emudhra
Trust Delivered

CASE STUDY

eMudhra Provides Managed PKI Solution to ensure Encrypted Communication and Telematic Device Security for a Smart Car Manufacturer in Europe

About Customer

Our customer is a multinational automotive company with 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

They 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, our customer 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, and setting up a root CA inhouse involves core PKI expertise, expensive infrastructure and trained resource at hand. Which is why our customer opted for PKI service provider with a centralized platform for issuing, renewing, and revoking digital certificates, which reduces the administrative burden and ensures 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. The results of this service were passed to the certificate generation service
- **Certificate generation service**: creating and signing certificates based on the identity and other attributes verified by the registration service using API connectors
- **Dissemination service**: disseminating of certificates to subjects
- **Revocation management service**: processes requests relating to revocation certificates. The results of this service were distributed through the revocation status service
- **Revocation status service**: providing certificate revocation status information to relying parties. This was based on CRL and OCSP which provides certificate status information on an individual basis.

Value added to our Customer

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

- **Secure Communications**: This deployment provided a secure communication environment for connected vehicles, infrastructure, and other devices. It ensured that only authorized devices were allowed to communicate with each other, and all communications were encrypted to prevent eavesdropping and tampering.
- **Authentication and Authorization**: The Managed PKI provided strong authentication and authorization mechanisms for the connected vehicles and infrastructure. It ensured that only authorized devices (T-box, etc.) were allowed to access the network and specific services, and helped prevent spoofing and other types of attacks.
- **Simplified Management**: It simplified the management of digital certificates and keys for the CVIP ecosystem. Automated the certificate issuance, renewal, and revocation process, reduced the administrative burden and ensured that certificates are always up-to-date and properly configured.
- **Interoperability**: Managed PKI helped ensure interoperability between different devices and services in the CVIP ecosystem. It established a common trust framework that allowed different devices and services to communicate with each other securely and reliably.
- **Compliance**: It helped ensure compliance with relevant standards and regulations for connected vehicles and infrastructure. Provided a centralized system for managing certificates, making it easier to track and audit certificate usage and ensured that certificates are issued and managed in accordance with relevant regulations.
- **Cost Savings**: Ultimately, managed PKI deployment by eMudhra helped our customer reduce the costs associated with certificate management, such as hardware and software infrastructure, staffing, and training. This led to significant cost savings, particularly for an organization that needed to manage large volumes of certificates and keys.

Overall, the Root and Sub CA deployment in a hosted/managed format for the CVIP ecosystem provided our customer a secure, interoperable, and compliant environment for connected vehicles and infrastructure. It helped ensure that communications are secure, devices are authenticated and authorized, and certificate management is simplified, automated and seamless.

About eMudhra

As the world goes Digital, security is ever more crucial to protect identities, data, and enable trust in a digital society. eMudhra focuses on Secure Digital Transformation to enable organizations to progress and evolve without sacrificing "Trust," which matters the most in our society. With an end-to-end stack around trust services, PKI, Paperless transformation, and Digital Authentication, eMudhra is optimally placed to aid digital journeys where identity assertion is critical. eMudhra chairs the Asia PKI Consortium, is a board member of the Cloud Signature Consortium and a member of the CA Browser Forum. Having been in business for over 15 years and built a reach that spans more than 50 countries, eMudhra is deeply committed to bringing change and helping societies not just go digital but do it in a secure