emudhra
Trust Delivered

STELLANTIS

CASE STUDY

How Stellantis Secured Millions of Connected Vehicles with a Fully Managed PKI Ecosystem from eMudhra

About Customer

Stellantis is a multinational automotive company with a strong presence in both Europe and North America. They are one of the largest automotive companies in the world by sales volume, with a multitude of brands under its umbrella. The company aims to become a leader in the rapidly changing automotive industry by investing heavily in new technologies such as electric and autonomous vehicles. They are also committed to reducing their carbon footprint with a goal to achieve carbon neutrality by mid of this century.

Business Scenario

Stellantis wanted a PKI deployment as an essential component of their Connected Vehicle Infrastructure and Protocol (CVIP) as it provides a secure and efficient way to manage digital certificates, protect sensitive information, and prevent unauthorized access to the connected vehicle infrastructure.

The CVIP PKI requirement involved setting up of a private PKI (root CA) which would issue identity certificates to their infrastructure and also included the Telemetric devices installed in the vehicles. Apart from this primary requirement, Stellantis also needed multiple Sub-CAs to issue TLS client certificates for B2B service providers or for end-users' mobile application. Hence, they required a solution which could be scaled as per their evolving needs.

As the CVIP ecosystem involves a large number of connected vehicles and infrastructure components, each of which requires a unique digital certificate to authenticate and authorize communication, managing these certificates manually can be time-consuming and prone to errors. Setting up a root CA inhouse involves core PKI expertise, expensive infrastructure and trained resources at hand. Which is why Stellantis opted for a PKI service provider with a centralized platform for issuing, renewing, and revoking digital certificates—reducing the administrative burden and ensuring consistency and accuracy in operations.

eMudhra Solutions

eMudhra provided a fully managed PKI solution by setting up a CVIP Root CA in our Data Center and stored the keys and certificates in a fully secure Hardware Security Module (HSM). We deployed highly secure standards for encryption algorithm, signature algorithm and hash algorithm to ensure watertight security of the CVIP ecosystem and all the communicating parties such as T-Box, server and end-users.

eMudhra also provided a high availability hosted platform to ensure CVIP CA services flowed smoothly into other sub-services including:

- **Registration service**: to verify the identity and specific attributes of a subject
- **Certificate generation service**: ccreating and signing certificates using API connectors
- **Dissemination service**: distributing certificates to subjects
- **Revocation management service**: phandling certificate revocation requests
- **Revocation status service**: providing status information via CRL and OCSP

OVER 15 YEARS EXPERIENCE IN DIGITAL IDENTITY AND TRANSACTION MANAGEMENT

1000K CHANNEL PARTNERS

900+ ENTERPRISE CUSTOMERS

Value added to our Customer

By deploying a Managed PKI for its CVIP (Connected Vehicle Infrastructure and Protocol) ecosystem, Stellantis was able to achieve:

- **Secure Communications**: ensuring only authorized devices communicate within the ecosystem
- **Authentication and Authorization**: preventing spoofing and enhancing network protection
- **Simplified Management**: automation of certificate issuance, renewal, and revocation
- **Interoperability**: creating a common trust framework for reliable device interaction
- **Compliance**: meeting regulatory standards with centralized auditing and control
- **Cost Savings**: reducing operational and infrastructure expenses through managed services

Overall, the Root and Sub CA deployment in a hosted/managed format for the CVIP ecosystem provided Stellantis a secure, interoperable, and compliant environment for connected vehicles and infrastructure.