

Africa PKI Consortium

Building the trust layer for Africa's digital future.



Presented by

Engr. Abisoye Coker-Odusote

Interim Chairman

Solomon Kofi Richardson

Interim Secretary

Africa's digital transformation is accelerating.

Across the continent, governments and citizens are moving services, identity, and commerce onto digital rails — at an unprecedented pace.

Identity

Digital ID & foundational IDs

Foundational ID systems & mobile IDs scaling fast.

Government

eGovernment & service delivery

Portals, e-signatures, e-procurement, eTax.

Trade

AfCFTA & digital trade

A single continental market going digital.

Payments

Mobile money & instant rails

PAPSS, fintech, and cross-border flows.

Health

eHealth & data exchange

Records, prescriptions, cross-border care.

Borders

Smart borders & mobility

e-Passports, e-visas, cross-border services.

Africa is digitising rapidly. But...

Digital transformation without trust will fail.

01

Citizens

Will not adopt systems they do not trust. Privacy, security, and verifiability are preconditions for adoption — not afterthoughts.

02

Governments

Cannot interoperate securely without a shared trust framework. Data exchange, e-signatures, and APIs require verifiable identities.

03

Markets

Cross-border digital trade requires trusted identity, signed documents, and transactions that are recognised across jurisdictions.

Introducing

PKI — the trust layer for digital society.



What is PKI? In one sentence.

*Public Key Infrastructure lets digital systems trust **people, devices, documents, and transactions** — across organisations and borders.*

Authenticate

Prove who you are — to a portal, an API, or a counterparty.

Sign

Apply a digital signature with the same legal weight as a handwritten one.

Encrypt

Protect data in transit and at rest from interception or tampering.

Non-repudiate

Lock in proof — a signer cannot later deny a transaction.

PKI powers the entire eGovernment ecosystem.

A single trust fabric underpins every high-value digital service a government delivers.



Without PKI, secure digital government cannot scale.

The role of National PKI.

National PKI is the establishment of sovereign digital borders through PKI, ensuring that the state holds the authority to verify trust, protect national data, and issue digital keys to the country's critical infrastructure.

01

Citizens

Access to state secured services, secure transactions with the state, trusted identities that open doors.

02

Governments

Provision of trusted source data and secured services, continuity of critical digital systems, and control over critical state infrastructure.

03

Markets

Secure trusted operating environments that enable legitimate business operations and protection against illegal activities.

Introducing

National PKI — the keys to the kingdom and the rest of the world.



Why PKI is critical to modern identity infrastructure.

As ID4Africa has framed for a decade, digital identity is **public infrastructure**. To behave like infrastructure, identity systems must be trustworthy by design.

PKI delivers the cryptographic backbone that makes IDs verifiable, interoperable, and resistant to fraud — at population scale.

"PKI is no longer optional for modern identity ecosystems."

What PKI enables for ID

- 01 **Strong authentication** — passwordless, phishing-resistant logins for citizens and officials.
- 02 **Secure ID credentials** — smartcards, mobile IDs, eMRTDs, verifiable credentials.
- 03 **Biometric integrity** — signed templates and tamper-evident enrolment records.
- 04 **Federation & interoperability** — trusted exchange between agencies and across borders.
- 05 **Mobile ID at scale** — secure wallets, signed attestations, on-device key protection.

Africa's current PKI challenge.

Low adoption

Few countries have a functioning national PKI in production.

Fragmented deployments

Pockets of capability with no continental coherence.

Weak interoperability

Certificates rarely cross borders or sectors.

Inconsistent regulation

Divergent e-signature and trust service laws.

Low awareness

Decision-makers underestimate PKI's strategic role.

Vendor-driven approaches

Procurement leading policy, not the other way around.

No standards harmonisation across the continent

Each national initiative re-invents policy, profiles, and root models — at high cost.

"Many countries invested in PKI but achieved little value due to lack of ecosystem understanding."

The problem is not technology. It is coordination.

National silos will not scale to a continental market.

Every flagship continental ambition — AfCFTA, PAPSS, mutual recognition of IDs, cross-border services — depends on certificates and signatures being trusted *across* jurisdictions, not just within them.

Cross-border trade

Customs documents, e-CoOs, signed manifests must verify everywhere.

Digital payments

Pan-African instant rails need shared certificate trust anchors.

Digital certificates

A certificate issued in Accra must be valid and verifiable in Abidjan.

Mutual recognition

Of identities, signatures, and trust service providers.

Regional integration

RECs, AU bodies and national agencies need a shared trust framework to interoperate.

Africa cannot build interoperable digital trade on fragmented trust frameworks.

The case for harmonised standards & trust frameworks.

Harmonisation is not about uniformity. It is about **compatible policy, profiles, and process** so that African digital trust can interoperate — and so African identities are recognised globally.

What we harmonise

Legal frameworks for e-signatures & trust services

Root CA models & certificate hierarchies

Certificate policies (CP) & practice statements (CPS)

Interoperability profiles & trust lists

Mutual recognition of digital signatures

Cybersecurity alignment & audit regimes

Anchored in global standards

African solutions must be globally interoperable — not parochial — so that African identities can be recognised, accepted, and trusted worldwide.

ISO

ETSI

X.509

RFC 5280

AU Frameworks

AfCFTA

Shared standards turn 54 national PKIs into one continental trust ecosystem.

Africa must act early — before fragmentation hardens.

Africa is still early in PKI adoption. That is a **strategic advantage**, not a deficit — if we coordinate now.

Lesson 01

Telecom fragmentation

Roaming and number portability took decades — and significant cost — to reconcile across borders.

Lesson 02

Payment fragmentation

Closed mobile money walls and incompatible switches still slow cross-border value flow today.

Lesson 03

Identity silos

Sectoral IDs proliferated before harmonisation — we are still un-doing that legacy.

The opportunity

*With PKI, Africa can build interoperability **by design**.*



Introducing

The Africa PKI Consortium

A peer-driven, non-profit continental platform dedicated to harmonising PKI adoption across Africa.

Collaborative

Member-state & ecosystem driven

Non-profit

Public-interest, vendor-neutral

Peer-driven

Country-to-country learning

Technical

Standards & implementation support

Policy

Advocacy & legal alignment

Capacity building & interoperability — for governments, regulators, and trust service providers across the continent.

The Consortium exists to help Africa get PKI right the first time.



Five strategic pillars.

A focused, manageable scope that translates ambition into deliverables across the Consortium's working groups.

01

Standards & interoperability

Profiles, trust lists, root models, and cross-border recognition.

02

Policy & regulation

Model laws for trust services aligned with AU and AfCFTA priorities.

03

Capacity building

Certification courses, training, and peer-to-peer knowledge transfer.

04

Research & innovation

R&D on African PKI trends, pilots in finance, health, and trade.

05

Partnerships & sustainability

Public-private alliances and long-term funding of the trust ecosystem.

Working groups — where the work gets done.

Each pillar is operated by a member-led working group. Countries, regulators, CAs, and partners contribute experts and rotate leadership.

WG 01 • Technical Standards Certificate profiles, trust lists, interoperability test beds.

WG 02 • Policy & Regulation Model laws, regulator engagement, mutual recognition agreements.

WG 03 • Capacity Building Curriculum, certifications, country-to-country mentoring.

WG 04 • Innovation Pilots in eHealth, financial services, AfCFTA trade documents.

WG 05 • Sustainability & Partnerships Funding, public-private partnerships, sustainability of national PKIs.

What countries gain by joining.

Peer support

Learn directly from countries already running national PKIs.

Implementation guidance

Reference architectures, blueprints, and reviewable playbooks.

Model laws & frameworks

Ready-to-adapt legal & policy templates aligned to global norms.

Standards alignment

ISO, ETSI, X.509, and AU-aligned profiles out of the box.

Training & certification

Build national PKI expertise — operators, auditors, policymakers.

Interoperability roadmap

A clear path to cross-border recognition and trust lists.

Continental influence

A seat at the table where African digital trust is being shaped.

Shared lessons

Avoid pitfalls others have already paid for in time and cost.

Reduced implementation risk

Faster time-to-value on national PKI investments.

Countries do not have to navigate PKI adoption alone.

Founding countries & momentum.

From a five-country declaration to a continental consortium, in just over a year.

2024

Nairobi · The Declaration

Five African countries commit to establishing the consortium.

2026 →

From founding to scale

Working groups operational; new member states joining.

Aug 2025

Accra · The Maiden AGM

Ghana hosts the first AGM. AfPKIC is officially established.

The Nairobi Declaration · Founding Countries

Kenya

Founding

Ghana

Host · 2025 AGM

South Africa

Founding

Cameroon

Founding

Uganda

Founding

Momentum continues — additional member states are joining and aligning to AfPKIC's continental trust framework.

Africa can build the world's most interoperable digital trust ecosystem.

We are early enough to design for interoperability, late enough to learn from every other region. The window is open — but not for long.

For citizens

Identities accepted at home and abroad.

Secure logins, signed documents, and verifiable credentials they actually trust and use.

For governments

eGov that interoperates by default.

Shared trust anchors, lower fraud, faster service delivery, smarter borders.

For business

AfCFTA on a real trust rail.

Cross-border contracts, payments, and trade documents that verify in seconds.

*But only if we collaborate **now**.*

Join us.

Shape Africa's trust framework — together.

01

Join the Consortium

Bring your country, agency, or regulator into the founding cohort.

02

Participate in working groups

Contribute experts to standards, policy, capacity, innovation, sustainability.

03

Build interoperable trust

Align national PKI with continental standards — and global recognition.

"Africa's digital future requires an African trust framework."



Thank you.

Let's build Africa's trust framework — together.

Stay connected

Engr. Abisoye Coker-Odusote

Interim Chairman · AfPKIC

Solomon Kofi Richardson

Interim Secretary · AfPKIC

Questions & conversation welcome.