Communications Authority in Africa Builds a Sovereign Digital Trust Infrastructure with eMudhra CertiNext KMS & CLM

Client Overview

The Communications Authority in Africa (Communications Authority in Africa) is the statutory body responsible for regulating the Information and Communications sector, including broadcasting, telecommunications, and postal and courier services. The Communications Authority in Africa oversees a rapidly digitising public and commercial landscape and is mandated to foster a trusted, secure digital environment for government, enterprise, and citizens. As part of the country's broader Digital Economy Blueprint, Communications Authority in Africa is driving the adoption of digital trust infrastructure to support e-government services, digital identity, and secure online transactions.

The Challenge

Despite being the national licensing authority for digital certificates, Communications Authority in Africa's own PKI ecosystem was largely inactive prior to 2021. The organisation had completed a limited pilot phase, but two foundational gaps prevented it from reaching operational scale: the absence of a secure, centralised Key Management System (KMS) to protect and govern cryptographic keys at the root and issuing CA level, and the lack of an automated Certificate Lifecycle Management (CLM) platform to govern issuance, renewal, revocation, and audit across the ecosystem.

Without a dedicated KMS, Communications Authority in Africa had no assured mechanism for generating, storing, and controlling the private keys underpinning its CA hierarchy. Cryptographic keys were managed ad hoc, exposing the organisation to key compromise risks and making it impossible to demonstrate the chain-of-trust assurance that regulated entities and international frameworks require. Alongside this, certificate lifecycle management was entirely manual — issuance turnaround stretched to two weeks or more, audit trails were incomplete, and no multi-CA framework existed to support subordinate certification authorities at national scale.

> "We had the mandate to be the country's digital trust authority, but without secure key management and automated certificate lifecycle governance, we could not operationalise that role. Both gaps had to be closed simultaneously."
>
> **Director, ICT Infrastructure & Cybersecurity, Communications Authority in Africa**

Compounding these gaps was a growing regulatory imperative. International PKI standards and cross-border digital trust frameworks increasingly require governments to demonstrate hardware-backed key protection and auditable certificate governance. Without a KMS and CLM backbone, Communications Authority in Africa risked falling behind peer regulators and constraining the country's participation in regional digital identity and e-government interoperability initiatives.

The Solution

Communications Authority in Africa selected eMudhra's CertiNext platform — an integrated Key Management System (KMS) and Certificate Lifecycle Management (CLM) solution — to simultaneously close both critical gaps and operationalise its national PKI infrastructure. The engagement was scoped to take Communications Authority in Africa from a dormant pilot to a fully governed, multi-CA digital trust authority.

At the cryptographic foundation, CertiNext KMS was deployed with HSM (Hardware Security Module) integration to establish a hardware-backed root of trust for Communications Authority in Africa's entire PKI hierarchy. The KMS governs the full key lifecycle — generation, storage, rotation, backup, and destruction — for both root CA and issuing CA private keys, all within tamper-resistant hardware boundaries. Dual-control and split-knowledge policies were enforced at the operator level, ensuring that no single administrator could unilaterally access or use sensitive cryptographic material. This gave Communications Authority in Africa, for the first time, a sovereign, auditable key management capability that meets international PKI standards such as WebTrust and ETSI.

Built on top of this secure KMS foundation, CertiNext CLM was deployed as the centralised management layer for the entire certificate ecosystem. The platform's multi-CA architecture enabled Communications Authority in Africa to establish and operate five distinct certification authority entities, each mapped to specific government and regulated-sector use cases including e-procurement, digital identity, and secure interagency communications. Policy-driven automation replaced manual processes end-to-end: certificate requests are now validated, approved, and issued through configurable workflows aligned to Communications Authority in Africa's regulatory policies, with automated renewal alerts and revocation workflows eliminating the risk of unmanaged certificate expiry.

eMudhra's implementation team worked closely with Communications Authority in Africa's technical and compliance staff to design the CA hierarchy, configure certificate profiles, and integrate CertiNext with Communications Authority in Africa's existing IT environment. Role-based access controls govern operator and registrar functions across both KMS and CLM modules, while unified real-time dashboards give Communications Authority in Africa's governance team complete visibility — from key custody status to certificate inventory — across the entire ecosystem. The solution was delivered with structured knowledge transfer, enabling Communications Authority in Africa's team to independently operate, audit, and expand the platform as the national digital trust programme scales.

Results

The integrated deployment of CertiNext KMS and CLM transformed Communications Authority in Africa's PKI capability from a fragmented pilot into an active, sovereign digital trust infrastructure. Five CA licenses were successfully operationalised, each underpinned by HSM-backed key management that provides the cryptographic assurance required for national-scale PKI governance.

Metric	Before	After
Active CA Licenses Operational	None (pilot, inactive)	5 fully operational CAs
Cryptographic Key Protection	Ad hoc; no HSM-backed storage	Hardware-secured KMS with full key lifecycle governance
Certificate Lifecycle Automation	Manual / ad hoc	End-to-end automated via CertiNext CLM

Metric	Before	After
Certificate Issuance Turnaround Time	7–14 business days	Under 24 hours
PKI Ecosystem Adoption (Govt entities)	Limited / fragmented	Expanding; multi-sector onboarding underway
Compliance & Audit Readiness	Incomplete audit trails	Full KMS + CLM audit trail; regulator-ready reporting

With hardware-secured key management now at the core of its PKI hierarchy, Communications Authority in Africa can demonstrate chain-of-trust assurance to international standards — a prerequisite for cross-border digital trust recognition and interoperability. Simultaneously, CLM automation reduced certificate issuance turnaround from up to two weeks to under 24 hours, removing a critical barrier for government agencies adopting digital signing and secure communications. Unified audit trails spanning both key custody events and certificate lifecycle actions have placed Communications Authority in Africa in a strong compliance posture, ready to satisfy domestic regulatory requirements and engage with international PKI governance frameworks.

About eMudhra

eMudhra is a globally trusted provider of digital trust services, offering eSignatures, PKI, Certificate Lifecycle Management, Multi-Factor Authentication, and Identity & Access Management solutions. Licensed by the Controller of Certifying Authorities (CCA), India, eMudhra serves 1000+ enterprises across 40+ countries, helping organisations build secure, compliant, and paperless digital ecosystems.