EMCA · MANUFACTURING · MIDDLE EAST

A Manufacturing Conglomerate in the Middle East Deploys Internal PKI to Secure Factory and Enterprise System Communications with eMudhra emCA

SECTOR	REGION	SOLUTION
Manufacturing	Middle East	emCA

CLIENT OVERVIEW

The organisation is a manufacturing conglomerate based in the Middle East with operations spanning building materials, industrial equipment, and consumer goods. The group operates four manufacturing plants, a logistics division, and a shared corporate services function, employing around 4,500 people across the GCC. A digital operations improvement programme initiated three years ago has resulted in the deployment of industrial IoT sensors, a manufacturing execution system, and enterprise-wide ERP — all of which require secure, trusted network communication.

THE CHALLENGE

As the group added IoT-enabled equipment and cloud-connected manufacturing systems, the need for trusted certificates within the operational technology environment became more pressing. The group's IT and OT teams were issuing self-signed certificates for internal system communication — a workable short-term solution that had become increasingly difficult to manage as the number of connected devices and systems grew. There was no certificate inventory for the OT environment, and replacing expired certificates on industrial systems required planned downtime, making reactive certificate management particularly disruptive. The group's cybersecurity team had flagged the OT certificate situation as a risk item, noting that the mix of unprotected and self-signed certificates created exploitable trust gaps in the manufacturing network.

> *"Managing certificates on industrial systems with no inventory and no plan is one of those risks that sits quietly on the register until something breaks. We decided to address it before something did."*
>
> **Group Head of IT and OT Security**

THE SOLUTION

eMudhra deployed emCA to establish a private CA for the group's IT and OT environments. The deployment included a Root CA and two subordinate Issuing CAs — one for IT systems and one for the OT environment — with separate certificate policies governing each domain. Private keys were protected in an HSM at the group's primary data centre. Certificate profiles were configured for enterprise application servers, API services, industrial IoT device authentication, and manufacturing execution system connections. A governed certificate request workflow was set up for each plant's IT coordinator, enabling them to request certificates for new equipment and systems through an online process rather than generating self-signed certificates locally. Self-signed certificates in the OT environment were replaced in a planned, phased migration to avoid production disruption.

RESULTS

The phased OT certificate migration was completed across all four plants within 14 weeks. The cybersecurity team closed the OT certificate risk item following completion of the migration. The group has not experienced an unplanned production disruption related to certificate issues since the private CA went live.

METRIC	BEFORE	AFTER
OT certificate trust model	Self-signed; no inventory; exploitable gaps	Private CA issuing governed OT certs across 4 plants
IT/OT certificate inventory	No inventory for OT environment	Full inventory under emCA management
OT migration timeline	No migration plan; ongoing risk	All 4 plants migrated within 14 weeks
Production disruptions from cert issues	Risk of unplanned downtime from reactive renewals	Zero unplanned disruptions post-deployment
Cybersecurity risk register	OT certificate gap flagged as open risk	Risk item closed post-migration

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.