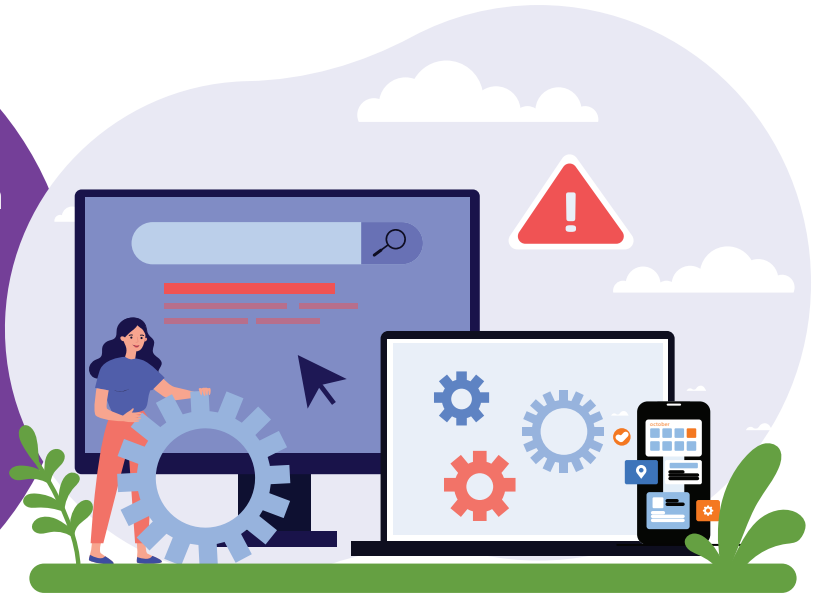
A Computer Support and Services Centre in East Africa Establishes Enterprise CA Infrastructure for Trusted Transactions with eMudhra emCA



Client Overview

A Computer Support and Services Centre in East Africa is a specialised technology distribution and solutions organisation operating in the digital trust and cybersecurity space. Serving enterprise and government clients across its operating markets, A Computer Support and Services Centre in East Africa acts as a trusted intermediary in the digital trust value chain — delivering security technology solutions, PKI services, and digital certificate infrastructure to organisations that require robust, standards-compliant cryptographic trust capabilities. As A Computer Support and Services Centre in East Africa expanded its service portfolio and deepened its engagement with enterprise clients requiring end-to-end trusted transaction infrastructure, the organisation identified a critical gap at the core of its own capability: the absence of an in-house Certificate Authority infrastructure from which to issue, validate, and govern the digital certificates underpinning its clients' trusted transactions.

The Challenge

A Computer Support and Services Centre in East Africa's enterprise clients — spanning regulated industries with stringent requirements for authenticated digital transactions, secure communications, and verifiable digital identities — required a trusted certificate issuance and validation infrastructure that could be governed within a defined policy framework and integrated directly with their operational environments. A Computer Support and Services Centre in East Africa's existing model, which relied on external Certificate Authority service providers for certificate issuance, introduced structural limitations that constrained its ability to meet these enterprise requirements with the speed, flexibility, and governance assurance its clients demanded.

The dependency on third-party CA providers meant that certificate issuance timelines, policy configurations, and certificate profile definitions were subject to external provider constraints rather than being directly configurable to A Computer Support and Services Centre in East

> "Our clients needed a trusted certificate infrastructure they could rely on for mission-critical transactions — and we needed to be the provider of that infrastructure, not a reseller of someone else's CA. Building our own enterprise CA capability with emCA was the step that made us a genuine end-to-end digital trust partner. "
>
> **Chief Executive Officer, A Computer Support and Services Centre in East Africa**

Africa's client-specific requirements. For enterprise clients operating in sectors where certificate parameters — key lengths, validity periods, extended attributes, and policy object identifiers — must be precisely aligned to internal governance standards or regulatory requirements, this inflexibility was a material service limitation. Each certificate issuance request that required customisation or expedited processing was subject to the external provider's operational workflows and support queue, introducing delays and reducing A Computer Support and Services Centre in East Africa's ability to deliver responsive, differentiated service to its enterprise client base.

Equally significant was the absence of an in-house certificate validation infrastructure. Without an operational Online Certificate Status Protocol (OCSP) responder or Certificate Revocation List (CRL) distribution capability, A Computer Support and Services Centre in East Africa could not provide the real-time certificate validity assurance that enterprise relying parties require to trust certificates in high-volume, automated transaction environments. Trusted transactions — whether digital signing workflows, secure API communications, or authenticated system-to-system exchanges — depend on the ability to validate certificate status at the point of use. Without this capability operating under A Computer Support and Services Centre in East Africa's own governance, the organisation could not position itself as a self-sufficient, accountable CA for its enterprise clients.

The Solution

A Computer Support and Services Centre in East Africa selected eMudhra's emCA — a purpose-built, enterprise-grade Certificate Manager — to implement a complete, self-contained CA infrastructure encompassing both certificate issuance and validation services under A Computer Support and Services Centre in East Africa's direct governance and operational control.

The emCA deployment established A Computer Support and Services Centre in East Africa's own enterprise CA hierarchy: a Root CA and subordinate Issuing CA architecture configured to issue digital certificates across the range of use cases required by A Computer Support and Services Centre in East Africa's enterprise client base — including SSL/TLS certificates for secure web and application communications, client authentication certificates for user and device identity, code signing certificates, and document signing certificates for trusted transaction workflows. Certificate profiles were configured by A Computer Support and Services Centre in East Africa's team — with eMudhra's implementation support — to reflect the specific cryptographic standards, validity periods, key usage extensions, and policy attributes required across A Computer Support and Services Centre in East Africa's client portfolio, giving the organisation the profile flexibility that third-party CA dependency had previously made impossible.

Alongside the CA issuance infrastructure, emCA's integrated validation services were deployed to provide A Computer Support and Services Centre in East Africa with a fully operational certificate validation capability. An OCSP (Online Certificate Status Protocol) responder was configured to provide real-time, automated certificate status responses to relying party systems, enabling trusted transaction workflows that depend on instantaneous validity confirmation. CRL (Certificate Revocation List) distribution was established in parallel, ensuring that certificate revocation information is consistently propagated and accessible across all relying party environments in A Computer Support and Services Centre in East Africa's ecosystem. Together, the issuance and validation infrastructure gave A Computer Support and Services Centre in East Africa the complete, end-to-end CA capability required to underpin trusted transactions across its enterprise client base without reliance on any external provider.

The emCA platform was configured with role-based access controls governing operator, administrator, and auditor functions, with approval workflows enforcing separation of duties across sensitive CA operations. A comprehensive internal audit trail — spanning every certificate request, issuance event, revocation action, and key operation — provides A Computer Support and Services Centre in East Africa's compliance and governance team with the full accountability record required to demonstrate CA operational integrity to enterprise clients and auditors. eMudhra delivered structured knowledge transfer throughout the implementation, enabling A Computer Support and Services Centre in East Africa's technical team to independently operate, maintain, and scale the enterprise CA infrastructure as its client base and certificate volumes grow.

Results

The deployment of eMudhra emCA delivered a definitive transformation in A Computer Support and Services Centre in East Africa's capability as a digital trust solutions provider — establishing a fully self-sufficient enterprise CA infrastructure that positions A Computer Support and Services Centre in East Africa as an end-to-end trusted certificate authority for its enterprise clients, independent of any third-party CA provider.

Metric	Before	After
Enterprise CA Infrastructure	Absent; no in-house issuance capability	Fully operational emCA-powered enterprise CA deployed

Metric	Before	After
Certificate Issuance Capability	Reliant on external providers	Independent issuance under A Computer Support and Services Centre in East Africa governance and control
Certificate Validation Infrastructure	Not in place	OCSP and CRL-based validation services operational
Trusted Transaction Enablement	Constrained by lack of trust infrastructure	End-to-end certificate-backed trusted transactions enabled
Certificate Policy Governance	Governed by third-party CA policies	A Computer Support and Services Centre in East Africa-defined policy framework enforced via emCA
Audit Trail & Compliance Visibility	Fragmented; externally held records	Complete internal audit trail across CA lifecycle
Scalability for Enterprise Growth	Dependent on provider capacity	Self-managed, scalable CA infrastructure under A Computer Support and Services Centre in East Africa control

With emCA operational, A Computer Support and Services Centre in East Africa can issue, validate, and govern digital certificates entirely within its own infrastructure and policy framework — eliminating the provider dependency that had constrained its service flexibility and responsiveness. Enterprise clients now receive certificates configured to their precise governance and technical requirements, issued under A Computer Support and Services Centre in East Africa's own CA authority, with real-time OCSP validation available to support trusted transactions at scale. The complete internal audit trail enables A Computer Support and Services Centre in East Africa to demonstrate CA operational integrity to enterprise clients and regulatory auditors with confidence, while the self-managed infrastructure provides the scalability to grow certificate volumes in step with client demand without external capacity constraints.

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.