CASE STUDY

EMCA · TELECOMMUNICATIONS · EAST AFRICA

A National Telecom Operator in East Africa Issues Employee Digital Identity Certificates and Secures Internal Network Communications with eMudhra emCA

SECTOR	REGION	SOLUTION
Telecommunications	East Africa	emCA

CLIENT OVERVIEW

The organisation is a national telecom operator in East Africa providing mobile, broadband, and enterprise services to both consumer and corporate customers. The company employs around 1,800 staff and operates a mix of on-premises and cloud-hosted systems for network management, billing, customer care, and internal operations. As part of a broader cybersecurity improvement programme, the company identified PKI as a foundational capability it needed to build internally.

THE CHALLENGE

The operator's internal system communications relied on a mix of commercial SSL certificates, self-signed certificates, and in some cases unencrypted connections between systems that were considered low priority. An internal security review identified that the absence of a trusted internal certificate infrastructure created authentication gaps — in particular, that the operator had no mechanism to issue individual employee digital identity certificates for use in secure email signing and document authentication. The review also noted that the self-signed certificates on several internal network management interfaces were a latent security risk that the security team wanted to address systematically rather than on a system-by-system basis. Building an internal CA would address both the authentication and the encryption gaps simultaneously.

> *"We wanted to move towards strong employee authentication and signed internal communications. Starting with a proper internal PKI was the right foundation — everything else builds on top of it."*
>
> **Head of Cybersecurity**

THE SOLUTION

eMudhra deployed emCA to establish the operator's internal PKI, including a Root CA and two subordinate Issuing CAs — one for employee identity certificates and one for system SSL/TLS certificates. Employee digital identity certificates were configured for use in email signing and document authentication, with a registration authority process set up through the HR and IT teams for certificate enrolment and renewal. Internal network management and billing system certificates were migrated from self-signed to internally issued certificates under the new CA hierarchy. HSM integration ensured that the Root and Issuing CA private keys were hardware-protected. CertiNext was deployed for lifecycle tracking across all internally issued certificates. eMudhra delivered knowledge transfer sessions enabling the operator's security team to manage CA operations, issue certificates, and handle revocation independently.

RESULTS

Employee identity certificate issuance began within 60 days of PKI go-live, starting with the security, legal, and executive teams as an initial cohort. Internal network management certificates were migrated from self-signed within 10 weeks. The cybersecurity improvement programme rated the PKI deployment as one of its most significant completed milestones.

METRIC	BEFORE	AFTER
Employee identity certificates	No internal certificate issuance capability	Digital identity certs issued to first cohort within 60 days
Internal system cert trust model	Self-signed on network management interfaces	Internally trusted certs from company CA
HSM-backed key protection	No HSM; keys unprotected	Root and Issuing CA keys hardware-protected
CA operational self-sufficiency	No internal PKI capability	Team trained; independent CA operations
Cybersecurity programme milestone	PKI identified as capability gap	Rated as major milestone on completion

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.