CASE STUDY

CERTINEXT · GOVERNMENT & PUBLIC SECTOR · SOUTHEAST ASIA

A National Government Technology Agency in Southeast Asia Centralises Certificate Management Across Shared Services Infrastructure with eMudhra CertiNext

SECTOR	REGION	SOLUTION
Government & public sector	Southeast Asia	CertiNext

CLIENT OVERVIEW

The organisation is a government technology agency responsible for shared digital infrastructure used across multiple ministries in a Southeast Asian country. Its portfolio includes a national identity verification platform, a government cloud environment, shared payment services, and several inter-agency data exchange APIs. The agency operates a relatively lean IT security team responsible for maintaining security standards across the shared services it provides to other government entities.

THE CHALLENGE

Managing certificates across the agency's shared services portfolio had become unwieldy. Different services had been deployed by different teams at different times, with certificates procured through separate processes and tracked informally within each team. The IT security team had no single view of the certificate estate and depended on individual service owners to flag upcoming renewals. In one instance, an inter-agency API used by four ministries experienced a certificate expiry that disrupted data exchange for around six hours before it was identified and resolved. The agency's oversight body raised certificate management as a finding in its annual security audit, requiring the agency to implement a formal governance process within the next review cycle.

> *"We were managing certificates for shared services used by multiple ministries, and we had no way of seeing the full picture. The audit finding focused our minds."*
>
> **Head of Cybersecurity, Government Technology Agency**

THE SOLUTION

eMudhra deployed CertiNext to provide centralised certificate lifecycle management across the agency's shared services infrastructure. A discovery scan identified 210 certificates across the national identity platform, government cloud services, payment infrastructure, and inter-agency APIs. Certificate ownership was mapped to the responsible service team for each entry, and automated renewal workflows were configured with team-level notifications at 90, 60, and 30 days. For inter-agency API certificates — classified as high-priority due to their cross-ministry dependencies — renewal workflows were triggered at 120 days and included escalation to the agency's IT security head. A private CA was deployed for internal service-to-service certificates within the government cloud, removing dependence on external CAs for connections that did not require public trust. The audit finding was included in the remediation plan submitted to the oversight body.

RESULTS

The discovery scan found 18 certificates that were expired or within 45 days of expiry, all of which were addressed within three weeks. The annual security audit in the following cycle closed the certificate management finding. No certificate-related disruptions to shared services were recorded in the 12 months after deployment.

METRIC	BEFORE	AFTER
Shared services certificate visibility	No centralised view; team-dependent tracking	210 certificates in unified CertiNext dashboard
At-risk certificates at discovery	18 expired or within 45-day window	All addressed within 3 weeks
Inter-agency API disruption	6-hour disruption from expired certificate	Zero cert-related disruptions post-deployment
Audit finding status	Certificate management finding raised	Finding closed in next annual review cycle
External CA dependency (internal certs)	External CAs used for all certificates	Internal certs moved to 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.