CERTINEXT · GOVERNMENT & PUBLIC SECTOR · INDIA

A State Government IT Department in India Bring Certificate Management Under Control Across Its e-Governance Portals with eMudhra CertiNext

SECTOR	REGION	SOLUTION
Government & public sector	India	CertiNext

CLIENT OVERVIEW

The organisation is the IT department of a state government in India, responsible for operating and maintaining the state's e-governance infrastructure — including citizen service portals, departmental applications, and API integrations with central government systems such as DigiLocker and UIDAI. The department manages digital services used by several million citizens and coordinates technology delivery across more than 30 state departments.

THE CHALLENGE

The state's e-governance portals had been built over several years by different vendors and project teams, each using their own certificate procurement processes. By the time the department conducted a review, it had no consolidated picture of how many certificates were in use, which ones were approaching expiry, or who was responsible for renewing them. During one annual review cycle, two certificates on citizen-facing portals lapsed without renewal — causing brief SSL trust errors that were visible to citizens using those services. The incident prompted the state's IT secretary to direct the department to implement a formal certificate management process. A CERT-In advisory issued around the same time also recommended that government entities establish certificate lifecycle governance frameworks.

> *"Two of our citizen portals showed security warnings in browsers because certificates had expired without anyone noticing. That was embarrassing and it was avoidable."*
>
> **State Chief Information Security Officer**

THE SOLUTION

eMudhra deployed CertiNext across the state's e-governance infrastructure. A discovery scan identified 140 certificates across the department's portals and API integration endpoints. Ownership for each certificate was assigned to a designated technical officer within the relevant department, with automated renewal notifications sent at 60, 30, and 15 days before expiry. A private CA was deployed for certificates used in inter-departmental API communication, removing the need to procure external certificates for internal service connections. The CertiNext dashboard gave the state CISO a consolidated view of the full certificate estate — including renewal status, issuing CA, and responsible owner — that the department had never had before. A quarterly report was configured for the IT secretary's office, summarising the certificate compliance posture across all portals.

RESULTS

The discovery scan found 12 certificates that were expired or within 30 days of expiry, all of which were renewed before the next reporting cycle. In the 12 months following deployment, no certificate-related errors occurred on citizen-facing services. The department's response to the CERT-In advisory included a CertiNext deployment summary as evidence of its certificate governance framework.

METRIC	BEFORE	AFTER
Certificate estate visibility	No consolidated inventory	140 certificates tracked in CertiNext
At-risk certificates at discovery	12 expired or within 30-day window	All renewed before next reporting cycle
Citizen portal SSL errors	2 incidents in prior year	Zero in 12 months post-deployment
Certificate ownership	No assigned owner for most certificates	Every certificate has a designated owner
CERT-In advisory response	No formal framework in place	CertiNext deployment submitted as evidence

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.