EMCA · TELECOMMUNICATIONS · SOUTHERN AFRICA

A Telecommunications Equipment Distributor in Southern Africa Establishes PKI for Secure Dealer and Warranty System Access with eMudhra emCA

SECTOR	REGION	SOLUTION
Telecommunications	Southern Africa	emCA

CLIENT OVERVIEW

The organisation is a technology and telecommunications equipment distributor operating across four Southern African countries, supplying hardware and services to corporate customers, reseller partners, and government entities. The company operates a dealer portal, a warranty management system, and a product configuration platform used by its reseller network and field service engineers. Securing authenticated access to these systems — and the integrations between them — had become a priority as the number of active reseller accounts grew.

THE CHALLENGE

The company's dealer portal and warranty system used commercial SSL certificates that were managed by the hosting vendor, with the company having limited visibility into renewal timelines. The product configuration platform — used by field engineers on customer sites — had been running on self-signed certificates for over two years. When the company's IT auditors reviewed the situation, they found that the field service platform's self-signed certificates had expired entirely in some instances, with engineers having set browsers to ignore the warnings. The company was also looking for a way to issue client certificates for authenticating reseller accounts on the dealer portal, replacing the shared API key model that had been in place since the portal launched.

> *"Field engineers working around expired certificate warnings on customer sites is not the image we want to present. And shared API keys for reseller authentication were always going to be a problem waiting to happen."*
>
> **Head of IT Operations**

THE SOLUTION

eMudhra deployed emCA to establish a private CA for the company's internal and partner-facing systems. A Root CA and Issuing CA were deployed, with certificate profiles configured for the dealer portal, warranty system, and product configuration platform. Expired self-signed certificates on the field service platform were replaced immediately with certificates issued from the private CA, eliminating the browser warnings that engineers had been bypassing. A client certificate issuance process was set up for the dealer portal, enabling the company to issue individual certificates to each reseller account for portal authentication — replacing the shared API key model. Certificate lifecycle management was integrated with CertiNext to track renewals across all internally issued certificates and generate renewal notifications in advance of expiry.

RESULTS

Field service certificates were replaced within two weeks of go-live, eliminating the browser warnings on the product configuration platform. Client certificates were issued to 180 active reseller accounts within four weeks, replacing all shared API keys. The IT audit finding was closed at the next scheduled review.

METRIC	BEFORE	AFTER
Field service platform certificates	Expired self-signed; engineers bypassing warnings	Trusted certs issued from private CA; warnings gone
Reseller authentication model	Shared API keys; no individual identity	Individual client certs for 180 reseller accounts
Dealer portal security	Shared key model; risk of key compromise	Certificate-based authentication per reseller
Certificate replacement timeline	Expired certs tolerated in production	All replaced within 2 weeks of go-live
IT audit finding	Expired cert and shared key model flagged	Finding closed at next scheduled review

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.