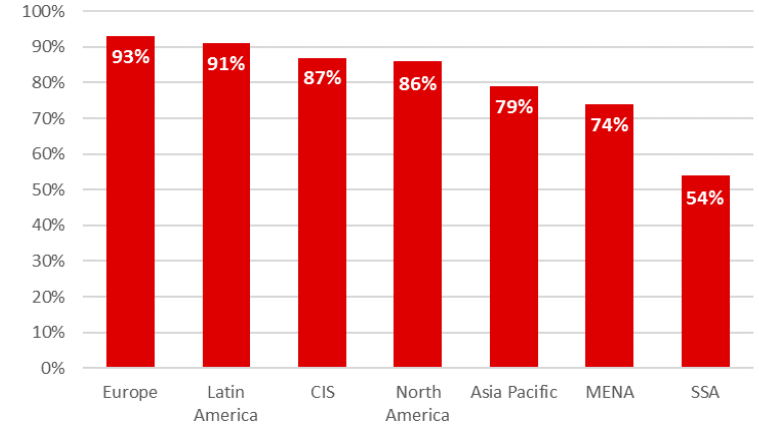
[1] Omidyar Network/UNECA, 2019
[2] World Bank, 2018

State of identity in Sub-Saharan Africa

There have been concerted efforts to introduce identity in Africa over the last 10 years, by governments and regional organisations. The 1st Government Forum on Electronic Identity in Africa (ID4Africa) took place in 2015 in Tanzania, and more recently the UN has recognised legal identity as a Sustainable Development Goal for 2015-2030.

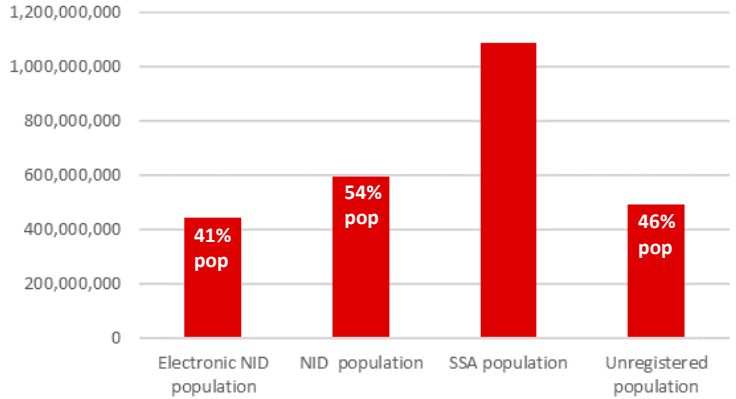
However, compared to the rest of the world, the proportion of the 1.1 billion population in SSA with a legal/official national Identity (NID) is still low at just 54%.

Registered national ID worldwide (percentage of population), 2018



Source: ID4D, GSMA intelligence

Registered/unregistered national ID in SSA (percentage of population), 2018

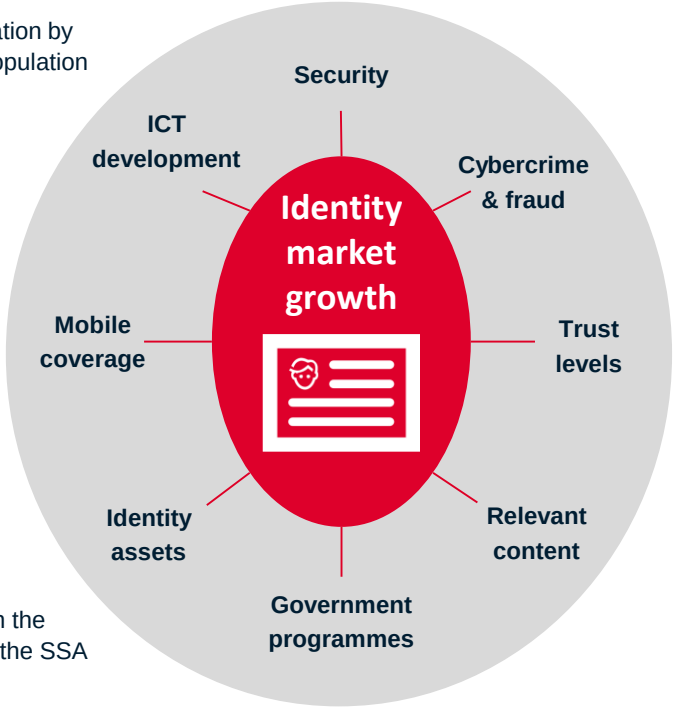


Source: World Bank ID4D, 2018

Evolving electronic NID, currently used by 41% of the population, into online digital identities that can be used for single sign-on to internet services and apps is seen as a significant opportunity to drive the digital economy. The opportunity has been fully recognised by the AU and other regional agencies; the AU recently met to consider a framework for Good Digital Identity in Africa as a basis for participating in the African Continental Free Trade Area (AfCFTA). The Good Digital Identity Framework clarifies the principles to be upheld by providers involved in digital identity services as they drive participation in the digital economy for more than 1 billion people in SSA.

Market drivers of digital identity services in SSA

1. **Mobile coverage:** SSA has comparatively low mobile internet connectivity and smartphone penetration by population, but by 2025 these are expected to reach 40% (500 million) and 58% (715 million)[1] by population respectively, providing a robust basis for digital identity services.
2. **Identity assets:** high mandatory SIM registration combined with 36% penetration of mobile money services in the region[2] help operators collect customer and credit reference data, providing them with the consented digital identity assets required to develop new revenue streams from financial services and other third-party service providers.
3. **ICT development:** provision of cybersecurity solutions, technical training, digital literacy and an attractive environment for global identity players drive supply and demand for identity products.
4. **Trust levels**: institutional trust levels in the region are thought to be comparatively low. For example, only 14% of South Africa's population trust government. Where trust is absent, the popularity of trusted identity, authentication and documentation services can rise sharply.[4]
5. **Data security**: national ID schemes in Africa will need to address data security issues before implementation. Aadhaar in India addressed data leaks by adding a layer of data security with a virtual ID, automating security procedures, and planning response to data breaches.
6. **Cybercrime and fraud**: the cost of cybercrime in Africa was estimated to be $3.5 billion in 2017, driving enterprise and consumer demand for both public and private identity solutions.[5]
7. **Relevant content:** Locally relevant content and services at affordable prices drive engagement with the mobile ecosystem. The GSMA Global Mobile Engagement Index is a measure of this engagement; the SSA region currently scores low at 1.5, compared to an average score for Europe of 4.0.[6]
8. **National, regional and global government programmes**: AU's Good Identity Initiative and the UN Sustainable Development Goals are driving considerable activity and investment around digital identity.



[1] GSMA Intelligence, 2019
[2] GSMA M4D Mobile Money, 2018
[3] GSMA M4D Mobile Money
[4] Edelman Trust Barometer
[5] Serianu, 2017
[6] GSMA intelligence

GSMA Intelligence

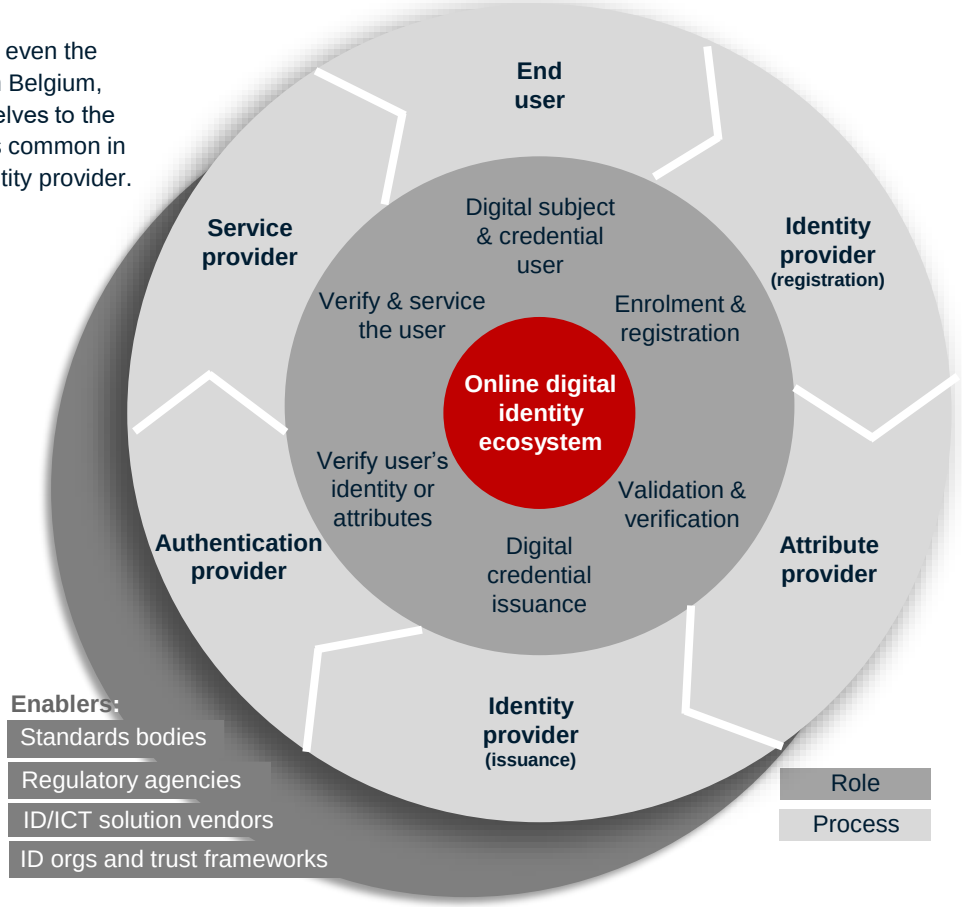
The role of mobile operators in identity markets

The operator role in the identity ecosystem

Mobile operators have the potential to play a variety of roles in the ecosystem – even the identity provider role, through partnerships with private companies (e.g. Itsme in Belgium, BankID in Norway). However, operators' resources and capabilities lend themselves to the roles of attribute provider, authentication provider and service provider. It is less common in the rest of the world for operators to take the role (and liability) of being the identity provider.

Role	Operator asset
Identity provider (registration)	SIM registration, customer relationship, physical outlets/agents for enrolment
Attribute provider	Customer and network data, consent channel, ICT capability, and mobile money services
Identity provider (issuance)	Customer portal, operator single sign-on (SSO)
Authentication provider	SSO login, Mobile Connect, cross-operator collaboration
Service provider	Operator media and services (e.g. mobile money)

Thanks principally to mobile money wallets in SSA, users have 'everyday' engagement with operator brands helping to build trusted relationships between customer and operator. Combining this trust with offline/online customer channels, and the responsibility of managing the user's data, provides mobile operators with the assets and capability to play a primary role in the digital identity ecosystem.



Total addressable market for identity services

Most operators in SSA have the resources to address three key identity market sectors: identity and authentication; fraud detection and prevention; and credit reference data. The total addressable market of these sectors combined is estimated to reach $4 billion by 2025.[1] In these sectors, operators can compete with other identity services to carve out a share of the total addressable market value.

Identity and authentication

Definition: the market for identity and authentication services designed to enable the creation of identity credentials, and to validate, issue and authenticate them.

Identity and authentication

Total addressable market value in SSA by 2025[1]

$1.2bn

Fraud prevention and detection (FDP)

Definition: FDP systems analyse data from a wide range of data sources, reporting anomalous trends and transactions to prevent fraudulent access, verifying user identity and maintaining data integrity.

Fraud detection

Total addressable market value in SSA by 2025[1]

$0.77bn

Credit reference data

Definition: credit history from mobile money services and prepaid accounts, as well as alternative data derived from operators' customer and network data.

Credit reference data

Total addressable market value in SSA by 2025[1]

$2.0bn

[1] GSMA Intelligence, 2019

Leveraging operator assets for Identity propositions

Operators in SSA have considerable resources and capabilities that can be marshalled to produce attractive value propositions in each of the target identity sectors:

Identity and authentication

- SSO provides easier, more secure login with fewer drop-outs due to forgotten passwords.
- Step-up* strong multifactor authentication replaces weak SMS OTP and complies with European PSD2 regulation.
- SSO enhances security of private key authentication where trade requires digital signature.
- Linkable with national identity.
- Guest login / passwordless login / cookie replacement.
- Simplify login and registration for users who are new to SPs. Operator SSO could be used as cookie replacement or to enable access to content on a trial basis.

* Authentication that enables a step up to stronger level of assurance depending on the context

Fraud prevention and detection

- Handset, as primary factor, less vulnerable to scalable attack.
- ‘Binding’ of mobile operators’ network attributes uniquely enhances ID verification and anti-fraud attribute services.
- Operators are in a user-facing and contracting position, enabling them to gain consent for sharing.
- Private mobile network rather than public internet helps prevent man-in-the-middle (MiTM) attacks.
- Registration of the service provider with the operator creates extra security layer against phishing/scamming.
- Privacy by design supports user consent and authorisation of data sharing.
- Removing frictional website registration using attributes to ‘autofill’ forms.
- Enhancing operators’ current enterprise offering (e.g. Wi-Fi, VPN).

Credit reference data

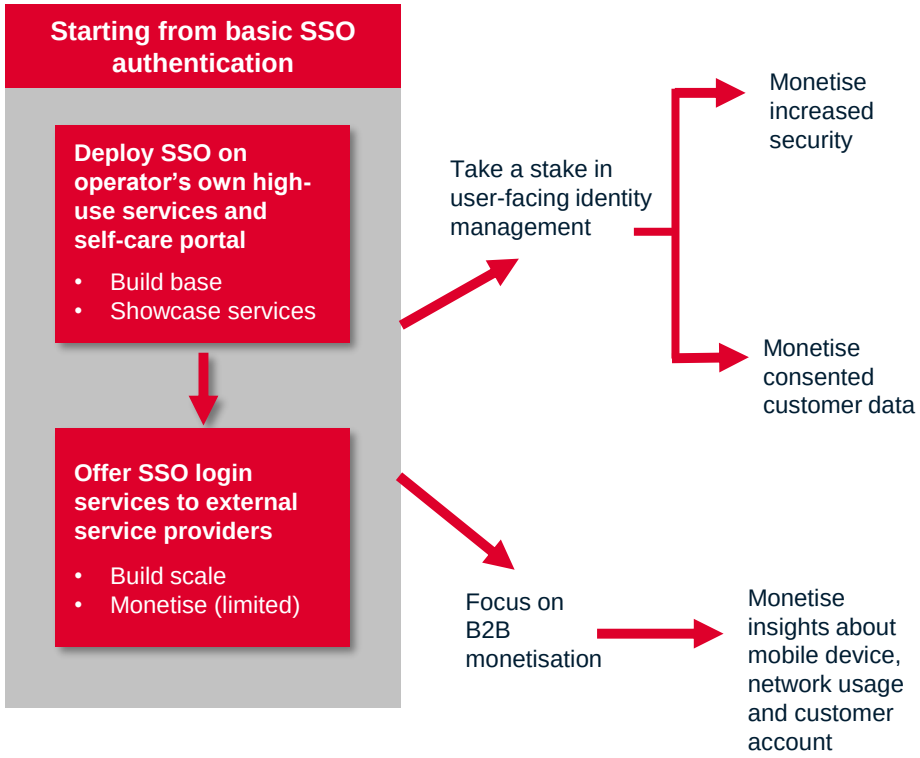
- Operators have a differentiated dataset with the ability to link data together, as well as link with a user’s real ID.
- Operator-controlled customer data from subscriber accounts, dynamic networks and behavioural attributes provide valuable information for credit scoring.
- Credit reference data from registered prepay accounts and mobile money is a powerful tool for financial inclusion in SSA.
- Enables operators to give unbanked customers an 'on-ramp" to otherwise unattainable financial products and services.

GSMA Intelligence

The commercial opportunity for identity services in Sub Saharan Africa

GSMA Intelligence

Paths to monetisation



Strong authentication or authorisation

- For banking, payments, government, and supply chain management for SMEs.
- Enterprise and SME opportunity can be addressed by a single mobile operator as B2B accounts have a corporate contract with just one operator.

Identity attributes

- Greatest value lies in 'true' identity – i.e. linked to national ID.
- Simpler, valuable products can be deployed until user data quality and coverage is sufficient, e.g. identity verification for antifraud or registration for e-commerce.
- Data privacy considerations are particularly important.

Network attributes

- Network attributes are unique to mobile operators.
- Antifraud services for banking and other sectors can be seamless for end-user.
- Mobile operator launch timelines can be quicker with reduced impact on the user flow.

GSMA Intelligence

The commercial opportunity in the identity and authentication sector

GSMA Intelligence

Identity and authentication: use cases

Key use cases enable the connected population's participation in the digital economy – for secure identification to access government services, humanitarian aid, credit and financial services, cross-border payments, e-commerce and ownership rights management.

Foundational and functional identity use cases	Example identity solutions
• Refugee identification: regain lost identity • Access to humanitarian aid: secure and transparent delivery of funds for groceries at reduced operational cost	• WFP Building Blocks (EyePay) based on blockchain
• National government digital identity schemes: provide access to government services and unify ID across the country • Enable e-commerce: mobile money wallet login, website login • National Registration Bureaus: manage ownership rights: help to document and authenticate assets and land ownership	• Ghana card (version: Dual Interface Chip Card) • Gambia card • Nigerian National Identification Number (NIN) • eCitizen in Kenya • Aadhaar (national digital card in India)
• Grow digital content consumption: For example, easy SSO is central to Turkcell's strategy of encouraging consumption of more Turkcell products and services.	• Turkcell's Fast Login (powered by Mobile Connect) – made mandatory for logging into services
• KYC: an imperative for combatting fraud • Credit referencing: credit information and referencing due diligence for banks	• Bank Verification Number (BVN) in Nigeria as well as the above national ID cards
• Self-sovereign identification: self-asserted ID and management of personal data • SSO login and signup: simple and secure digital access to services	• WISeID suite of mobile applications built on blockchain • Yoti – self-asserted digital ID

Identity and authentication: operator opportunities

To enable these opportunities, authenticators should be chosen to align with the region's market requirements, such as universal subscriber reach, security, simplicity and a data connection unessential for physical use:

1. **Digital enhancement of national identity programmes:** 54% of the region's population are covered by NID, 41% of which are in electronic format.[1] Given that NID has already provisioned identity, extending usability to the digital environment is an attractive option for opening up the digital economy. *Opportunity: operators in SIM registered environments are well positioned to make the phone number, linked with NID, a bridge to the digital economy.*
2. **Mobile operator digital single sign-on (SSO):** many operators in Africa have self-care portals and are growing their VAS portfolio (e.g. Songa, Safaricom's music service). Turkcell started in the same way and has found launching SSO authentication for all its services essential to growth of its content offering. Turkcell is now attracting third-party service providers willing to pay for its SSO service. *Opportunity: Mobile operators can leverage their mobile money wallets to quickly build their own SSO login user base and then market it to third parties.*
3. **Identity and authentication for enterprise:** more than 90% of African businesses lack the basic requirements to ensure minimum levels of cyber-security.[2] *Opportunity: developing SSO and KYC products for enterprise will contribute to basic security for SME businesses in Africa.*

[1] World Bank ID4D, GSMA intelligence
[2] Serianu, 2017
[3] Myriad Group

Authenticating technology

USSD and SMS OTP are currently the most penetrated authentication technologies in SSA.[3]

Authenticator	Description	Benefit	Challenge
SMS OTP (e.g. most SSA countries)	One-time password sent to mobile number and used to login	Simple to use. Involves operator. Universal reach.	SMS interception. SIM swap and call-forwarding fraud
SIM Auth. Applet (e.g. Kenya)	Encrypted code sent to a server for verification	E2E secure encryption. Seamless user experience.	Needs data connection and smartphone
Header Enrich. (e.g. South Africa, Zambia)	Adds user/device identifiers in HTTP header	Simple to use	Human-readable and unencrypted
USSD (e.g. all SSA countries)	Authenticates on mobile network not on IP	No data needed. Works on all devices.	Message response needed in real time
Biometrics (e.g. Tanzania, The Gambia)	Adds another factor 'something you are' (e.g. finger, iris, face)	Local storage for fraud security. Easy to use.	Biometric methods need premium smartphone.
Behavioural AI (emerging)	Profiles a user's unique keystrokes and device set-up to create behavioural identity	Invisible authentication	Needs data connection and behavioural attributes

Currently appropriate for SSA | Established but insecure | Emerging technology

GSMA Intelligence

The commercial opportunity in the fraud detection and prevention sector

Fraud detection and prevention: use cases

Fraud detection and prevention is a growing market in SSA, with financial fraud expected to grow further as the region's national governments become more successful at driving financial inclusion. Telecoms fraud is also a major problem in Africa, with 80% of operators falling victim.

Identity use cases	Example identity solutions
• *Payment fraud prevention:* detect, possibly in real time, unusual behavioural patterns and report them (e.g. SIM swap, call forwarding etc)	• Turkcell deployed Oracle Exadata Database Machine X2-2 HC Full Rack to prevent prepaid card calling fraud using in-database analytics
• *Digital KYC checks:* selected customer data matched against operators' customer data	• Telesign APIs are customisable to prevent real-time threats by improving the user verification process (working in China and Brazil)
• *Account Takeover Protection (ATP):* prevents account takeover fraud such as SIM card cloning and SIM swap	• SK PASS is the Korean operator's authentication solution that claims to have reduced ATP to zero
• *SMS fraud:* increases illegitimate traffic on mobile networks, preventing it reduces cost and safeguards SMS revenue • *SMS OTP fraud is high in Africa*: SSO authentication can replace SMS OTP and improve security • *Countering international call bypass fraud (e.g.SIM box fraud):* illegally terminates international VoIP traffic masked as local mobile network traffic	• Deutsche Telekom's SMS+ is an A2P messaging protection service • Mobile Connect for basic and strong SSO authentication • Tighter SIM registration with KYC checks can contribute to the fight against SIM boxing

Fraud detection and prevention: operator opportunities

1. **Telecoms fraud:** communications fraud cost operators $33 billion worldwide in 2018, around 3% of revenues, with more than 65% tied to international communications traffic.[1] Main categories include voice, SMS, international bypass (SIM box fraud), and signalling fraud, but the emergence of IoT and 5G will expand these threats further. Effective prevention and detection of this type of fraud will also strengthen defences against Identity theft and financial fraud.
   Opportunity: operators' customer, network and behavioural data combined with big data analytics, AI, deep packet inspection and ICT solutions could enable operators to reduce their own fraud costs and set up new revenue streams from combatting fraud for third parties.

2. **Financial fraud:** the average annualised cost of global financial cyber crime per firm is up 40% from nearly $13 million in 2014 to over $18 million in 2017, with a quarter of the cost hitting financial services.[2] In addition, growth in agriculture micro-insurance and mobile money micro-finance is expected to drive significant demand for fraud detection and prevention services.
   Opportunity: operators have a powerful set of assets for enhancing cybersecurity capable of providing ATP, KYC and MSISDN verification – to name just three current identity service opportunities.

Cybercrime and cybersecurity in Africa

The cost of cybercrime as a whole in Africa was estimated to be $3.5 billion in 2017 – a third of it from Nigeria and Kenya. While Africa doesn't even account for 0.5% of the estimated $1 trillion that cybercrime costs globally, it has grown 75% in the region year-on-year.[3]

Combatting cybercrime requires commitment to cybersecurity, something that the ITU Global Security Commitment Index states is only at the 'initiating' stage across most of SSA. As mobile coverage grows and IoT devices become more widespread, the threat landscape will continue to expand, indicating that cybersecurity will be a growing opportunity for mobile operators.

[1] Europol, Cyber-Telecom Crime Report, 2019
[2] Cost of Cybercrime, Accenture/Ponemon institute 2017
[3] Cost of Cybercrime in Africa, Serianu, 2017

GSMA Intelligence

The commercial opportunity in the credit reference market

Credit reference market: use cases

Microloans through microfinance institutions operating in Sub-Saharan Africa reached $9 billion in 2017. Strong growth in the credit reference market will help drive growth in microloans resulting in improved financial inclusion across the region.[1]

Functional identity use cases	Example identity solutions
• *Credit scoring using traditional and alternative data:* gathered from mobile phone transactions. These companies often partner with operators as a consumer channel and to gather information.	• Experian: a global credit reference company operating in South Africa. • XDS: locally owned credit information bureau with subsidiary operations in Ghana, Nigeria and Zimbabwe. • Compuscan: established in South Africa and targeting microloans. • Transunion Mobile Score Card: a mobile loan information service that enables lending firms to access a loan applicant's credit status
• *Introduce unbanked to financial services*: with 66% of Sub Saharan Africa unbanked, getting started is the biggest problem for people particularly without a functional Identity.[2]	• Juvo: establishing financial ID, based on mobile data, prioritising people who are creditworthy, yet financially excluded.
• *Digitise agriculture supply chain:* creates digital business history that farmers can use to gain first-time access to small business financing.	• 2Kuze: a platform developed by MasterCard Lab for Financial Inclusion in agriculture.
• *Behavioural banking*: leverages and attempts to modify controllable behaviours linked to banking risks that lead to 80% of the reasons why individuals do not meet their financial obligations.	• Discovery Bank: new banking division of South Africa's largest health insurer, Vitality. Allows new users to sign up using a live selfie for verification that is compared to the database of images in the Department of Home Affairs, which issues identification documents and passports.

[1] Microfinance Barometer, 2018

[2] World Bank, 2018

Credit reference market: identity opportunity

- **Alternative credit reference data:** Sub-Saharan Africa is a hotbed of banking innovation, according to McKinsey, due to 'low levels of banking penetration, heavy use of cash, sparse credit bureau coverage, and limited branch and ATM networks'.[1] There are an estimated 81 million SMEs based in SSA, with an outstanding credit gap of $132 billion according to the European Investment Bank. This presents a major credit opportunity for banks, fintechs and non-bank SME lenders. However, smaller firms present major risk control challenges and are expensive to manage given their smaller transactions and accounts. Managing this kind of volume and complexity requires automation and alternative datasets to address the lack of credit history in the region and verify important customer data. Operators have a rich supply of both credit history from mobile money and alternative customer and network data that can be used to derive credit scoring for individuals and small businesses. *Opportunity: Operators have a range of alternative credit reference data highly sought-after by SME lenders. The data can provide local context and end-user characteristics, and can be mixed to derive credit reference data customised to the needs of the growing fintech space.*

[1] McKinsey Global Banking Report, 2018

Mobile operators' alternative credit reference data

Mobile money data	Mobile network data
Mobile money services provide alternative data for customer credit scoring: • estimate user's income • evaluate financial behaviour • business transactions	Derived attributes from network data can score users: • buys airtime regularly = stable income • international calls = high living standard
Mobile customer data	**Mobile behavioural data**
Customers' registered data can be used for KYC and other analysis: • phone type • demographic • social class • gender	Behavioural data can tell a more complete story: • phone set-up • apps used • geo-location shows transport type

GSMA Intelligence

Identity recommendations for mobile operators in Sub Saharan Africa

Recommendations for mobile operators (1)

The digital identity opportunity provides operators with a strategic position central to digital transformation in the SSA region, offering the following:

- a new revenue opportunity from the growing identity market
- strengthening of operators' customer relevance
- an enhanced value proposition to enterprise
- an enhanced value proposition to service providers
- extended reach to cross-border service providers.

The following recommendations are designed to help operators capture some of the above benefits.

1. **Policy is a powerful driver: work closely with national and regional government agencies**

   Operators should work in step with all relevant policy initiatives as regional and national governments are powerful drivers of digital identity in SSA. Most recently, the AU's Good Digital Identity initiative is helping to improve privacy/data protection frameworks in countries mandating SIM registration. Operators could help governments take their NID online by attaching it as a credential to operator SSO.

2. **Obtain senior management endorsement**

   The need for broad internal support across departments to roll out digital identity services requires endorsement by senior management. At Turkcell, senior management and strategy teams understood the importance of the initiative and encouraged the promotion of Fast Login as the primary login option.

3. **Deploy high-coverage authenticators with two factors, if necessary for higher-risk environments**

   In this region of Africa, high coverage authenticating technologies include USSD, Header Enrichment, and SMS OTP. Weaknesses listed below can be solved by stepping-up to two factors and introducing realistic pricing:

   - USSD*:* e.g. many banks in the region have made USSD their primary authentication channel for services. But USSD is expensive for operators to run and 'under-priced', and once the channels are above their threshold, operators risk failing to meet their network quality KPIs.
   - SMS OTP: this basic technology has been used for authentication for many years but is increasingly seen as a security risk vulnerable to man-in-the-middle attacks.
   - Header Enrichment: classic header enrichment is human-readable and unencrypted, leaving device and subscriber identity data vulnerable.

Recommendations for mobile operators (2)

4. **Collaborate and align product with other operators to drive scale with service providers**

   One way of ensuring coverage is to align with other operators in-market. Maximising population and mobile subscriber coverage requires operators in a country to deploy aligned products in a similar time-frame. This is especially important to attract key external service providers such as banks and global web brands. If operators share an aligned product roadmap, scaling of identity products in the market can be significantly accelerated.

5. **Identity and authentication services should be aligned with the SSA region's market environment:**
   - **Standalone basic SSO authentication:** launched initially on operators' own services and subsequently to third-party service providers. SMS OTP replacement being a primary value proposition.
   - **Federated basic SSO authentication**: launched in collaboration with fellow country operators for enhanced coverage (see the GSMA's Mobile Connect service)
   - **PKI Digital Signature**: government use and enterprise contractual use cases require strong credentials and authentication. Public Key Infrastructure (PKI) solutions that employ the right mix of authentication, encryption and digital signatures are likely to be in demand.

6. **Launch SSO authentication even in low coverage territories**

   Mobile internet and smartphone penetration of population in SSA are low compared to the rest of the world at 24% and 31% respectively[1]. However, mobile internet is growing at 15% year-on-year and penetration of smartphones in the population is estimated to reach nearly 58% in SSA by 2025 (715 million smartphones)[2]. Deployment of digital authentication now, will ride the growth in smartphones and internet connections. But also considering the SSA context, 'offline' digital identity is essential to livelihoods.

7. **Security by design: make security a priority at the beginning**

   Whether partnering with government in the region or launching SSO services in collaboration with other operators, operators should address data security issues at the very beginning. For example, at launch, India's Aadhaar card suffered from information leaks and data storage issues. An extra security layer was eventually added using virtual IDs, automated security procedures, privacy training and plans for responding to data breaches.

8. **Build identity assets: expand collection and curation of customer data**

   Customer, network and behavioural data are essential for providing people with their own digital identity and access to credit, as well as the fight against cybercrime estimated to be worth $3.5 billion in 2017.[3]

[1] GSMA Intelligence, 2019
[2] GSMA Intelligence, 2019
[3] Serianu, 2017

Recommendations for mobile operators (3)

9. **Build customer trust through consent and transparency**

   In a region where 10/12 countries indexed by Freedom House[3] are classed as 'not free' or partly' free, institutional trust is low. Consequently consumers are looking for tangible trust in the identity services they use. Operators in SSA can position themselves as trusted providers of authentication and other identity services….

10. **Creativity is needed to design sustainable business models**

    Nordic digital identity solutions such as BankID are rare examples of digital identity solutions paid for by consumers. Certainly in SSA it is service providers or enterprise customers that will be operators' paying customers. Whether targeting authentication or sectors that require data services, operators will need to be creative in designing business models. Examples of sustainable business model options in SSA are likely to include:

    - per transaction or transaction bundle pricing
    - per user subscriptions (similar to standard software licences)
    - indirect value uplift: authentication for operator paid services that incorporate authentication costs and receive an incremental uplift from enhanced trust and simplicity.
    - combinations of the above options.

[3] Freedom World Report, 2019, Freedom House

11. **Launch SSO on a highly utilised service such as mobile money or self-care portals**

    Start by launching SSO on an operator's own properties. Rapid adoption of an SSO service will help secure full internal buy-in. For SSA, this will mean likely launching the solution on mobile money or self-care portals. This provides a fast-moving test-bed, enabling the project team to make impactful changes quickly.

12. **Identity attribute services should be aligned with the SSA region's market environment:**

    - **KYC***:* developing markets starting to introduce online digital identity have a strong demand for checking customer credentials in line with KYC principles.
    - **ATP:** allows additional checks on a user's mobile phone status to determine whether a device has been compromised. Gives an indication of whether there has been a recent SIM swap and may optionally return other information relating to the user's mobile account: recent SIM change (MSISDN - IMSI pairing), active unconditional call diverts, device reported lost or stolen, recent device change (timestamp of last MSISDN - IMEI pairing change) and mobile phone account status (active or inactive).
    - **Credit reference or credit scores:** operators in the SSA region often have mobile money services providing valuable credit reference history that can be resold directly (with user's consent). Even without mobile money data, operators have a considerable range of data attractive to credit reference customers.

GSMA Intelligence

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Author

Mark Little
Senior Manager, Consulting

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com