Seamfix



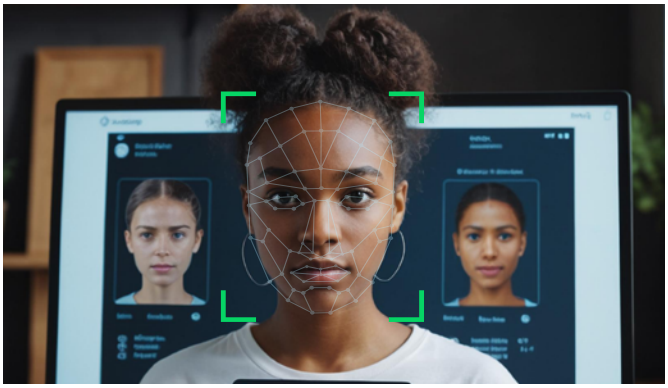
The African Digital Trust & Compliance Report

Industry Intelligence & 2027 Outlook on Identity, Payments, Telecom, Insurance & Digital Public Infrastructure

Section 1 – What Happened?

1.1. Executive Summary

Identity verification has emerged as Africa's fastest-growing trust infrastructure in 2026, driven by regulatory reform, rising identity-centric fraud & expanding digital public services across telecommunications, financial services and government.



Africa's digital economy has entered a new phase. Mobile technologies contributed approximately **US$240 billion**, representing **7.8% of Africa's GDP**, while supporting **13 million jobs** and generating **US$45 billion in public revenues.** The industry's focus simultaneously shifted beyond connectivity toward identity verification, fraud prevention and digital trust services.

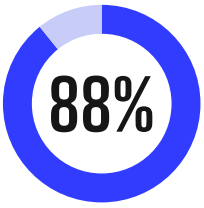
This transition was reflected across multiple sectors. **Ten African operator groups** committed to the GSMA Open Gateway initiative, with operators in **Nigeria, South Africa, Kenya, Egypt, Morocco and Cameroon** actively piloting or commercialising network APIs such as SIM Swap and Number Verification, allowing banks, governments and enterprises to authenticate users using real-time network intelligence.

Regulators also intensified efforts to strengthen digital identity governance. In **Nigeria**, the Nigerian Communications Commission (NCC) introduced the **Telecommunications Identity Risk Management System (TIRMS)** to help financial institutions, telecom operators and regulators detect SIM swaps, recycled numbers and other identity-related risks before they result in fraud. In **South Africa**, the government initiated a review of SIM registration and RICA enforcement as part of broader efforts to strengthen national security and digital trust.

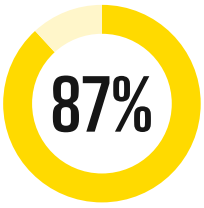
Meanwhile, fraud continued to evolve. According to TransUnion's H1 2026 fraud update, overall suspected digital fraud across monitored African markets declined to **2.6%**, yet attacks became significantly more sophisticated, increasingly targeting identity rather than transactions through account takeover, impersonation and social engineering. Complementing this trend, the GSMA reported that



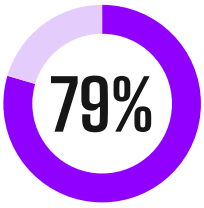
Identity Fraud



Social Engineering



Insider Fraud



SIM Swap Fraud

were the most prevalent fraud typologies affecting mobile money providers globally, with direct implications for Africa's rapidly expanding digital financial ecosystem.

Together, these developments point to a structural shift in Africa's digital economy. Identity is no longer viewed solely as a compliance requirement for onboarding customers; it is increasingly being treated as critical infrastructure for securing digital payments, protecting telecom networks, enabling remote government services and building trust across the continent's digital economy.

Five developments that defined Africa's Digital Trust landscape in 2026

1. Identity became Africa's newest trust infrastructure

Identity verification has emerged as a strategic capability across Africa throughout 2026. Ten African operator groups joined the GSMA Open Gateway initiative, with operators in Nigeria, Kenya, South Africa, Egypt, Morocco and Cameroon piloting APIs such as Number Verification and SIM Swap. These services allow banks, governments and enterprises to authenticate users using real-time network intelligence instead of passwords or SMS OTPs.

> **Key takeaway:** Telecom operators are evolving from connectivity providers into identity providers, creating new opportunities for fraud prevention and trusted digital services. For example, a bank can now verify a customer's mobile number directly through telecom network intelligence before approving a high-risk transaction, reducing reliance on passwords and security questions.

2. SIM registration became a national security priority

SIM registration moved beyond subscriber compliance as regulators increasingly recognised mobile numbers as critical identity credentials. Nigeria introduced the Telecommunications Identity Risk Management System (TIRMS) to monitor SIM lifecycle events and proposed a 14-day SIM churn notification period, while South Africa launched a review of RICA and SIM registration processes to strengthen national security and combat organised crime.

> **Key takeaway:** Protecting SIM integrity is becoming essential for secure banking, digital government and mobile financial services. For example, a financial institution can detect whether a customer's mobile number was recently swapped, recycled or deactivated before authorising sensitive account changes.

3. Identity fraud overtook transaction fraud

Fraud became increasingly identity-centric during H1 2026. TransUnion reported a 2.6% suspected digital fraud rate across monitored African markets, while the GSMA found that 90% of mobile money providers identified identity fraud as a leading threat, ahead of social engineering (88%), insider fraud (87%), and SIM swap fraud (79%).

Key takeaway: Organisations are shifting their focus from securing transactions to continuously verifying customer identity throughout the digital journey. For example, a fraudster using a synthetic identity may be stopped during onboarding through biometric and identity verification checks before ever gaining access to a digital service.

4. Governments accelerated digital public infrastructure

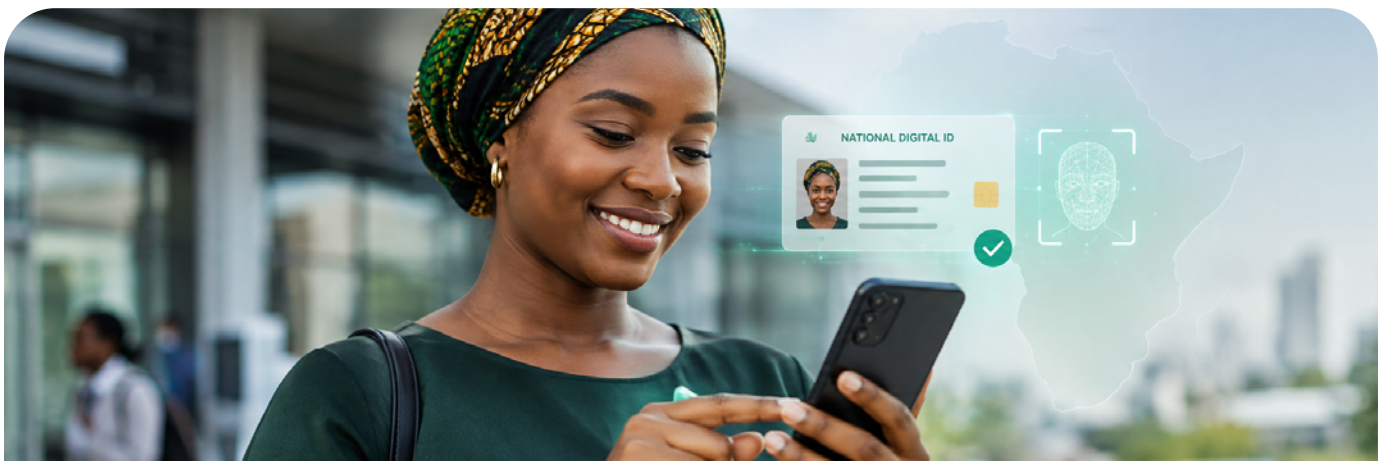
Governments continued investing in digital identity and citizen services across Africa. Nigeria enacted a new NIMC Act to strengthen its digital identity framework, while mobile technologies contributed an estimated US$240 billion, representing 7.8% of Africa's GDP, according to the GSMA. Digital identity increasingly underpins passport services, citizen verification and digital public service delivery.

Key takeaway: Digital identity is becoming foundational infrastructure for modern government services. For example, a citizen living abroad can renew a passport online using trusted digital identity verification rather than travelling to an embassy or government office.

5. Cross-sector collaboration became the new regulatory model

Regulators increasingly recognised that digital trust requires collaboration across industries. Telecommunications operators, financial institutions and governments expanded cooperation on identity verification, fraud prevention and authentication, supported by initiatives such as network identity APIs and Nigeria's TIRMS. Identity is no longer managed in sector-specific silos but as shared infrastructure.

Key takeaway: The future of digital trust depends on interoperable identity ecosystems rather than isolated compliance programmes. For example, telecom operators, banks and government agencies can increasingly rely on the same identity signals to verify users and reduce fraud across multiple services.



1.2. Trust Pulse

Africa Digital Trust Index - 2026 So Far

Indicator	Status	Trend	Executive Assessment
Telecom Identity Assurance	🟡 Moderate	↑ Improving	Operators are strengthening SIM lifecycle management and exposing network identity APIs to enterprise customers. (GSMA)
SIM Registration Integrity	🟡 Improving	↑	Regulators increasingly view SIM registration as critical national infrastructure rather than administrative compliance. (TechAfrica News)
Identity-Based Fraud	🔴 High	↑	Identity fraud, account takeover and social engineering have overtaken traditional transaction fraud as primary threats. (TransUnion Africa)
Mobile Money Trust	🟡 Stable	↑	Fraud controls continue improving, but identity verification remains the industry's biggest challenge. (GSMA)
Insurance Digital Maturity	🟡 Moderate	↑	Insurers continue digitising onboarding and claims processes, creating greater demand for trusted identity verification. (Industry direction; comprehensive pan-African datasets remain limited.)
Digital Government Readiness	🟢 Accelerating	↑	Governments expanded investment in national identity systems and remote digital public services. (State House)
Passport Digitisation	🟢 Improving	↑	Governments continued expanding digital passport renewal and remote identity verification capabilities for citizens, including diaspora populations. (Reliable Africa-wide metrics remain limited; national initiatives continue to expand.)
Regulatory Activity	🔴 Very High	↑	Telecommunications, financial services and identity regulators increased joint enforcement and regulatory coordination. (Mondaq)
AI-enabled Identity Threats	🟡 Emerging	↑	AI is accelerating impersonation, phishing and synthetic identity attacks, increasing demand for network-based and biometric verification. (GSMA)

Section 2 – Why Did It Happen?

2.1. The forces reshaping digital trust across Africa

The developments observed so far in 2026 are part of a broader transformation taking place across Africa's digital economy. As governments digitise public services, financial institutions expand digital channels, and telecom operators evolve into providers of digital identity services, the ability to establish trust online has become a strategic priority.

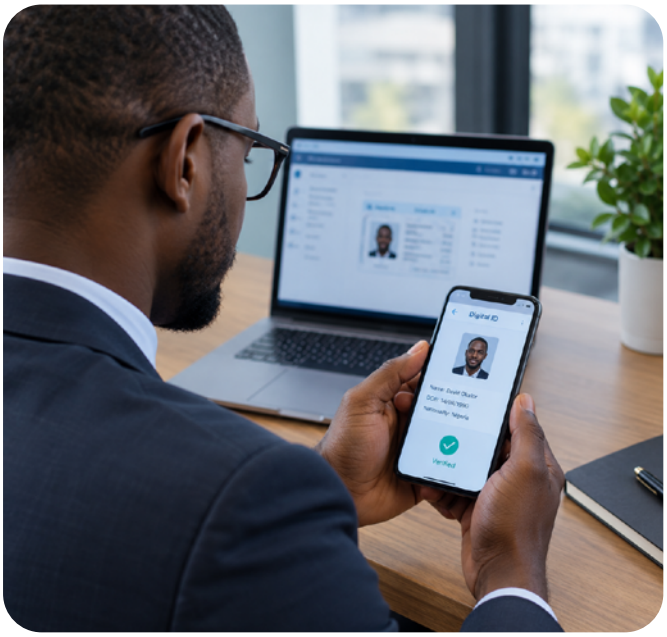
Four interconnected forces are accelerating this shift.



Digital services have outgrown traditional identity verification

Africa's digital economy continues to expand through mobile money, digital banking, online government services and remote customer onboarding. While this growth has improved access to essential services, it has also exposed the limitations of traditional identity verification methods such as passwords, SMS OTPs and manual document checks.

Organisations are increasingly investing in biometric verification, network intelligence and continuous identity assurance to support secure digital interactions at scale.



Identity is becoming the foundation of every regulated industry

Identity is no longer confined to customer onboarding. It now underpins payment authentication, SIM registration, insurance onboarding, passport services and access to government platforms.

As organisations increasingly rely on the same identity signals to deliver services, trust is becoming a shared responsibility across telecommunications, financial services, insurance and government rather than being managed independently within each sector.



Fraud is becoming more sophisticated and prevention-focused

The rapid adoption of AI, social engineering and synthetic identity techniques has changed how fraud occurs. Rather than targeting transactions alone, attackers increasingly exploit weaknesses in identity verification, customer onboarding and authentication.

This shift is driving organisations to invest in proactive fraud prevention and real-time identity intelligence that reduce risk before transactions occur.



Regulation is increasingly focused on digital resilience

Across Africa, regulators are moving beyond traditional compliance requirements toward building more resilient digital ecosystems. New policies increasingly emphasise identity assurance, interoperability, data quality and cross-sector collaboration to support secure digital transformation.

Section 3 – Where Is This Happening?

Digital trust transformation across key sectors

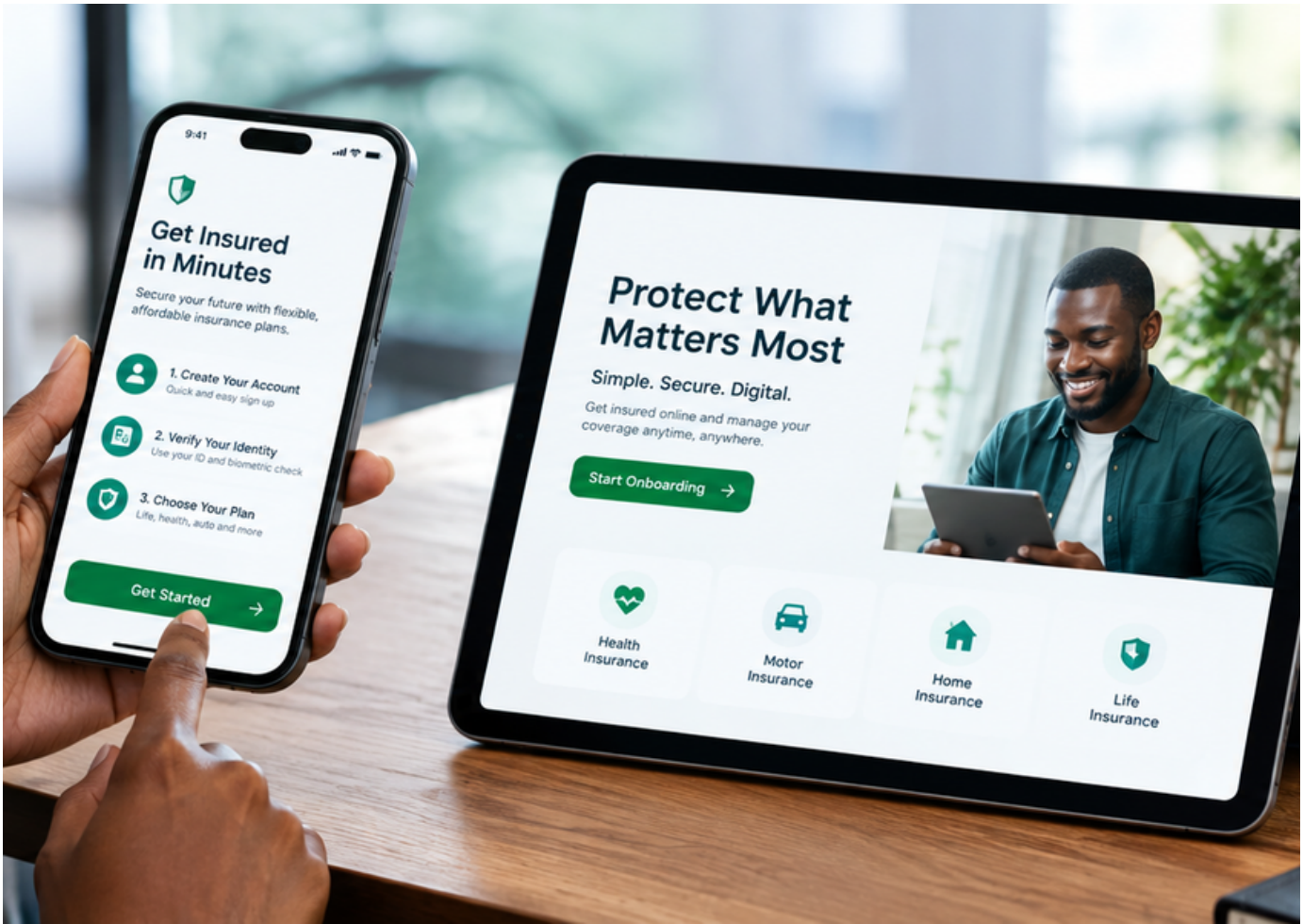
Telecommunications operators are commercialising network identity services, financial institutions are strengthening authentication to combat identity-led fraud, insurers are digitising customer verification, and governments are embedding digital identity into public service delivery.

3.1. Insurance

Digital onboarding is reshaping insurance operations

What's happening

Across Africa, insurers continue digitising customer onboarding and claims processing as part of broader digital transformation programmes. While H1 2026 did not produce a single defining regulatory event comparable to telecoms, the direction of travel is clear: insurers are increasing investment in digital identity verification, remote onboarding and fraud prevention to improve customer experience and reduce operational risk. This mirrors wider financial services trends toward stronger identity assurance. For instance: A customer purchases insurance through a digital channel. Instead of relying solely on manually submitted documents, the insurer verifies the applicant's identity against trusted identity records before issuing coverage, reducing onboarding risk and improving fraud detection.



3.2. Telecommunications

Telecom operators are becoming digital identity providers

What's happening

Africa's telecommunications sector is evolving beyond connectivity into a provider of trusted identity services. By the end of 2025, **10 African operator groups** had adopted the **GSMA Open Gateway** initiative, joining a global ecosystem of **79 operators representing approximately 80% of mobile connections worldwide.** Operators in **South Africa, Nigeria, Kenya, Egypt, Morocco and Cameroon** are piloting or commercialising APIs such as **Number Verification** and **SIM Swap**, enabling enterprises to verify identities using real-time network intelligence.

Evidence

Indicator	2026 So Far
African operator groups adopting GSMA Open Gateway	**10**
Global operators participating	**79**
Global mobile market covered	**~80%**
African countries actively commercialising APIs	**6**

Telecom operators are creating a new category of digital infrastructure by exposing trusted network signals that support fraud prevention, authentication and digital identity verification across multiple industries. For instance: If a bank receives a request to reset a customer's credentials. Before approving the request, it checks whether the customer's mobile number was recently swapped. If a SIM swap is detected, additional verification is triggered before access is restored.



3.3. Payments

Identity is becoming the first layer of fraud prevention

What's happening

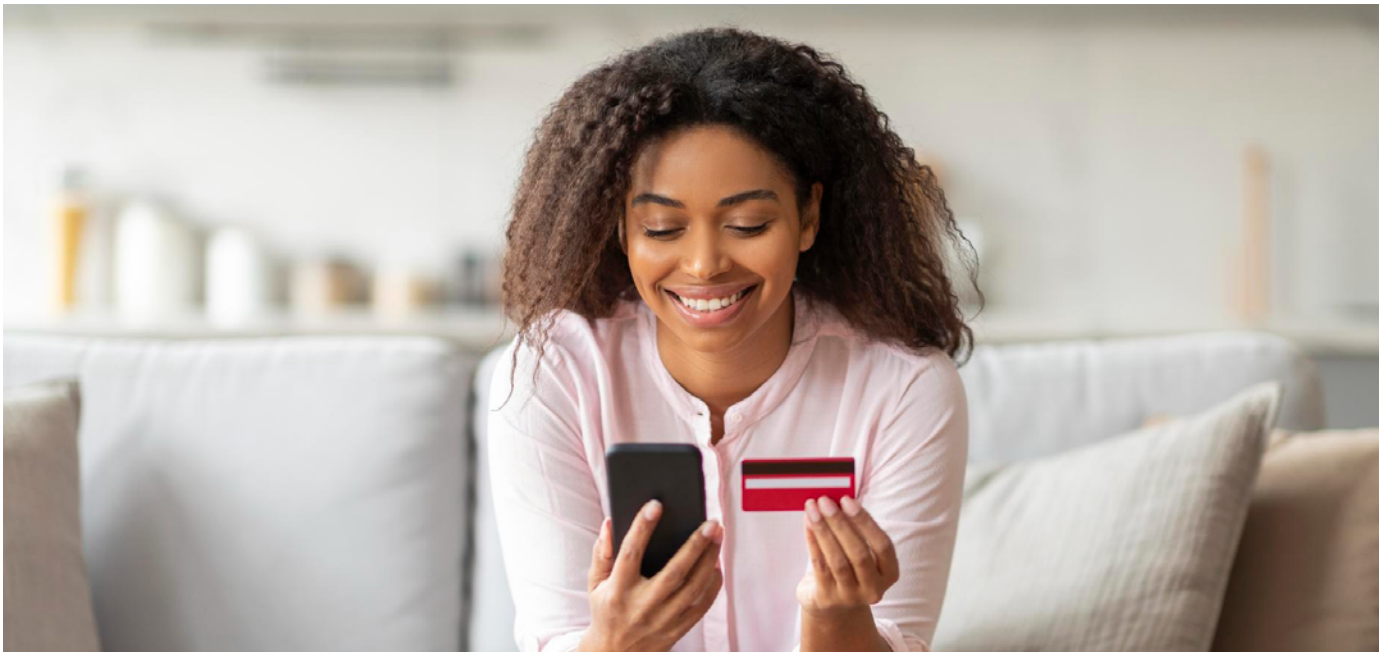
Financial institutions are increasingly integrating telecom identity signals into fraud prevention as mobile numbers become critical identifiers for banking, mobile money and digital payments. Nigeria's proposed **Telecommunications Identity Risk Management System (TIRMS)** enables banks and regulated institutions to verify whether a mobile number has been swapped, recycled, churned or barred before authorising high-risk transactions.

At the same time, identity-led attacks continue to dominate. The GSMA reports that **90% of mobile money providers** identified identity fraud as a major threat, followed by **social engineering (88%), insider fraud (87%) and SIM swap fraud (79%)**.

Evidence

Indicator	2026 So Far
Mobile money providers citing identity fraud	**90%**
Reporting social engineering	**88%**
Reporting insider fraud	**87%**
Reporting SIM swap fraud	**79%**

Trust in action: A fraudster gains access to a customer's banking credentials and attempts to initiate a high-value transfer. The transaction appears legitimate, but a real-time check reveals that the customer's mobile number was recently recycled. The transfer is flagged for review before funds leave the account.



3.4. Government

Digital identity is becoming public infrastructure

What's happening

Governments across Africa have continued investing in **Digital Public Infrastructure (DPI)** throughout 2026, placing digital identity at the centre of public service delivery. In **Benin**, the government expanded **ePass**, enabling citizens in **80+ countries** to renew their passports online without visiting an embassy. The country also strengthened its national identity programme, with **7.7 million citizens enrolled** and **6.1 million digital identity certificates issued**. Meanwhile, **Nigeria** strengthened its digital identity framework through reforms to the National Identity Management Commission (NIMC), while several African governments accelerated investments in digital identity and citizen authentication. These developments reflect a broader continental shift towards secure, digital-first government services.

Evidence

Indicator	2026 So Far
Countries supported by Benin ePass	**80+**
Beninese enrolled in national digital identity programme	**7.7 million**
Digital identity certificates issued	**6.1 million**
Mobile economy contribution to Africa	**US$240 billion (7.8% of GDP)**

Trust in action: Before digital passport services, a Beninese citizen living in Paris or Toronto might have needed to travel to an embassy, take time off work and wait weeks to begin a passport renewal. Today, the same process can be initiated online, demonstrating how digital identity infrastructure is making government services more accessible to citizens wherever they live.



3.5. Seamfix: Building Africa's Trust Infrastructure

The developments highlighted throughout this report point to a common challenge facing governments, financial institutions, telecom operators and insurers: the need to establish trusted digital interactions at scale.

While the specific use cases vary by industry, the underlying requirements remain consistent:

Trusted identity verification	Secure digital onboarding	Fraud prevention
Regulatory compliance	Digital service delivery	Interoperable trust infrastructure

Seamfix works with governments, telecom operators, financial institutions and regulated industries across Africa to help build these capabilities through identity, compliance and digital public infrastructure solutions.

Seamfix Trust Portfolio

Solution	Industry Focus	Key Capability
BioSmart X	Telecommunications	Trusted subscriber registration, identity verification and SIM lifecycle integrity
RegSmart	Telecommunications & Regulators	Compliance monitoring, regulatory intelligence and subscriber risk visibility
InsureGov	Insurance Ecosystem	National insurance identity, policyholder verification and ecosystem transparency
ePass	Government & Diaspora Services	Digital passport renewal and citizen service delivery

Section 4 – What's Happening Next?

4.1. Technology Watch

Technologies reshaping digital trust

Technology	Why it's important	Adoption Signal	Industries Impacted
Network APIs	Real-time identity verification through telecom networks	GSMA Open Gateway expanding across Africa	Telecom, Banking, Government
AI-powered Fraud Detection	Detects behavioural anomalies and identity fraud	Rapid adoption by banks and fintechs	Banking, Insurance
Network APIs	Real-time identity verification through telecom networks	GSMA Open Gateway expanding across Africa	Telecom, Banking, Government
Biometric Authentication	Reduces reliance on passwords and OTPs	Increasing government and telecom deployments	Government, Telecom
Digital Identity Wallets	Gives citizens control of verified credentials	Early pilots globally, expected African adoption	Government, Financial Services
Verifiable Credentials	Enables trusted digital document verification	Growing W3C ecosystem	Government, Education
Continuous Identity Verification	Verifies users throughout a session instead of only at login	Emerging enterprise capability	All regulated industries

Technology Outlook

Organisations will increasingly combine multiple trust signals, biometrics, mobile network intelligence, behavioural analytics and government-issued digital identities, to build adaptive identity assurance rather than relying on single authentication methods.

4.2. Country Spotlight

Markets to Watch

The countries shaping Africa's digital trust landscape

Country	Why It Matters	2026 Highlights	2027 Outlook
Benin	Digital Public Infrastructure	Continued expansion of ePass for diaspora passport renewals across 80+ countries; national digital identity programme surpassed 7.7 million enrolments.	Expansion of digital identity into additional government services.
Nigeria	Telecom Identity & Financial Trust	Introduction of TIRMS, continued NIN ecosystem reforms, stronger collaboration between telecom and financial regulators, rapid fraud prevention innovation.	Greater adoption of network identity intelligence by banks, fintechs & government agencies.
Kenya	Digital Identity & Mobile Money	Continued enhancement of the Maisha Namba digital identity programme alongside the world's most mature mobile money ecosystem.	Deeper integration of digital identity with financial and public services.
South Africa	Digital Identity Policy	Progress on the national Digital Identity framework, review of SIM registration and RICA enforcement, increasing focus on digital fraud.	Formalisation of digital identity policy and stronger identity assurance standards.
Rwanda	Digital Government	Continued investment in e-government platforms, digital citizen services and regional digital transformation initiatives.	Expansion of digital public services supported by trusted digital identity.
Ghana	National Identity & Financial Inclusion	Continued adoption of the Ghana Card across banking and public services, strengthening identity verification for regulated sectors.	Increased use of national identity infrastructure for digital onboarding and service delivery.
Morocco	Telecom Innovation	Active participation in GSMA Open Gateway initiatives and continued investment in digital transformation and identity-enabled services.	Expansion of network APIs and enterprise identity services.

Country	Why It Matters	H1 2026 Highlights	H2 Outlook
Egypt	Digital Economy	Ongoing investment in Digital Egypt initiatives, digital government and trusted digital services for citizens and businesses.	Growth in digital public infrastructure and digital identity adoption.
Côte d'Ivoire	Regional Digital Growth	Continued expansion of digital financial services and government digitisation programmes within Francophone West Africa.	Greater investment in digital identity and secure digital service delivery.
Ethiopia	National Digital ID	Continued rollout of the Fayda digital ID programme as part of broader Digital Ethiopia reforms.	Increased integration of digital identity into financial inclusion and public services.

4.3. Looking Ahead

Five developments to watch during H2 2026 and 2027

1

Identity APIs will move into mainstream enterprise adoption
Expect more banks, insurers and government agencies to adopt telecom identity services for customer verification.

2

AI-driven fraud will increase
Deepfakes, synthetic identities and AI-assisted phishing are expected to place greater pressure on existing authentication methods.

3

Governments will expand digital public infrastructure
National identity programmes will increasingly become platforms for passport services, healthcare, taxation and social protection.

4

Cross-sector regulation will continue growing
Expect closer collaboration between telecom, financial and identity regulators.

5

Trust will become a competitive differentiator
Organisations with stronger identity assurance will onboard customers faster, reduce fraud losses and deliver better digital experiences.

Trend	Likelihood	Expected Impact
AI identity fraud increases	High	High
Network APIs become mainstream	High	High
Digital identity expansion	High	High
Digital insurance onboarding	Medium	Medium
Digital passport services expand	Medium	High
Biometric authentication adoption	High	High
Continuous identity verification	Medium	High
Cross-border digital identity initiatives	Medium	High



Section 5 – What Should Leaders Do?

5.1. Key Priorities and Actions for H2 2026 and 2027

The first half of 2026 highlighted a clear shift in Africa's digital trust landscape. The second half will be defined by how quickly organisations adapt to changing regulations, evolving fraud patterns and growing demand for trusted digital services. Leaders should monitor the following developments while strengthening their own digital trust strategies.

Timeline	What to Watch	Why It Matters
Q4 2026	GSMA Open Gateway expansion across Africa	More telecom operators are expected to commercialise network identity APIs, creating new opportunities for fraud prevention and identity verification.
Q4 2026	Digital identity and SIM registration reforms	Governments and regulators are expected to continue strengthening digital identity governance & subscriber verification frameworks.
Q4 2026	Digital identity and SIM registration reforms	Governments and regulators are expected to continue strengthening digital identity governance & subscriber verification frameworks.
Q4 2026 – 2027	Growth in AI-enabled fraud	Organisations should prepare for increasing use of synthetic identities, deepfakes and AI-assisted social engineering.
Q4 2026 – 2027	Expansion of Digital Public Infrastructure initiatives	More governments are expected to integrate digital identity into public services, citizen authentication and financial inclusion programmes.
Throughout 2027	Cross-sector regulatory collaboration	Expect stronger cooperation between telecom, financial, insurance and identity regulators across multiple African markets.

5.2. Key Actions

For Telecommunications Operators

- Accelerate deployment of network identity capabilities such as Number Verification and SIM Swap APIs.
- Strengthen SIM lifecycle management to reduce identity fraud and improve enterprise trust.
- Build stronger partnerships with banks, fintechs and government agencies around trusted identity services.

For Financial Institutions & Payment Providers

- Shift fraud strategies from transaction monitoring to continuous identity assurance.
- Incorporate telecom network intelligence into high-risk authentication journeys.
- Review customer authentication methods in preparation for AI-driven fraud threats.

For Insurance Providers

- Strengthen identity verification during onboarding and claims processing.
- Integrate national identity and biometric verification where regulatory frameworks permit.
- Improve fraud analytics by combining identity, behavioural and transactional signals.

For Governments & Regulators

- Continue investing in interoperable Digital Public Infrastructure.
- Strengthen collaboration between telecom, financial and identity regulators.
- Expand secure digital services that reduce reliance on in-person verification while maintaining citizen trust.

For Technology & Compliance Leaders

- Assess whether existing identity controls are sufficient for AI-enabled fraud.
- Develop a roadmap for adopting continuous identity verification and risk-based authentication.
- Align digital trust strategies with emerging regulatory expectations and cross-sector identity standards.

5.3. Digital Trust Maturity Checklist

Is your organisation ready?

Question	Yes	No
Do we verify identity beyond passwords and OTPs?		
Can we detect SIM swaps or compromised mobile identities?		
Are identity checks integrated across all digital channels?		
Are we prepared for AI-driven identity fraud?		
Does our identity strategy align with emerging regulatory expectations?		
Do we leverage trusted national or telecom identity ecosystems where appropriate?		

Organisations that answer "No" to three or more questions should consider digital trust a strategic priority over the next 12 months.

Conclusion

The organisations that will lead Africa's digital economy over the next five years are unlikely to be those with the most digital services, but those with the most trusted digital services. As digital identity becomes the common foundation across telecommunications, financial services, insurance and government, competitive advantage will increasingly depend on an organisation's ability to establish trust at every stage of the digital journey. Those that invest early in interoperable identity, proactive fraud prevention and resilient digital infrastructure will be better positioned to navigate evolving regulation, reduce operational risk and deliver secure digital experiences at scale.

About Seamfix

Seamfix is an African technology company building trust infrastructure for governments, financial institutions, telecom operators and regulated industries.

Our solutions help organisations verify identities, deliver digital services, strengthen compliance and reduce fraud across critical sectors of the economy.

Today, Seamfix technologies support initiatives spanning:

- ✓ Digital public infrastructure
- ✓ National identity programmes
- ✓ Passport and citizen services
- ✓ Telecom subscriber management
- ✓ Insurance ecosystem modernisation
- ✓ Financial transaction assurance
- ✓ Regulatory technology and compliance

Operating across multiple African markets, Seamfix works with public and private sector organisations to create trusted digital experiences that enable secure growth and digital transformation. Contact us to learn more.