CERTINEXT · BANKING & FINANCIAL SERVICES · EAST AFRICA

A Large Bank in East Africa Certificate Governance and Unlocks Enterprise Digital Growth with eMudhra CertiNext KMS & CLM

SECTOR	REGION	SOLUTION
Banking & financial services	East Africa	CertiNext

CLIENT OVERVIEW

A Large Bank in East Africa is one of East and Central Africa's foremost financial institutions, headquartered in East Africa, with operations spanning multiple countries across the region. Serving over 20 million customers through an expansive network of branches, agents, and digital channels, A Large Bank in East Africa has built its reputation on democratising access to financial services across the region. As the bank accelerated its digital transformation agenda — scaling mobile banking, digital lending, corporate platforms, and fintech API partnerships — its leadership recognised that a robust, enterprise-grade digital trust infrastructure was the essential foundation on which every new digital initiative would stand or fall.

THE CHALLENGE

A Large Bank in East Africa's ambition to expand its digital footprint across multiple markets was being held back by three deeply connected gaps in its trust and security infrastructure. At the root of the problem was the absence of a governed Key Management System (KMS): the bank had no centralised, hardware-backed mechanism for generating, storing, and controlling the cryptographic keys that underpin the security of its digital services, internal communications, and API integrations. Keys were managed informally across teams and systems, creating unacceptable risk of exposure and making it impossible to demonstrate the cryptographic assurance that regulators, enterprise clients, and technology partners increasingly demand.

Compounding this was a chronic weakness in certificate governance. Digital certificates across A Large Bank in East Africa's multi-country, multi-system environment were tracked manually — typically in spreadsheets maintained by individual teams — with no unified inventory, no automated renewal workflows, and no early warning system for approaching expiry dates. The result was a pattern of reactive fire-fighting: certificate expiry incidents that disrupted digital

> *"Our digital ambitions were outpacing our trust infrastructure. Without governed key management and automated certificate lifecycle controls, every new digital initiative carried a hidden risk we could not fully quantify or contain. "*
>
> **— Group Chief Information Security Officer, A Large Bank in East Africa**

services, eroded customer trust, and consumed disproportionate engineering time to resolve. Each incident also introduced compliance exposure, as banking regulators across A Large Bank in East Africa's operating markets tightened their expectations around PKI governance and audit traceability.

The third dimension of the challenge was strategic: restricted digital exposure. A Large Bank in East Africa's leadership was reluctant to extend certain enterprise digital services — particularly those involving external API connectivity and cross-border digital transactions — until the bank could demonstrate that the certificates and keys securing those channels were under disciplined, auditable governance. The trust infrastructure gap was not just an operational problem; it was a brake on revenue-generating digital initiatives that the business was ready to launch.

THE SOLUTION

A Large Bank in East Africa selected eMudhra's CertiNext platform — combining a centralised Key Management System (KMS) and Certificate Lifecycle Management (CLM) — to simultaneously resolve all three challenges: establishing a sovereign cryptographic foundation, bringing certificate governance under systematic control, and creating the trust infrastructure confidence required to accelerate enterprise digital initiatives.

The deployment began with CertiNext KMS, which established a hardware-secured root of trust for A Large Bank in East Africa's entire PKI environment. Integrated with HSM (Hardware Security Module) infrastructure, the KMS governs the complete key lifecycle — generation, storage, rotation, backup, and controlled destruction — for all CA private keys and high-value cryptographic material across the bank's operations. Dual-control and split-knowledge policies were enforced at the operator level, eliminating single-administrator key access. This gave A Large Bank in East Africa, for the first time, the ability to demonstrate to regulators, auditors, and enterprise partners that its cryptographic keys are managed to international banking security standards — a critical credibility requirement for the digital programmes the bank was preparing to launch.

Built on top of this secured foundation, CertiNext CLM replaced A Large Bank in East Africa's fragmented, manual certificate tracking with a unified, policy-driven lifecycle management platform. A complete certificate inventory was established across all systems, environments, and geographies, giving the bank's security team real-time visibility into every certificate's status, owner, expiry timeline, and associated key. Automated renewal workflows, configurable alert thresholds, and escalation paths eliminated the manual bottlenecks that had produced recurring expiry incidents. Certificate issuance turnaround — previously a process measured in business days — was reduced to under 24 hours through automated validation and approval workflows aligned to A Large Bank in East Africa's internal governance policies.

eMudhra's team worked with A Large Bank in East Africa's security, infrastructure, and compliance functions to map existing certificate sprawl, design a structured CA hierarchy, and configure CLM workflows to match the bank's multi-jurisdiction operating model. Role-based access controls across both KMS and CLM modules ensured that key custodianship and certificate administration responsibilities were clearly delineated and auditable. Unified dashboards spanning both modules provided senior management and compliance teams with the governance visibility needed to satisfy internal risk committees and external regulators alike.

RESULTS

The integrated deployment of CertiNext KMS and CLM delivered a transformation in A Large Bank in East Africa's digital trust posture — closing the governance gaps that had constrained the bank's digital ambitions and providing the credible, auditable foundation required to launch enterprise digital initiatives with confidence.

METRIC	BEFORE	AFTER
Cryptographic Key Protection	Informal; no HSM-backed governance	Centralised KMS with HSM-secured key lifecycle
Certificate Inventory Visibility	Fragmented; no central view	Full real-time inventory across all systems & regions
Certificate Issuance Turnaround	5–10 business days (manual)	Under 24 hours (policy-driven automation)

METRIC	BEFORE	AFTER
Certificate Expiry Incidents	Recurring; reactive remediation	Zero unplanned expiry events post-deployment
Digital Initiative Enablement	Constrained by trust & governance gaps	Enterprise digital programmes launched with confidence
Audit & Compliance Readiness	Incomplete trails; manual reporting	Full KMS + CLM audit trail; regulator-ready dashboards

With hardware-backed key management governing its cryptographic assets, A Large Bank in East Africa eliminated the unquantified key exposure risk that had shadowed its digital expansion plans. Zero unplanned certificate expiry events were recorded following deployment, ending a pattern of reactive incidents that had previously consumed engineering capacity and introduced compliance risk. Certificate issuance turnaround fell from up to ten business days to under 24 hours, removing friction for internal teams provisioning new digital services. Most significantly, the enterprise digital initiatives that A Large Bank in East Africa's business units had been preparing — including expanded API banking partnerships, cross-border digital transaction services, and enhanced corporate banking platforms — were launched with the full assurance of a governed, auditable trust infrastructure behind them.

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 1,000+ enterprises across 40+ countries, helping organisations build secure, compliant and paperless digital ecosystems.

Customer name withheld for confidentiality.