CERTINEXT · LAW ENFORCEMENT · MIDDLE EAST

Police Department in the Middle East Achieves Full Certificate Visibility and Automated Renewal Across Critical Infrastructure with eMudhra CertiNext KMS & CLM

SECTOR	REGION	SOLUTION
Law enforcement	Middle East	CertiNext

CLIENT OVERVIEW

Police Department in the Middle East (Police Department in the Middle East) is the primary law enforcement agency of the region, operating under the national Ministry of Interior. Responsible for public safety, crime prevention, traffic management, and emergency response across the region's diverse and rapidly developing urban and border environments, Police Department in the Middle East operates a sophisticated, technology-intensive infrastructure spanning command and control systems, digital citizen services, surveillance networks, interagency communication platforms, and law enforcement databases. As Police Department in the Middle East accelerated its digital transformation in alignment with the the region's Smart Government and National Cybersecurity Strategy objectives, the security and uninterrupted availability of its digital systems became a matter not merely of operational efficiency, but of public safety and national security.

THE CHALLENGE

Across Police Department in the Middle East's extensive application, server, and network infrastructure estate, digital certificates were deployed and managed in isolation — by individual system owners, application teams, and IT units operating without a shared visibility platform or unified governance framework. There was no centralised discovery mechanism, no consolidated certificate inventory, and consequently no reliable way for Police Department in the Middle East's cybersecurity leadership to answer the most basic certificate risk question: what certificates do we have, where are they deployed, and when do they expire?

This visibility gap carried serious operational and security consequences. Certificate expiry events were discovered reactively — at the point of service failure — rather than being anticipated and addressed in advance. For a law enforcement agency whose digital systems support active operations, emergency dispatch, interagency intelligence sharing, and citizen-facing services, unplanned outages caused by certificate expiry were far more than a routine IT inconvenience. They represented disruptions to operationally critical systems in an environment where availability is a public safety imperative. Each reactive remediation episode also diverted skilled cybersecurity personnel from proactive security work to urgent manual certificate recovery.

> *"In a law enforcement environment, system availability is not a convenience metric — it is an operational requirement. Certificate expiry events were creating blind spots in our digital infrastructure that we could not afford. We needed full visibility and proactive control."*
>
> **Director of Information Security, Police Department in the Middle East**

At the cryptographic foundation, the challenge was compounded by the absence of a governed Key Management System (KMS). Cryptographic keys underpinning Police Department in the Middle East's PKI infrastructure and digital certificates were managed without centralised oversight, hardware-secured storage, or enforced lifecycle controls. In a high-security government and defence context, where the integrity of digital keys directly affects the trustworthiness of classified communications, digital identities, and access control systems, this represented a material gap in Police Department in the Middle East's cybersecurity posture — and a potential point of vulnerability that the the region's National Cybersecurity Authority (NCA) frameworks require to be addressed with demonstrable, auditable controls.

THE SOLUTION

Police Department in the Middle East deployed eMudhra's CertiNext platform — combining a centralised Key Management System (KMS) and Certificate Lifecycle Management (CLM) — to replace fragmented, reactive certificate oversight with a unified, proactive, and security-hardened digital trust governance capability across its entire infrastructure estate.

The engagement was initiated with a comprehensive certificate discovery exercise using CertiNext CLM. The platform performed deep scanning across Police Department in the Middle East's applications, servers, and network infrastructure — systematically identifying, cataloguing, and profiling every deployed certificate across the organisation's IT estate. Each certificate was automatically inventoried with its issuing authority, validity period, expiry date, deployment location, responsible system owner, and cryptographic attributes — transforming what had been an opaque, fragmented landscape into a structured, searchable, and continuously maintained certificate register accessible to Police Department in the Middle East's cybersecurity, IT operations, and compliance teams in real time.

METRIC	BEFORE	AFTER
Expiry Alerting & Notifications	None; reactive discovery at point of failure	Automated multi-stage alerts (90 / 60 / 30 / 7 days)
Certificate Renewal Process	Manual, decentralised, error-prone	Policy-driven automated renewal workflows
Certificate Issuance Complete inventory across Turnaround all apps, servers & network devices Unplanned Service Disruptions	Days to weeks (manual handling) Recurring expiry-related outages	Under 24 hours via automated approval workflows Zero unplanned expiry incidents post-deployment
Compliance & Audit Readiness	Fragmented records; manual effort	Unified KMS + CLM audit trail; on-demand reporting

Centralised certificate discovery provided Police Department in the Middle East's cybersecurity leadership with complete visibility across applications, servers, and network devices for the first time — establishing the authoritative inventory that serves as the foundation for all subsequent lifecycle governance. Automated multi-stage expiry alerting and proactive renewal workflows eliminated the conditions that had previously produced reactive outages in operationally critical systems, with zero unplanned certificate expiry incidents recorded following deployment. The HSM-backed KMS met the hardware security and key governance standards required by the region NCA cybersecurity frameworks, while the unified KMS and CLM audit trail enabled compliance reporting that previously demanded significant manual effort across disconnected records.

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.

With the full certificate inventory established, CertiNext CLM's proactive lifecycle automation was deployed across the entire estate. Multi-stage automated expiry notifications were configured to alert certificate owners and IT operations personnel at 90, 60, 30, and 7 days before expiry, with escalation workflows ensuring that approaching deadlines were visible at the appropriate management level before they became operational risks. Policy-driven automated renewal workflows replaced the manual, decentralised renewal processes that had previously made timely certificate maintenance unreliable. End-to-end renewal — from request initiation through approval routing to issuance and deployment confirmation — was brought under systematic, auditable control, with certificate turnaround reduced to under 24 hours.

Underpinning the entire CLM framework, CertiNext KMS was deployed with HSM (Hardware Security Module) integration to establish hardware-secured governance over Police Department in the Middle East's cryptographic key estate. The KMS manages the complete key lifecycle — generation, secure storage, rotation, backup, and controlled destruction — for CA private keys and all high-value cryptographic material, within tamper-resistant HSM boundaries appropriate for a government and defence operating environment. Dual-control and split-knowledge policies enforce that no single administrator can unilaterally access or exercise sensitive key material. A unified audit trail spanning key custody events and the full certificate lifecycle provides Police Department in the Middle East's compliance and security leadership with the on-demand, regulator-ready reporting required under the region NCA cybersecurity frameworks and internal governance standards.

RESULTS

The deployment of CertiNext KMS and CLM delivered a step-change in Police Department in the Middle East's certificate security posture — replacing an environment of reactive, fragmented certificate management with a proactive, centralised, and fully governed digital trust framework across its critical infrastructure.

METRIC	BEFORE	AFTER
Certificate Inventory Visibility	Absent; no centralised discovery	Complete inventory across all apps, servers & network devices
Cryptographic Key Governance	Unstructured; no HSM-backed controls	Centralised KMS with HSM-secured full key lifecycle