CASE STUDY

EMCA · TELECOMMUNICATIONS · INDIA

A Telecom Infrastructure Company in India Deploys Internal PKI to Secure Tower Operations and Partner Communications with eMudhra emCA

SECTOR	REGION	SOLUTION
Telecommunications	India	emCA

CLIENT OVERVIEW

The organisation is a telecom tower infrastructure company in India operating a portfolio of around 8,000 tower sites leased to mobile network operators across several states. The company manages a field operations platform, a tower performance monitoring system, and a partner portal used by tenant operators to access site data and raise maintenance requests. As the company digitised more of its operations, the need for a trusted internal certificate infrastructure became apparent.

THE CHALLENGE

The company's field operations platform and tower monitoring system used self-signed certificates that generated browser warnings for field engineers and back-office staff accessing the systems. The partner portal — used by the company's tenant operators, which included major mobile network operators — had been flagged by one tenant's security team as not meeting their third-party access security standards, specifically citing the use of a self-signed certificate on the portal login page. The tenant had indicated that continued use of the portal under those conditions would need to be reviewed at the next contract renewal. The company's IT head recognised that establishing a proper internal PKI would address both the internal usability issue and the tenant security concern.

> *"Having a major tenant flag our partner portal's certificate in their security assessment was a commercial risk we couldn't ignore. Fixing it was straightforward once we had the right infrastructure in place."*
>
> **Head of IT**

THE SOLUTION

eMudhra deployed emCA to establish a private CA for the company, covering the partner portal, field operations platform, and tower monitoring system. A Root CA and Issuing CA were deployed with HSM-backed key storage. The self-signed certificate on the partner portal was replaced with a certificate from the private CA, and the company shared the root CA certificate with its tenant operators so their systems would recognise and trust the portal. Self-signed certificates on the internal field operations and monitoring platforms were replaced similarly. A certificate issuance workflow was established for the IT team to request and issue certificates for new systems through a governed process. eMudhra integrated CertiNext alongside emCA to track certificate expiry and automate renewal notifications, ensuring the company did not face the same certificate management challenges in the future.

RESULTS

The partner portal certificate was replaced within two weeks. The tenant that had raised the security concern reviewed the updated portal and confirmed it met their third-party access standards ahead of the contract renewal. Internal browser warnings on field operations systems were eliminated.

METRIC	BEFORE	AFTER
Partner portal certificate trust	Self-signed; flagged by tenant security team	Private CA certificate; trusted by tenant systems
Tenant contract renewal risk	Security concern raised; contract review flagged	Concern resolved; contract renewed without issue
Internal system browser warnings	Routine on field ops and monitoring platforms	Eliminated across all internal systems
HSM-backed key protection	No HSM; self-signed keys unprotected	Root and Issuing CA keys in HSM
Certificate lifecycle governance	No formal renewal process	CertiNext integrated for ongoing lifecycle management

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.