CASE STUDY

CERTINEXT · BANKING & FINANCIAL SERVICES · SOUTH ASIA

A banking-technology provider centralises certificates, keys and its private CA across two data centres

CertiNext KMS and CLM, with an enterprise CA, bring every certificate and key under one policy across primary and secondary sites.

SECTOR	REGION	SOLUTION	
Banking-sector technology provider	South Asia	CertiNext	LIVE

IMPACT AT A GLANCE

2 sites
one certificate and key inventory

1 console
for certificates, keys and private CA

5 key apps
integrated for automated certificate operations

RFP winner
in a competitive banking-sector evaluation

THE CUSTOMER

The customer provides shared technology infrastructure to the banking sector, running services that many financial institutions depend on every day. With operations split across two data centres, it needed a single, auditable way to manage the certificates and cryptographic keys that secure those services, and it ran a formal RFP to select a platform.

THE CHALLENGE

For an organisation whose services sit underneath the banking system, a single expired certificate or mismanaged key can disrupt many institutions at once.

1

Two sites, no single view

Certificates and keys were managed separately at each data centre, making a complete inventory difficult to maintain.

2

Private and public trust

Internal services needed a private CA, while customer-facing services needed EV and wildcard public certificates, all under one policy.

3

Audit expectations

Banking-sector oversight demands clear evidence of who issued, renewed and controlled each certificate and key.

THE GOAL A single, auditable system for every certificate, key and private CA across both data centres.

THE SOLUTION

After a competitive RFP, the customer selected CertiNext as its certificate and key management platform, deployed across both sites under a perpetual licence.

CertiNext CLM

Central discovery, issuance, renewal and revocation for every certificate across both data centres.

CertiNext KMS

Central key management, so cryptographic keys follow the same policy and audit trail as certificates.

Enterprise CA

A private CA for internal services, managed from the same console as public certificates.

Public certificates & integration

EV and wildcard SSL certificates, plus implementation and integration for five critical applications.

WHAT THE CUSTOMER NEEDED	HOW EMUDHRA DELIVERED
One view across two data centres	CertiNext deployed at both sites with a single inventory
Private CA for internal services	Enterprise CA included and managed in CertiNext
Trusted public certificates	18 EV and 2 wildcard SSL certificates
Automation for key applications	Integration for up to five applications
Long-term assurance	Perpetual licence with three years of warranty and support

RESULTS

What changed for the customer

- Every certificate and key across both data centres is managed from one console, under one policy.
- Private and public certificates follow the same lifecycle controls and audit trail.
- Five critical applications are integrated for automated certificate operations.
- The provider is ready for shorter public TLS lifetimes with automation already in place.

WHY EMUDHRA

CLM, KMS and CA in one

CertiNext combines certificate lifecycle, key management and a private CA.

Proven in banking

Chosen through a formal RFP by a provider that serves the banking sector.

Multi-site by design

HA and multi-data-centre deployments are standard.

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.