One of the Large Banks in Middle East East Eliminates Certificate Expiry Risk Across 60,000 Endpoints with eMudhra CertiNext KMS & CLM

Client Overview

One of the Large Banks in the Middle East is one of the the region's oldest and most established financial institutions, founded in the mid-twentieth century. Operating across multiple regions globally, One of the Large Banks in the Middle East serves retail, corporate, and institutional clients through a broad portfolio of banking and financial services, including digital banking, trade finance, treasury, and wealth management. As one of the region's most digitally progressive banks — consistently recognised for technology-led innovation — One of the Large Banks in the Middle East operates a large, complex IT estate underpinning high-volume digital transactions, multi-market regulatory obligations, and an expanding ecosystem of API-driven financial services. The integrity and availability of that estate depends critically on the health of the digital certificates securing it.

The Challenge

Across One of the Large Banks in the Middle East's extensive IT infrastructure, digital certificates were proliferating without systematic oversight. Servers, applications, network devices, and customer-facing digital services across multiple geographies each carried their own certificates — but there was no centralised platform to discover, inventory, or monitor them. The bank's security and operations teams had no reliable answer to a question fundamental to their risk posture: how many certificates do we have, where are they, and when do they expire?

The consequences of this visibility gap were tangible and recurring. Certificate expiry events — when they occurred — were discovered reactively, typically at the point of service disruption. Engineering teams would respond under pressure, manually locating and renewing certificates in affected systems while downstream services queued for restoration. Each incident consumed significant operational time, introduced reputational risk with clients, and created

> "We were effectively flying blind on certificate health. With no centralised inventory or automated alerting, every expiry was a surprise — and in banking, surprises of that kind are never acceptable."
>
> **Head of Cybersecurity Operations, One of the Large Banks in the Middle East**

potential regulatory exposure in markets where CBUAE and international banking frameworks set explicit expectations around IT resilience and security control continuity.

Underpinning these lifecycle management failures was a deeper structural gap: the absence of a governed Key Management System (KMS). Cryptographic keys associated with One of the Large Banks in the Middle East's certificates and PKI infrastructure were managed inconsistently across teams, with no hardware-secured storage, no enforced key rotation policies, and no consolidated audit trail of key custody events. For a bank operating at One of the Large Banks in the Middle East's scale and regulatory profile, this represented a material risk — both to the cryptographic integrity of its digital services and to its ability to demonstrate compliance with security standards such as PCI DSS, ISO 27001, and CBthe region cyber risk guidelines

The Solution

One of the Large Banks in the Middle East deployed eMudhra's CertiNext platform — integrating Key Management System (KMS) and Certificate Lifecycle Management (CLM) capabilities — to replace reactive, fragmented certificate management with a unified, proactive, and auditable digital trust governance framework across its entire endpoint estate.

The engagement began with a comprehensive certificate discovery exercise powered by CertiNext CLM. Scanning across One of the Large Banks in the Middle East's servers, applications, network infrastructure, and digital service endpoints, the platform identified and catalogued over 60,000 endpoint certificates — a figure that significantly exceeded internal estimates and immediately validated the scale of the governance gap the bank had been

operating with. Each discovered certificate was automatically profiled: issuing CA, validity period, expiry date, associated system, responsible team, and cryptographic parameters — all consolidated into a single, searchable inventory accessible to security, operations, and compliance stakeholders.

With the full certificate estate now visible, CertiNext CLM's lifecycle automation was activated across the entire inventory. Configurable, multi-stage expiry notification workflows were established, alerting certificate owners and IT operations teams at 90, 60, 30, and 7 days before expiry — with automatic escalation paths ensuring that approaching deadlines could not be overlooked. Proactive renewal workflows, aligned to One of the Large Banks in the Middle East's internal governance policies, automated the end-to-end certificate renewal process: from request initiation and approval routing through to issuance and deployment confirmation. The combination of early alerting and automated renewal eliminated the conditions that had previously produced reactive expiry incidents.

In parallel, CertiNext KMS was deployed to establish a hardware-secured cryptographic foundation for One of the Large Banks in the Middle East's PKI infrastructure. Integrated with HSM hardware, the KMS governs the full key lifecycle — generation, storage, rotation, backup, and controlled destruction — for CA private keys and high-value cryptographic material across the bank's operations. Dual-control policies and role-based access controls ensure that key custody is clearly assigned, governed, and auditable at every stage. The unified KMS and CLM audit trail — spanning key events, certificate issuance, renewals, and revocations — provides One of the Large Banks in the Middle East's compliance team with the on-demand reporting needed to satisfy CBthe region examinations, PCI DSS assessments, and internal risk committee reviews.

Results

The deployment of CertiNext KMS and CLM delivered an immediate and measurable transformation in One of the Large Banks in the Middle East's certificate security posture. The discovery phase alone reshaped the bank's understanding of its own risk exposure — revealing 60,000 endpoint certificates that had previously existed outside any systematic governance framework.

Metric	Before	After
Endpoint Certificates Discovered	Unknown; no central inventory	60,000+ certificates mapped across all endpoints
Certificate Expiry Visibility	Absent; expiry found reactively	Real-time dashboard with expiry timelines for all certs
Expiry Notification & Alerting	None; manual monitoring by teams	Automated multi-stage expiry notifications in place

Metric	Before	After
Certificate Renewal Workflow	Manual, ad hoc, error-prone	Proactive, policy-driven renewal workflows automated
Cryptographic Key Governance	Unstructured; no HSM-backed controls	Centralised KMS with HSM-secured full key lifecycle
Unplanned Outages from Cert Expiry	Recurring service disruptions	Zero unplanned expiry-related outages post-deployment
Regulatory Audit Readiness	Fragmented records; manual compilation	Unified KMS + CLM audit trail; on-demand reporting

With automated multi-stage expiry notifications and proactive renewal workflows now operating across the full 60,000-certificate inventory, One of the Large Banks in the Middle East recorded zero unplanned service outages attributable to certificate expiry following deployment — ending a pattern of reactive incidents that had previously placed avoidable strain on engineering teams and introduced compliance risk. The HSM-backed KMS established the cryptographic governance discipline required to satisfy PCI DSS key management controls and CBthe region cybersecurity expectations, while the consolidated audit trail enabled compliance reporting that previously required manual effort across multiple disconnected systems.

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 1000+ enterprises across 40+ countries, helping organisations build secure, compliant, and paperless digital ecosystems.