The region's A Transport Authority in a Middle East Unifies Certificate and Key Governance with eMudhra CertiNext KMS & CLM

Client Overview

The Transport Authority (the organisation) is the government entity responsible for planning, building, and operating the region's integrated transport network — encompassing roads, bridges, tunnels, public transit, maritime transport, and smart mobility infrastructure. Serving millions of daily journeys across one of the world's fastest-growing cities, A Transport Authority in the Middle East operates a highly complex, technology-driven estate that includes intelligent traffic management systems, metro and bus networks, digital citizen service platforms, toll systems, and interagency data exchange infrastructure. In alignment with the region's Smart City vision and the the region's National Cybersecurity Strategy, A Transport Authority in the Middle East has made digital transformation and cyber resilience central pillars of its operational strategy — making the integrity and governance of its digital certificate and key infrastructure a matter of direct strategic importance.

The Challenge

Across A Transport Authority in the Middle East's extensive and continuously expanding digital infrastructure, certificate provisioning had long been a manual, decentralised process. Individual system teams and application owners managed certificate requests, issuance, and renewal independently, without a shared platform, consistent policy framework, or centralised oversight. The result was a fragmented identity and certificate governance landscape: certificates were scattered across systems with no unified inventory, provisioning timelines were unpredictable, and the risk of expiry-driven service disruption was a persistent, unquantified liability in an environment where operational continuity directly affects millions of daily commuters and transport users.

The governance gap extended to identity management. Without a centralised CLM platform, the link between digital certificates and the system identities, service accounts, and operator credentials they authenticated was maintained informally — making it difficult to enforce consistent identity governance policies, detect anomalies, or demonstrate the

> "Our certificate provisioning was entirely manual and spread across teams with no common visibility. We had no reliable picture of our certificate estate, no systematic renewal process, and no hardware-grade protection for the keys underpinning our PKI. For infrastructure of A Transport Authority in the Middle East's criticality, that was an untenable position."
>
> **Chief Information Security Officer, A Transport Authority in the Middle East**

certificate-to-identity traceability that national cybersecurity frameworks increasingly demand from critical infrastructure operators.

At the cryptographic foundation, A Transport Authority in the Middle East lacked an integrated Key Management System with HSM (Hardware Security Module) backing. Cryptographic keys underpinning the authority's certificates and PKI infrastructure were provisioned and stored without hardware-secured controls, without enforced lifecycle governance, and without the tamper-resistant key custody assurances required by the region NCA cybersecurity standards for critical government infrastructure. The absence of KMS-HSM integration meant that A Transport Authority in the Middle East could not demonstrate the root-of-trust assurance that its own risk governance frameworks and external regulators required — creating a compliance exposure that grew in urgency as the region cybersecurity oversight of critical infrastructure operators intensified.

The Solution

A Transport Authority in the Middle East selected eMudhra's CertiNext platform — integrating a Key Management System (KMS) with HSM and Certificate Lifecycle Management (CLM) — to replace its fragmented, manual certificate and key governance with a unified, hardware-secured, and policy-driven digital trust framework spanning its entire infrastructure estate.

The deployment was architected from the cryptographic foundation upward, beginning with the integration of CertiNext KMS with A Transport Authority in the Middle East's HSM infrastructure. This established a hardware-secured root of trust for A Transport Authority in the Middle East's entire PKI environment: all CA private keys and high-value cryptographic material are now generated, stored, and managed exclusively within the HSM boundary,

eliminating software-based key exposure. The KMS governs the complete key lifecycle — generation, secure storage, rotation, backup, and controlled destruction — with dual-control and split-knowledge policies enforced at the operator level to ensure that no single administrator can unilaterally access or exercise sensitive key material. The KMS-HSM integration delivers the tamper-resistant key custody assurance required under the region NCA critical infrastructure cybersecurity guidelines, and provides A Transport Authority in the Middle East with an auditable, hardware-attested chain of trust for every certificate issued under its PKI.

Built on this secured foundation, CertiNext CLM was deployed to automate and centralise certificate provisioning and lifecycle governance across A Transport Authority in the Middle East's full infrastructure estate. The platform performed a comprehensive discovery exercise, establishing a unified certificate inventory across all of A Transport Authority in the Middle East's applications, servers, network devices, and digital service platforms — replacing the previously fragmented, team-level records with a single, real-time, searchable register. Each certificate entry is linked to its associated cryptographic key, system identity, and responsible owner, enabling the certificate-to-identity governance traceability that A Transport Authority in the Middle East's security and compliance teams require.

Manual provisioning workflows were replaced end-to-end with policy-driven automation: certificate requests are now initiated, routed for approval, validated against A Transport Authority in the Middle East's governance policies, issued, and deployed through automated CLM workflows — with turnaround reduced from a process measured in days to completion within hours. Multi-stage automated expiry notifications alert certificate owners and IT operations at 90, 60, 30, and 7 days before expiry, with management escalation paths ensuring that renewal timelines are met well in advance of any risk to service availability. The unified KMS and CLM audit trail — spanning hardware key events, certificate issuance, renewals, revocations, and identity linkages — provides A Transport Authority in the Middle East's CISO, compliance team, and the region NCA auditors with on-demand, regulator-ready governance reporting across the entire digital trust lifecycle.

Results

The integrated deployment of CertiNext KMS with HSM and CLM delivered a comprehensive transformation of A Transport Authority in the Middle East's certificate and key governance posture — replacing manual, siloed processes with an automated, hardware-secured, and fully auditable digital trust framework suited to critical government infrastructure at scale.

Metric	Before	After
Certificate Provisioning Process	Manual, decentralised, error-prone	Automated, policy-driven provisioning via CertiNext CLM
Cryptographic Key Protection	Unstructured; no HSM-backed governance	HSM-integrated KMS with full hardware-secured key lifecycle

Metric	Before	After
Certificate & Identity Governance	Fragmented across silos and teams	Unified CLM + KMS governance framework
Certificate Inventory Visibility	Absent; no consolidated view	Real-time inventory across all systems and infrastructure
Expiry Alerting & Renewal	Reactive; manual monitoring	Automated multi-stage alerts and renewal workflows
KMS-HSM Integration	Not in place	Fully integrated; keys generated and stored within HSM boundary
Audit & Compliance Readiness	Manual compilation; fragmented records	On-demand audit trail spanning KMS events and CLM lifecycle

The KMS-HSM integration established, for the first time, a hardware-attested root of trust for A Transport Authority in the Middle East's PKI — meeting the region NCA requirements for critical infrastructure key governance and eliminating the software-based key exposure that had previously represented a material compliance gap. Centralised certificate provisioning through CertiNext CLM replaced unpredictable, error-prone manual workflows with consistent, policy-governed automation, while the unified certificate inventory and identity linkage gave A Transport Authority in the Middle East's security leadership the cross-estate visibility needed to enforce governance at scale. Automated expiry alerting and renewal workflows removed the conditions for reactive certificate incidents, safeguarding the operational continuity of systems on which millions of daily transport users depend.

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.