

# Reflections on regulatory best practices to enable digital identity proofing and eKYC from across the African continent

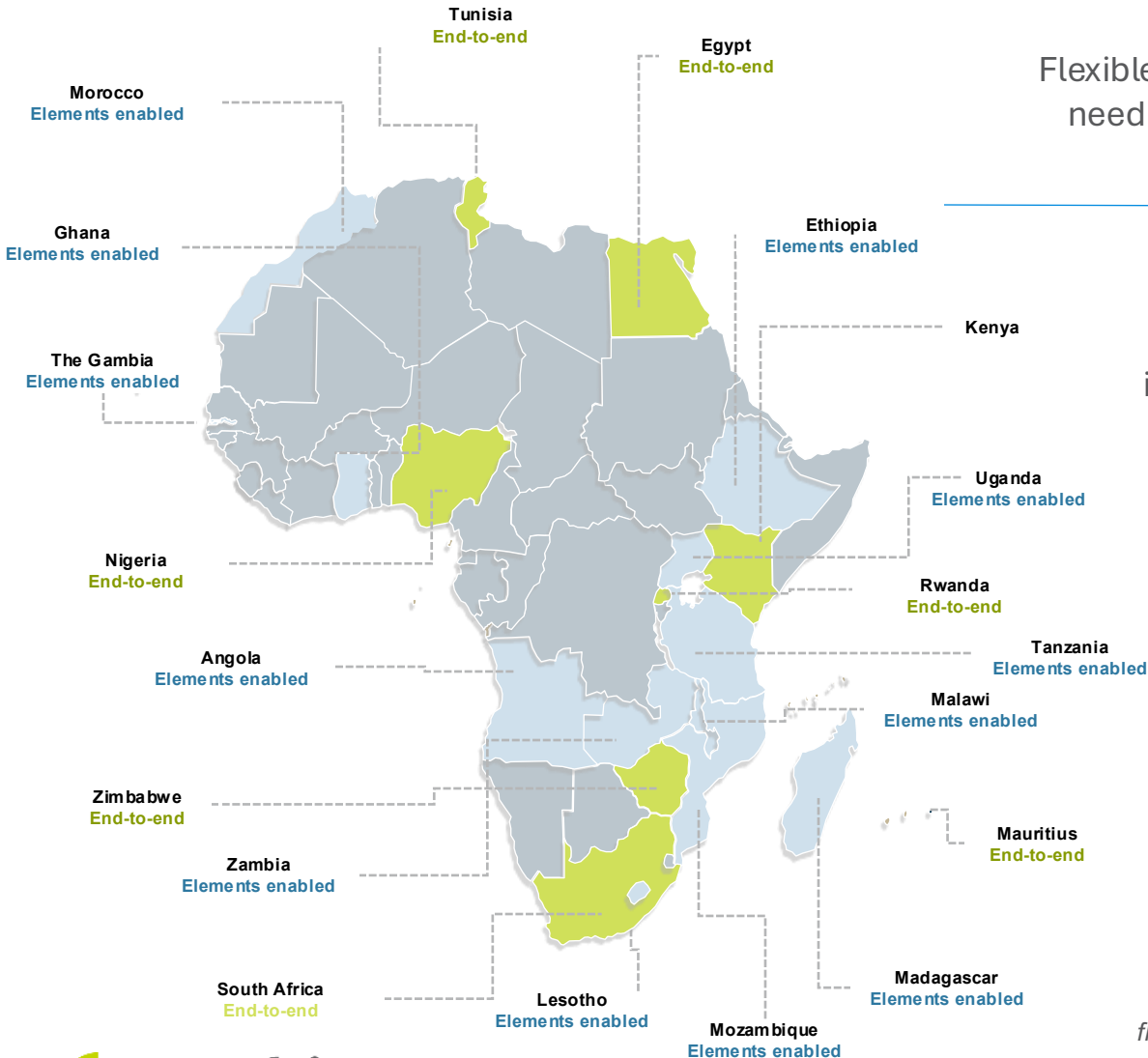
Balancing innovation with compliance through risk-based and outcomes-based regulation

Vera Neugebauer | Senior Associate



# The regulatory landscape for eKYC in Africa

eKYC is increasingly being enabled by regulators on the continent



Flexible regulatory frameworks and clear guidance need to be in place to unlock the private sector's transition to end-to-end eKYC\*.

Regulators are increasingly recognizing the potential for eKYC to strengthen financial integrity and reach excluded or underserved segments of the population

Based on a regulatory assessment of 21 African countries, all countries enabled elements of eKYC

Only 8 countries enable end-to-end eKYC

*\*For end-to-end eKYC means regulation surrounding customer attribute submission, credentials, and verification should either explicitly allow electronic processes or be flexible enough to accommodate them. Moreover, it should be possible to conduct all these steps remotely.*

# eKC enabler #1: Implement a risk-based approach

Align requirements with actual risk, and focus on outcome of achieving effective identity verification



The **risk-based approach** (RBA), recommended by the FATF, means tailoring identity verification requirements to the actual risk posed by a customer, product, transaction, or channel. For example, someone using low-value, services may not need the same level of verification as someone making large transactions. **The outcomes-based approach** complements this by focusing on whether identity is successfully verified, not how. This allows providers to choose appropriate methods—such as biometrics, digital credentials, or video KYC—as long as they meet the regulatory objective.

Many countries still implement **rules-based** or **input focused** regulations with little to no flexibility for PSPs to determine the most appropriate methods. For instance, requiring specific documents like proof of address; or deciding remote interactions should always be classified as high-risk - discouraging use of innovative technology to verify customers



## #1 Implement a risk-based approach

- **Apply proportional eKYC requirements:** allow simplified due diligence for low-risk users and scale requirements only when warranted by the risk. This allows PSPs to better cater to individuals who may not have traditional identity documents.
- **Avoid prescribing specific documents or channels:**
  - Focus regulation on the desired outcome and not the inputs - FATF recommendations are flexible and endorse using "reliable, independent source documents, data, or information" for customer identification and verification – this also includes digital methods.
  - Move away from classifying remote interactions as high risk even if adequate risk mitigation measures are in place, which discourages innovation and accessibility.

# eKYC enabler #2: Provide regulatory clarity on use of eKYC

Clear guidance on digital identity verification empowers providers to adopt inclusive eKYC solutions

Advancements in technology make it possible for PSPs to **obtain and verify identity attributes electronically**



Yet, regulation is **often written with physical and paper-based interactions** in mind, assuming the customer is there in person to sign and provide documentation.

This **lack of clarity creates uncertainty** for providers and may deter them from using innovative eKYC tools



## #2 Provide regulatory clarity on use of eKYC

- **Clearly define** what is allowed in terms of electronic attribute submission, digital credentials, and non-face-to-face verification.
- **Issue regulatory guidance** or circulars that provide practical interpretation of rules to reduce uncertainty.
- Where possible, adopt **technology-neutral** language that allows adaptation as tools and infrastructure evolve.
- Engage regularly with PSPs and industry to support compliance and promote responsible innovation in digital identity verification.

# eKYC enabler #3: Promote efficient data-sharing practices for identity verification

eKYC systems are most effective when identity data can be securely verified across institutions and platforms



A key enabler of inclusive digital identity proofing and eKYC is the ability for FSPs to **access and validate identity data that has already been verified**—whether by public registries, other financial institutions, or trusted third parties.

Yet, many regulatory frameworks lack **clear rules for data sharing**, and existing digital ID systems are not always accessible to financial institutions creating duplication, increased costs, and barriers for providers—especially non-banks—to conduct remote identity verification.



## #3 Promote efficient data-sharing practices

- Establish legal and technical frameworks that support secure, interoperable data-sharing between government ID systems and PSPs for identity verification.
- Ensure equitable access to national ID and population databases for both bank and non-bank PSPs to support digital-first models.
- Promote a collaborative approach to CDD which both enables PSPs to rely on other regulated PSPs, as well as service providers for eKYC
- Integrate data protection and consent mechanisms to build trust in digital identity systems and ensure responsible data use.

# Thank you

Vera Neugebauer

[vera@cenfri.org](mailto:vera@cenfri.org)

## About Cenfri

Cenfri is a global think-tank and non-profit enterprise that bridges the gap between insights and impact in the financial sector. Cenfri's people are driven by a vision of a world where all people live their financial lives optimally to enhance welfare and grow the economy. Its core focus is on generating insights that can inform policymakers, market players and donors who seek to unlock development outcomes through inclusive financial services and the financial sector more broadly.

