EMCA · HEALTHCARE & LIFE SCIENCES · INDIA

A Private Hospital Network in India Establishes Internal PKI for Secure Clinical System Communication with eMudhra emCA

SECTOR	REGION	SOLUTION
Healthcare & life sciences	India	emCA

CLIENT OVERVIEW

The organisation is a private hospital network operating six hospitals across two Indian states, with a combined capacity of around 1,800 beds. The network runs a hospital information system, electronic medical records platform, a pharmacy management system, and a laboratory information system — all of which exchange sensitive patient data across the network's internal infrastructure. As the network moved towards a more integrated clinical information model, securing the communication channels between these systems became a priority.

THE CHALLENGE

The hospital network's internal systems communicated over connections that were either unencrypted or secured using self-signed certificates that browsers and systems frequently flagged as untrusted. Clinicians accessing the patient records system from workstations within the hospital received browser security warnings, which they had been trained to ignore — a security practice the network's IT head was uncomfortable with. The network also had no standardised process for issuing certificates for new systems being brought online, with each IT project handling its own certificate needs independently. With the network expanding and planning to add two more hospitals, the IT leadership decided to establish a private CA that could issue trusted internal certificates consistently across all sites and systems.

> *"We had doctors clicking through browser security warnings every time they accessed patient records. That's not a security culture we wanted to normalise. We needed a proper internal PKI"*
>
> **Head of IT, Hospital Network**

THE SOLUTION

eMudhra deployed emCA to establish a private Certificate Authority for the hospital network, enabling it to issue internally trusted certificates for all clinical and administrative systems. The deployment included a Root CA and an Issuing CA, with private keys protected in an HSM. Certificate profiles were configured for internal web services, system-to-system API connections, and workstation authentication. Once the private CA was operational, self-signed certificates across the network's systems were replaced with certificates issued under the hospital's own trusted root — eliminating browser warnings and standardising trust across the estate. A registration authority process was set up so that the IT team at each hospital could request certificates through a governed workflow rather than generating ad hoc self-signed certificates. eMudhra delivered staff training to enable the network's IT team to manage the CA independently.

RESULTS

Self-signed certificates across all six hospitals were replaced within eight weeks of go-live. Clinicians no longer encounter browser security warnings when accessing patient records or clinical applications. The network has since added two new hospitals, both of which were issued certificates from the private CA within days of their systems going live.

METRIC	BEFORE	AFTER
Internal certificate trust model	Self-signed certs; browser warnings on clinical systems	Private CA issuing trusted certs across all 6 hospitals
Browser security warnings — clinical staff	Routine; staff trained to ignore	Eliminated post private CA deployment
New hospital certificate onboarding	Ad hoc; independent per project	Governed RA workflow; certs issued within days
HSM-backed key protection	No HSM; keys unprotected	Root and Issuing CA keys in HSM
New hospitals onboarded	No consistent PKI model for expansion	2 new hospitals issued certs from private CA

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.