Borderless Identity

The Implementation Gaps in AfCFTA's Digital Trade Protocol

DIAMOND ADVOCATES | Partner WONE GLOBAL

1. **Introduction: AfCFTA's Integration Promise**

The African Continental Free Trade Area (AfCFTA) was inaugurated in 2018 and has been operational since 2021. It represents Africa's most ambitious economic integration project, bringing together 54 countries into a single market of over 1.3 billion people and a combined GDP exceeding USD 3.4 trillion.

Its objective is to dismantle tariff barriers, facilitate the free movement of goods and services, stimulate industrialization, and reverse a history in which intra-African trade accounted for only about 16% of the continent's total trade, compared to far higher levels in Asia and Europe. While tariff reductions are underway and projections from UNECA suggest intra-African trade could increase by over 50% (or even double if non-tariff barriers are addressed) regulatory fragmentation continues to undermine the promise of seamless integration.

In a digital trade environment, fragmented national identity and verification systems risk operating as modern non-tariff barriers, increasing compliance costs and slowing cross-border financial and commercial activity. If AfCFTA is to move beyond tariff liberalization and truly function as a single market, it requires a legally grounded framework for interoperable digital identity that aligns regulatory systems as deliberately as it aligns trade policy.

Realizing this need, the AfCFTA Protocol on Digital Trade was adopted in February 2024. It represents a deliberate shift in how Africa approaches its digital economy.

The Protocol is a structural extension designed to support digitally enabled trade across the continent. By establishing common rules for digital trade, the Protocol aims to reduce fragmentation and enable more predictable cross-border digital transactions. In doing so, it positions digital infrastructure as a core driver of competitiveness and economic expansion.

Africa's digital economy is already evolving at speed. Mobile money ecosystems and fintech innovation across multiple jurisdictions are reshaping how value moves, how businesses operate, and how consumers engage in commerce. The Protocol responds to this momentum by introducing harmonized rules on issues such as personal data protection, cybersecurity, cross-border data transfers, and electronic commerce. Its objective is not merely regulatory alignment, but the creation of a secure, trusted, and interoperable digital trade environment across the continent.

The Digital Trade Protocol resolves the normative question of whether digital identity belongs within AfCFTA; the remaining question is whether Africa will implement interoperability in a manner that balances integration, sovereignty, and data protection without reproducing regulatory fragmentation.

2. **The AfCFTA Digital Trade Protocol**

The Protocol's core aim is to support AfCFTA's objectives by creating harmonized rules and common principles/standards for digital trade. It applies to measures adopted or maintained by a State Party affecting digital trade,

while excluding government procurement and government-held information.

It also affirms the right to regulate for public welfare, sustainable development, security interests, and legitimate public policy. The Protocol then builds "digital trade enablement" through legal validity of e-docs and trust tools (e-signatures, timestamps), authentication rules, paperless trading, e-contracts, e-invoicing, logistics/last-mile, and digital infrastructure support. Finally, it sets out a data governance layer (cross-border transfers, personal data protection, limits on forced data localization), plus trust topics like cybersecurity and consumer protection.

The Protocol defines "Digital Identity" as "a set of unique and validated digital attributes or credentials for identifying a natural or juridical person." Then it moves from definition to obligation: State Parties must adopt or maintain digital identity systems for both natural and juridical persons. It also mandates an Annex on Digital Identities specifically "to foster interoperability" between national systems, and even lists what the Annex should consider: common standards, comparable protection/recognition of legal effects, mutual recognition, and exchange of best practices. In plain terms, AfCFTA's digital market is being designed with the assumption that identity must travel.

It also ties identity to real use-cases. On digital payments, State Parties commit to promote interoperability of payment systems and enable "cross-border authentication and electronic know-your-customer verifications."

It also expands the idea of interoperability beyond identity alone, requiring promotion of mutual recognition mechanisms for digital identities and authentication tools, while allowing States to require higher performance standards for certain transactions.

The Annex operationalizes digital identity by moving from high-level interoperability commitments to concrete system obligations. State Parties must maintain systems that cover enrollment, issuance, and lifecycle management of credentials, and embed robust authentication features such as biometrics and multi-factor mechanisms.

It establishes a notification regime and a Secretariat-maintained database of national systems and issuing authorities, alongside mandatory breach notifications and consultation channels, creating transparency and peer scrutiny. It establishes non-discrimination and "comparable/equivalent protection" duties, requiring States to treat other Parties' digital identities no less favorably than their own and to afford equivalent protection to identities used in digital trade.

On technical governance, it disciplines standards and conformity assessment to prevent disguised restrictions on digital trade, requires harmonization and interoperability, and contemplates joint assessments, trusted lists, and conditional mutual recognition based on assurance levels.

Finally, it introduces the concept of a voluntary AfCFTA Digital Identity issued by designated African institution(s), sets

transparency and cooperation frameworks, and subjects disputes to AfCFTA's dispute settlement, shifting identity from policy aspiration to enforceable, structured integration.

3. **The Implementation Gaps**

Whereas mutual recognition is conditional, the conditions require machinery that does not yet exist. Recognition is tied to notification, interoperability principles, and "appropriate" assurance levels. As a result, the Protocol does not establish a continent-wide assurance framework by default. Instead, it states that States may agree on one or recognize each other's frameworks, leaving space for uneven standards and slow bilateralism.

The Annex creates a database, but not a strong enforcement model. The Secretariat must maintain a database of systems and issuing authorities, and States may request consultations. That is transparency and not enforcement. There is no clear compliance consequence if a State fails to notify properly, maintains weak controls, or ignores consultation outcomes.

Security incident reporting exists, but the operational details are lacking. States must notify breaches/threats and mitigate promptly. But the Annex does not define severity thresholds, timelines, minimum incident response standards, public notification duties, or cross-border containment procedures. These are the factors that determine whether trust survives the first major failure.

Whereas interoperability principles are listed, they are not standardized. Article 12 references open standards, audit trails, privacy-by-design, secure communications, data sovereignty, etc. That's directionally correct, but it's not a technical specification. Without minimum technical profiles, "interoperable" can become a label rather than a capability.

The principles of non-discrimination and "comparable protection" present practical gaps. Articles 7 and 8 of the Annex require equal treatment and comparable protection of digital identities. How this presents a gap on what counts as "comparable" protection when constitutional privacy thresholds, data retention rules, and surveillance powers differ widely. Without a shared baselines, these clauses risk becoming disputes rather than solutions.

There is no harmonized KYC baseline. Authentication mechanisms are listed under Article 5, and the Digital Trade Protocol links payments to cross-border authentication and e-KYC (Article 15(2) (c)). But neither instrument defines minimum KYC datasets, when enhanced due diligence applies, or how to treat beneficial ownership for juridical persons. These are key issues for fintech compliance and AML risk.

4. **Recommendations**

The Council of Members should adopt a mandatory minimum continental assurance baseline for digital identity use in cross-border transactions. This should include defined assurance tiers, standardized identity attributes, minimum authentication strength and clear mapping for "equivalence". Without this, "mutual recognition" will devolve into bilateral negotiations and regulatory patchwork.

The Annex contemplates a trusted list of recognized digital identity systems. The trusted list should be conditional upon:

- Independent conformity assessments
- Security audit certification
- Compliance with agreed technical specifications
- Demonstrated incident response capacity

Incident reporting obligations should be operationalized through continent-wide standards. While the Annex requires States to notify breaches or threats to security and take mitigating measures, it does not define reporting timelines, severity thresholds, or coordinated response procedures. A harmonized incident management framework would strengthen trust and prevent fragmentation in the aftermath of system failures. Identity systems are only as credible as their crisis response architecture.

The governance of the AfCFTA Digital Identity must be clarified before rollout. The Annex provides for its establishment and issuance by designated African institution(s), with voluntary acceptance by State Parties. That model requires transparent accountability structures, liability allocation rules, oversight mechanisms, and defined interoperability pathways with national systems. Without governance clarity, uptake will be cautious and politically sensitive.

Identity interoperability must be aligned with AML and KYC integrity. The Digital Trade Protocol connects cross-border authentication and electronic KYC to digital payments, but neither instrument establishes a harmonized KYC dataset or shared risk thresholds. A minimum cross-border KYC baseline would ensure that identity recognition strengthens financial integrity rather than weakening due diligence standards. Harmonization here is not about centralization; it is about reducing duplication while preserving safeguards.

Finally, public policy and security exceptions must be applied proportionately. The Protocol safeguards the right to regulate and permits restrictions on cross-border data transfers for legitimate objectives. However, interpretative guidance should clarify proportionality, necessity, and transparency requirements when such exceptions are invoked. Otherwise, sovereignty safeguards risk becoming default barriers that quietly undermine interoperability.

5. Conclusion

AfCFTA has already settled the normative debate: digital identity is no longer peripheral to Africa's integration project. It is embedded in the Digital Trade Protocol and operationalized through the Annex on Digital Identities. The legal architecture mandates systems, anticipates interoperability, structures mutual recognition, and anchors identity within payments, authentication, and data governance. The remaining challenge is not whether digital identity belongs within AfCFTA, but whether implementation will be disciplined enough to prevent sovereignty safeguards and uneven capacity from reproducing the very fragmentation the Protocol seeks to eliminate.

Interoperability must therefore be treated as infrastructure and not aspiration. It must be supported by common assurance baselines, credible supervisory coordination, transparent incident response mechanisms, and enforceable recognition standards. If States align technically but diverge operationally, the continent will have harmonized text and fragmented practice. If they align both legally and institutionally, digital identity will become the trust layer that makes cross-border trade function in real time.

CONTRIBUTORS

GALANDI TONY KIIRE
Managing and Founding Partner

+256 782 498687
kiiregt@diamondadvocates.com

PRISCILLA NAYIGA
Legal Associate

+256 744 594652
priscilla@diamondadvocates.com

DIAMOND ADVOCATES | Partner wone GLOBAL