CASE STUDY

EMCA · TELECOMMUNICATIONS · MIDDLE EAST

A Mobile Virtual Network Operator in the Middle East PKI to Issue Subscriber SIM Authentication Credentials with eMudhra emCA

SECTOR	REGION	SOLUTION
Telecommunications	Middle East	emCA

CLIENT OVERVIEW

The organisation is a mobile virtual network operator (MVNO) in a GCC country, providing mobile services to a focused subscriber segment under a differentiated brand. The MVNO operates over a host network operator's infrastructure and manages its own subscriber management system, customer portal, and a set of value-added services. As the MVNO grew its subscriber base and explored digital identity services, it identified the need for a dedicated PKI infrastructure.

THE CHALLENGE

The MVNO's subscriber management system used commercial SSL certificates procured through a third party, with limited internal control over renewal timelines. More significantly, the MVNO wanted to issue PKI-based credentials for SIM-based authentication — allowing subscribers to authenticate to partner digital services using their SIM identity. This required the MVNO to operate its own CA infrastructure capable of issuing SIM authentication certificates, rather than relying entirely on the host operator's PKI arrangements. The MVNO's IT team had no prior PKI operations experience, so the deployment needed to be straightforward to operate and maintain internally while meeting the technical requirements for SIM credential issuance.

> *"We wanted to offer SIM-based authentication as a value-added service, and that meant we needed our own CA. We also needed to be able to run it ourselves without a dedicated PKI team."*
>
> **Chief Technology Officer**

THE SOLUTION

eMudhra deployed emCA to establish the MVNO's PKI infrastructure, comprising a Root CA and two subordinate Issuing CAs — one for subscriber SIM authentication certificates and one for internal system SSL/TLS certificates. Private keys were protected in an HSM. Certificate profiles for SIM authentication credentials were configured in alignment with the relevant 3GPP and national regulatory standards for SIM-based identity. The subscriber management system and customer portal certificates were migrated from the third-party provider to the MVNO's own Issuing CA, bringing them under internal governance. eMudhra delivered a structured training programme enabling the MVNO's IT team to manage certificate issuance, renewal, and revocation independently. CertiNext was deployed alongside emCA for certificate lifecycle tracking and automated renewal alerts.

RESULTS

The MVNO launched its SIM-based authentication service within 90 days of PKI go-live. The subscriber management and customer portal certificates were migrated to the internal CA within the same timeframe. The MVNO's IT team manages all CA operations independently using the eMudhra-provided procedures and tooling.

METRIC	BEFORE	AFTER
SIM authentication capability	Not available; dependent on host operator	SIM auth certificates issued from MVNO's own CA
Internal certificate governance	Third-party managed; limited internal control	Fully internal management via emCA and CertiNext
SIM auth service launch timeline	Target: post-PKI deployment	Launched within 90 days of PKI go-live
HSM-backed key storage	No HSM infrastructure	Root and Issuing CA keys HSM-protected
IT team operational self-sufficiency	No internal PKI operations experience	Team trained; fully independent CA operations

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.