CASE STUDY

CERTINEXT · GOVERNMENT & LAW ENFORCEMENT · MIDDLE EAST

A Middle East law-enforcement agency brings every certificate under automated control

CertiNext gives full visibility and automated renewal across production, disaster recovery and test environments, including isolated network zones.

SECTOR	REGION	SOLUTION	
Law enforcement	Middle East	CertiNext	LIVE

IMPACT AT A GLANCE

All zones
connected and isolated networks covered

Automated
issuance and renewal with any CA

3 in 1
production, DR and test on one platform

47-day ready
for shrinking certificate lifetimes

THE CUSTOMER

The customer is a large law-enforcement agency that runs critical public-safety and citizen services on its own infrastructure. These services depend on thousands of certificates across connected and isolated networks. Following a formal RFP, the agency chose CertiNext to gain full visibility of its certificates and automate their lifecycle.

THE CHALLENGE

For a public-safety agency, a certificate outage can take a citizen service or an operational system offline without warning.

1

No complete inventory

Certificates from public and private CAs were spread across internal and external systems, with no single source of truth.

2

Isolated network zones

Some systems run in segregated or air-gapped zones that standard cloud tools cannot reach.

3

Shrinking lifetimes

Public TLS certificate lifetimes are falling to 200, then 100, then 47 days, so manual renewal will not keep up.

THE GOAL Complete visibility and automated renewal for every certificate, across every network zone.

THE SOLUTION

eMudhra deployed CertiNext on-premises in a high-availability configuration, with dedicated disaster-recovery and test instances.

Unlimited discovery

Scans internal and external networks, connected and isolated zones, and finds certificates from every public and private CA.

Automated issuance & renewal

Unlimited automated issuance and renewal with both private and public CAs, removing manual steps.

Resilient deployment

HA in the primary data centre, a separate DR site and a UAT environment for safe change testing.

Implementation & support

eMudhra handled implementation and integration, with 18 months of support.

WHAT THE CUSTOMER NEEDED	HOW EMUDHRA DELIVERED
Find every certificate	Unlimited discovery across internal, external and isolated zones
Work with every CA	Public and private CAs managed from one console
Remove manual renewal	Automated, unlimited issuance and renewal
Stay available in a disaster	HA production plus dedicated DR and UAT instances
Keep data in-house	Fully on-premises deployment

RESULTS

What changed for the customer

- The agency has one live inventory of every certificate it owns, across all network zones.
- Issuance and renewal are automated, reducing the risk of expiry-driven outages.
- Production, DR and test environments run on the same platform and policy.
- The agency is ready for 100-day and 47-day public certificate lifetimes.

WHY EMUDHRA

Built for sovereign environments

Fully on-premises, including isolated and air-gapped zones.

CA-agnostic

Manages certificates from any public or private CA.

Selected through RFP

Chosen after a formal evaluation by a public-safety agency.

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.