THOUGHT LEADERSHIP PAPER

THE BANKING ASSOCIATION SOUTH AFRICA

From Identity to Interoperability:

Understanding the Role of Digital ID in Cross-Border Financial Services

A conceptual guide to identification systems, digital identity and reusable KYC in support of African regional integration

- Trusted Identity
- Interoperable Systems
- Reusable KYC
- Regional Integration and Inclusion

CONNECTING INSIGHTS, INDUSTRY AND IMPACT

Contents

	Foreword	3
	Executive summary	4
01	The missing layer of regional integration	5
02	Identity is the starting point	6
03	Not all ID systems serve the same purpose	7
04	The building blocks of trusted identity	8
05	Why having an ID is not enough	9
06	From identity to reusable KYC	10
07	When KYC becomes a trade facilitation issue	12
08	Identity as an enabling layer of regional integration	13
09	Key considerations for advancing reusable KYC	13
10	Conclusion	14
	References	14

Foreword

Africa's ambition to deepen regional integration and expand intra-African trade depends not only on the movement of goods, services and capital, but also on the ability to establish trust across borders. For financial institutions, knowing who a customer is - remains fundamental to maintaining the integrity of the financial system. Yet increasingly digital and cross-border financial activity is exposing the limitations of fragmented identification systems, regulatory frameworks and KYC processes.

The challenge is therefore not whether KYC should be strengthened, but how it can be made more secure, effective, proportionate and reusable. Digital identity has an important role to play in this evolution, but technology alone cannot deliver interoperability. Progress requires greater alignment across legal and regulatory frameworks, identity systems, data governance and standards, supported by confidence that information exchanged across borders is trusted, secure and appropriately governed.

This is particularly important as the African Continental Free Trade Area (AfCFTA) seeks to reduce barriers to cross-border economic activity. More efficient and trusted approaches to customer identification and verification can help reduce friction in financial services while supporting financial integrity, inclusion and legitimate economic activity.

This paper contributes to that conversation by examining the relationship between digital identity, KYC and interoperability, and considering the opportunities and policy considerations for cross-border financial services in Africa. It is intended to support informed dialogue among industry, policymakers and regulators as we work towards a more integrated, trusted and digitally enabled African financial system.

Bongi Kunene

Managing Director

Banking Association of South Africa

Executive Summary

Africa's ambitions for deeper financial integration, digital trade and cross-border commerce depend not only on connected payment systems and harmonised trade rules but also on the ability of institutions to establish and trust who they are dealing with. As businesses and customers move across institutional and national boundaries, identity becomes a critical enabling layer for financial services, regulatory compliance and regional trade facilitation.

The report highlights an important distinction between having a recognised identity and having an identity that can be digitally verified, authenticated, trusted and reused across institutions and jurisdictions. While foundational identification systems provide the basis for legal identity, they do not automatically create the digital, legal and governance arrangements required for interoperable KYC.

For financial institutions, this gap has practical implications. Fragmented KYC processes can result in repeated verification, manual documentation, delays and increased compliance costs for customers and businesses seeking access to banking, payments, trade finance and other cross-border financial services. For smaller businesses in particular, these frictions can constrain participation in regional trade.

The central argument is that reusable KYC requires more than digital identity alone. It depends on trusted data sources, appropriate consent mechanisms, risk-based assurance, regulatory recognition, interoperability standards and governance arrangements that give institutions confidence to rely on verified identity information across borders.

The opportunity, therefore, is not to replace national identity systems or remove the customer-due-diligence responsibilities of financial institutions. Rather, it is to create trusted mechanisms through which verified identity information can be securely accessed, appropriately recognised and relied upon across authorised institutions and jurisdictions. In this way, digital identity and reusable KYC can support Africa's broader objectives for financial integration, cross-border payments and regional trade.

1. The Missing Layer of Regional Integration

As Africa becomes more digitally and economically interconnected, how can institutions establish with confidence who they are dealing with when customers, businesses and transactions move across institutional and national boundaries?

Regional integration increasingly depends on digital systems that enable people, businesses and institutions to transact across organisational and national boundaries. Yet beneath payments, digital trade platforms and cross-border financial services, lies a fundamental requirement: the ability to establish and trust who is participating in those systems.

This paper provides a practical introduction to the relationship between identification systems, digital identity, authentication, KYC and interoperability and explains why trusted and reusable identity infrastructure is becoming an important foundation for cross-border financial services and regional trade.

The expansion of digital financial services and the ambitions of the African Continental Free Trade Area (AfCFTA) are contributing to an increasingly inter-connected African economy. Businesses are trading across borders, individuals are accessing financial services through digital channels, and banks and financial technology companies are expanding into neighbouring markets.

Yet greater financial connectivity depends on something that is often taken for granted: the ability to establish with confidence **who a customer is**. Within the Financial Action Task Force (FATF) framework for combating money laundering and terrorist financing, customer due diligence (CDD) - commonly implemented by financial institutions through Know Your Customer (KYC) processes - is a fundamental component of an effective anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

Banks are required to identify and verify their customers, understand beneficial ownership and, using a risk-based approach, assess and manage the risks associated with customer relationships. These processes are essential to protecting the integrity of the financial system and combating money laundering, terrorist financing, fraud and other forms of financial crime.

However, while financial activity is becoming increasingly digital and cross-border, KYC remains largely organised around institutional and national boundaries. A customer verified by one bank may still have to undergo another verification process when opening an account with a second bank. Similarly, a business that has already established its identity and ownership in its home country may be required to provide substantially the same information when seeking banking or trade-finance services in another African jurisdiction.

A digital identity recognised by financial institutions in one country may also not automatically be recognised elsewhere. This creates an important distinction between having an identity and having an identity that can be trusted and reused.

2. Identity is the Starting Point

The starting point for addressing this challenge is the foundational identification infrastructure on which many other identity and verification systems depend. According to the World Bank's Identification for Development (ID4D) framework, a foundational identification system is designed to manage identity information for the general population and provide credentials that can be used as proof of identity across a wide range of public and private sector transactions.

Foundational identification infrastructure can take different forms, including civil registration systems, which record vital events such as births, marriages and deaths; population registers, which maintain records of residents or citizens; and national identification systems, which record personal information, assign unique identification numbers and issue credentials that can be used to establish a person's legal identity. Together, these systems can provide an authoritative source of basic identity information against which other institutions - including financial institutions - can verify a customer's identity.

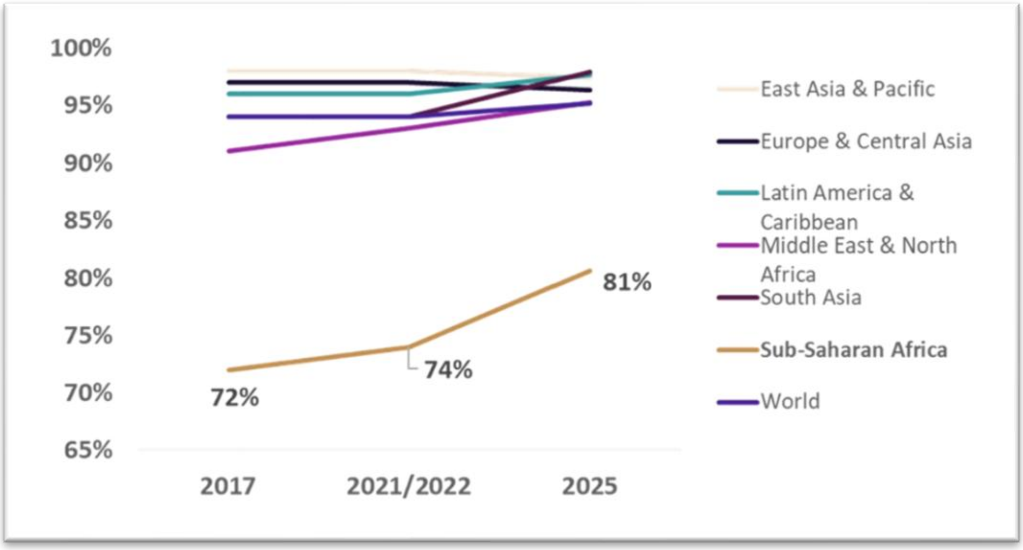
The latest data from the World Bank's ID4D Global Findex Database of 2025 illustrates both the progress that has been made in expanding access to this foundational identification infrastructure and the scale of the challenge that remains.

According to the latest World Bank ID4D data (see Figure 1), approximately 81% of adults in Sub-Saharan Africa have an official form of identification. While this represents substantial overall coverage, it is the lowest level of identification coverage among all major world regions. By comparison, coverage in East Asia and the Pacific, Europe and Central Asia, Latin America and the Caribbean, the Middle East and North Africa, and South Asia is close to or above 95%. The remaining identification gap in Sub-Saharan Africa therefore remains disproportionately large, with nearly one in five adults potentially excluded from the benefits of a recognised form of identification.

The World Bank's broader analysis also shows that access to a recognised identity does not necessarily translate into access to a government-recognised digital identity that can be used securely for online transactions.

Figure 1. Sub-Saharan Africa lags other regions for ID coverage

Adults with ID, by region (%)



Source: World Bank Identification for Development, (2025)

Understanding the nature of this identification gap also requires distinguishing between the different types of identity systems through which individuals may establish and prove their identity.

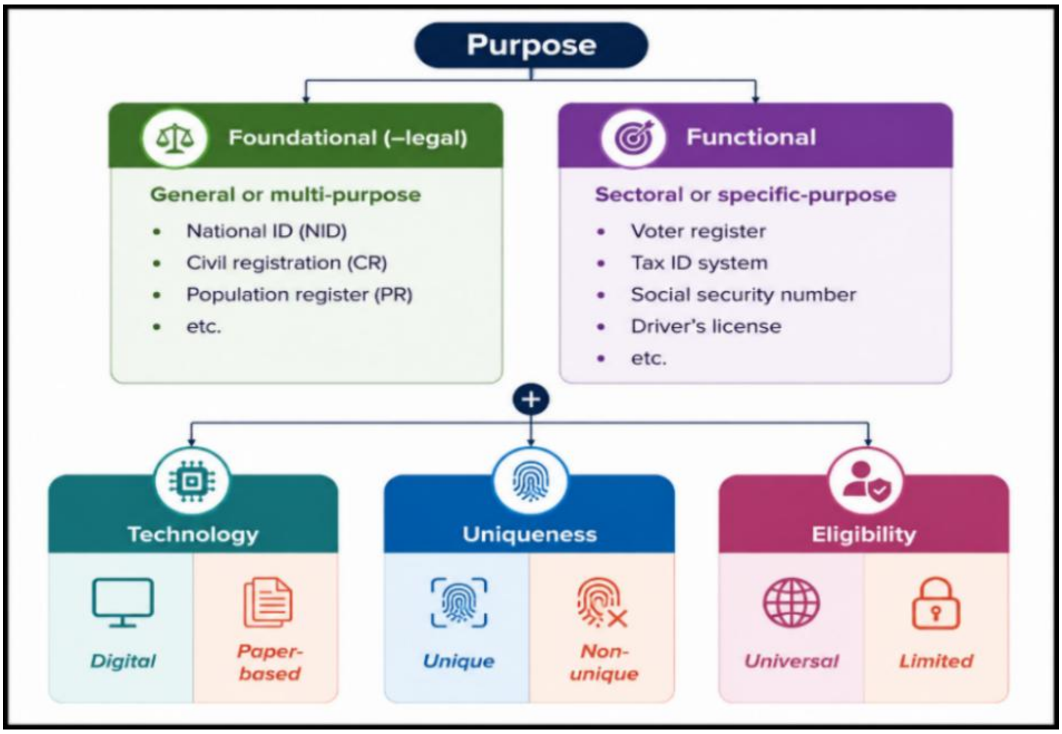
Key message: A recognised identity is the starting point for verification, authentication and the broader use of identity across service.

3. Not All ID Systems Serve the Same Purpose

Government identification systems are not all designed for the same purpose. A useful starting point is to distinguish between foundational and functional identification systems (see Figure 2).

Foundational identification systems are generally designed to establish and manage the identity of the population and to provide credentials that can be used as proof of identity across a range of public and private sector transactions. Functional identification systems, by contrast, are established primarily to support a specific programme, service or administrative purpose, such as taxation, voting, social protection or healthcare.

Figure 2: Classification of government ID systems



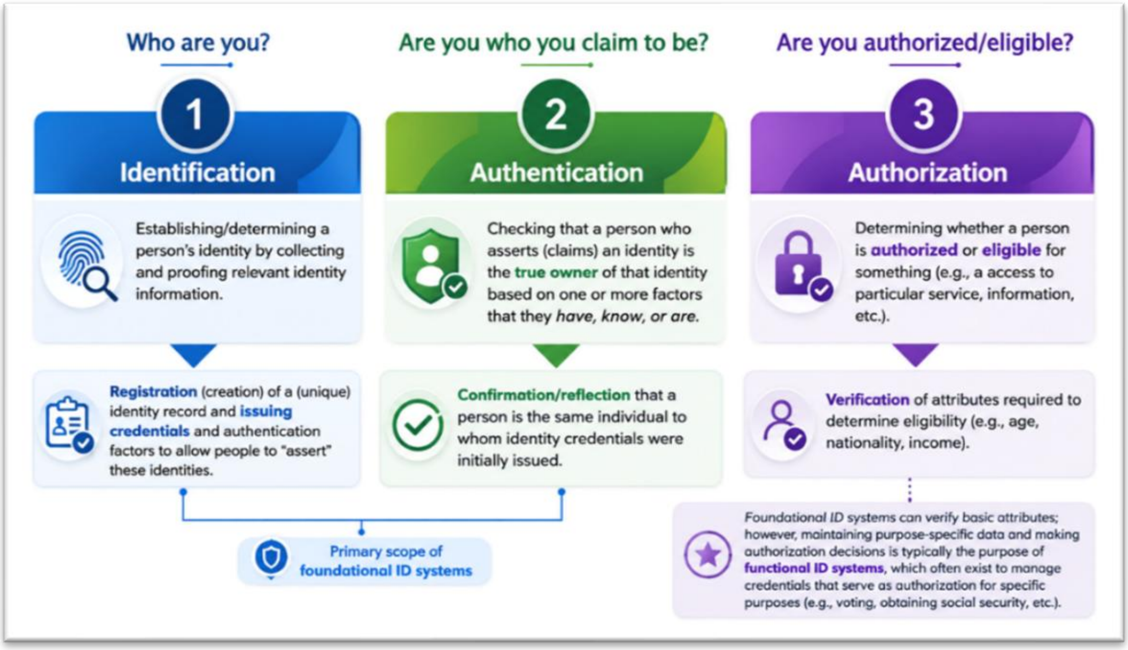
Source: World Bank Group Practitioners Guide (2019)

While functional systems may also verify or record aspects of an individual's identity, their use is generally linked to the function for which they were created. The distinction is particularly relevant in financial services, where institutions increasingly require identity infrastructure that can support verification across multiple services, institutions and, potentially, jurisdictions.

4. The Building Blocks of Trusted Identity

An identification system does more than issue a credential. It creates a mechanism through which an individual can establish who they are and, subsequently, prove that identity to institutions that need to rely on it. Beyond their purpose and scope, it is also important to consider the basic role of an identification system. ID systems collect and validate information about an individual in order to establish their identity and provide a means of proving that identity, typically through a credential such as a unique identification number, card, certificate or mobile ID. The credential allows an individual to assert their identity to a third party, or "relying party", such as a government agency, financial institution or employer, that requires assurance of who the individual is. In this context, ID systems perform three related but distinct functions: identification, authentication and authorization as outlined in Figure 3.

Figure 3: The basic roles of ID systems



Source: World Bank Group Practitioner's Guide (2019)

Identification establishes or determines who a person is by collecting and validating relevant identity information**. Authentication** confirms that the person presenting or asserting an identity is the legitimate holder of that identity, typically through one or more authentication factors. **Authorization** determines whether an identified and authenticated person is permitted or eligible to access a particular service, information or transaction.

These functions are complementary, but establishing an identity does not confirm that the person presenting it is the legitimate identity holder or that the person is authorised to undertake a particular activity.

5. Why Having an ID Is Not Enough

Possessing a government-recognised identity credential does not necessarily mean that the identity can be verified electronically, authenticated remotely or accessed by authorised institutions. Nor does it mean that identity information can be recognised across different institutions or national jurisdictions. A country may therefore have a relatively well-established foundational ID system without necessarily having created the infrastructure, legal arrangements or trust mechanisms required for digital interoperability and cross-border reliance.

For financial services, the distinction is critical. The challenge is not simply whether a customer possesses an identity document, but whether that identity can be reliably verified, authenticated and, where appropriate, relied upon by authorised institutions. KYC processes require financial institutions to establish confidence that a customer is who they claim to be and, where relevant, determine whether the customer is permitted to access a particular service.

In a digital environment, this requires more than the existence of a government-issued identity credential. Identity information must be capable of being electronically verified, the identity holder authenticated, and the resulting assurance relied upon by authorised institutions.

Where financial services extend across borders, the challenge becomes more complex as identity credentials, verification mechanisms and the legal basis for relying on identity information may differ across jurisdictions. Interoperable KYC therefore depends not only on the availability of foundational identification, but on the ability of authorised institutions to securely access, recognise and trust identity information across institutional and national boundaries.

The World Bank's recent analysis reinforces this point by highlighting that progress in identification must extend beyond coverage to ensure that identity systems are practical and broadly usable for accessing services.

6. From Identity to Reusable KYC

The gap between possessing an identity and being able to use verified identity information across digital, institutional and national boundaries can be described as an **identity-to-KYC gap**.

The journey from identity to interoperable KYC can be understood as a progression of increasing capability and trust as explained in Figure 4.

Figure 4: From identify to reusable KYC

This progression highlights an important point that possessing an identity does not necessarily mean possessing an identity that can be digitally verified, trusted by another institution or appropriately reused across borders.

Digital identity does not automatically create interoperability, and interoperability does not automatically create reusable KYC. Each stage requires additional technical, legal, regulatory and governance arrangements to establish the trust necessary for another institution or jurisdiction to rely on the identity information.

7. When KYC Becomes a Trade Facilitation Issue

This identity-to-KYC gap becomes increasingly important as African financial integration deepens. A customer may possess a valid national identity credential but still face repeated verification when interacting with different financial institutions.

Likewise, a business may have already established its legal existence, ownership and authorised representatives in one jurisdiction, yet be required to reproduce much of the same information when seeking financial services elsewhere.

KYC has traditionally been viewed primarily through a compliance lens However, as cross-border financial activity expands, fragmented identity and KYC processes are becoming increasingly relevant to the broader objective of intra-African trade facilitation.

A business seeking to trade across borders may require access to a bank account, cross-border payments, foreign exchange, trade finance, guarantees or other financial services. Each of these relationships can require the business, its directors, authorised representatives and, where applicable, beneficial owners to be identified and verified.

Where identity and business information cannot easily be verified across jurisdictions, businesses may face additional documentation requirements, manual verification, delays and higher administrative costs.

These challenges can be particularly significant for smaller businesses, which generally have less capacity than large multinational corporations to absorb repeated compliance and administrative requirements.

The implication is that KYC interoperability should not be viewed solely as a banking-sector efficiency initiative. As Africa seeks to deepen financial integration and expand intra-African trade, the ability to establish and verify trusted identities may increasingly form part of the infrastructure that supports cross-border banking, payments and trade finance.

The AfCFTA's digital trade agenda reinforces this direction by placing greater emphasis on harmonised rules, common standards and interoperability. Trusted digital identity and reusable KYC can provide an important enabling layer beneath these broader ambitions, helping to reduce unnecessary friction while preserving the integrity of financial-crime controls.

Trade does not move without payments, finance and financial relationships. Increasingly, those relationships cannot be established without the ability to identify and verify the people and businesses behind them.

The question is therefore no longer simply whether African countries can establish reliable national KYC systems. The more strategic question is:

Can a verified identity be trusted and appropriately relied upon when a customer crosses an institutional or national border?

8. Identity as an Enabling Layer of Regional Integration

The implications extend beyond improving the efficiency of individual KYC processes. As Africa seeks to deepen financial integration, expand digital trade and increase intra-African commerce, trusted identity may increasingly become part of the infrastructure that enables these ambitions.

Payments can be connected across borders, digital platforms can be made interoperable and trade rules can be harmonised. Yet financial institutions must still be able to establish with sufficient confidence who the individuals and businesses participating in those systems are.

Where identity and verification processes remain fragmented, the benefits of wider digital and financial connectivity may be constrained by repeated checks, manual processes and the need to recreate trust each time a customer crosses an institutional or national boundary.

This does not mean that a single African identity system or a uniform KYC process is necessarily required. Rather, the emerging challenge is to create the conditions under which identity information and verification outcomes can be securely accessed, appropriately recognised and relied upon across authorised institutions, while remaining subject to applicable legal, regulatory and risk-based requirements.

The progression from foundational identification to digital identity, interoperable identity and reusable KYC therefore represents more than a technological evolution. It reflects a broader shift in how trust may need to operate in an increasingly interconnected African economy.

9. Key Considerations for Advancing Reusable KYC

The reusable KYC will require more than technology. It will need common standards, trusted data sources, appropriate consent mechanisms, legal recognition, supervisory confidence and governance arrangements that clarify responsibilities between identity providers, financial institutions, regulators and customers.

10. Conclusion

From this perspective, identity interoperability is not merely an issue of technology or compliance. It may increasingly become an enabling layer of Africa's financial integration and regional trade ambitions.

The opportunity is not to replace national identity systems or remove the risk-based responsibilities of financial institutions. Rather, it is to create trusted mechanisms through which verified identity information can be securely accessed, appropriately recognised and relied upon across institutions and jurisdictions. In this way, digital identity and reusable KYC can become part of the enabling infrastructure for Africa's financial integration, cross-border payments and regional trade ambitions.

References

- **African Union (AU) (2023).** *Interoperability Framework for Digital ID in Africa*. Addis Ababa: African Union. https://au.int/en/documents/20231211/au-interoperability-framework-digital-id
- **African Union (AU) (2024).** *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade*. Addis Ababa: African Union. https://au.int/en/treaties/protocol-agreement-establishing-african-continental-free-trade-area-digital-trade-0
- **Financial Action Task Force (FATF) (2020)**. *Guidance on Digital Identity*. Paris: FATF. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html
- **Financial Action Task Force (FATF) (2023).** *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*. Paris: FATF. https://www.gov.pl/attachment/6bb8d97c-960a-4261-bced-5cfb0717838e
- **United Nations Economic Commission for Africa (2023).** *Africa Digital Identity Landscape*. https://www.uneca.org/sites/default/files/DITE-AFRICA/Africa%20Digtial%20ID%20Landscape%20Report%20%282023%29.pdf
- **World Bank (2025).** *Global Progress in Identification:* Three Findings from the Latest Data. Identification for Development (ID4D) Blog. Ansar, Saniya;

Clark, Julia Michal; Wolff, Jorin Margaux.
http://documents.worldbank.org/curated/en/099061526195037307

- **World Bank Group (2025).** *The Global 2025 Findex Database. Connectivity and Financial Inclusion in the Digital Economy.* https://openknowledge.worldbank.org/bitstreams/9288bdc5-7a9b-42de-a47c-3746fd68f22a/download
- **World Bank Group (2025).** *The State of Identification Systems in Africa.* Washington, DC: World Bank. https://openknowledge.worldbank.org/entities/publication/8fba09d2-4a4f-5bbf-b210-b83a05c8f11c
- **World Bank Group (2017).** *The State of Identification Systems in Africa: Country Briefs.* http://documents.worldbank.org/curated/en/298651503551191964
- **World Bank Group (2019).** *Identification for Development Practitioners Guide.* http://documents.worldbank.org/curated/en/248371559325561562

From Identity to Interoperability: Understanding the Role of Digital ID in Cross-Border Financial Services

Editorial Team:

Pearl Masondo - Lead Researcher

Pinky Rabotapi - Head of Payments Division

Maxine Hlaba – Head of SADC Banking Association

banking.org.za

+27 11 645 6700

THE BANKING ASSOCIATION SOUTH AFRICA