

PrimeKey and Thales provide security solution for transportation manufacturer preparing for a future of electric and self-driving fleets

Background

A large manufacturer of commercial vehicles, such as trucks and buses was looking for an on-demand security solution for their fleet management. Building the necessary foundation for the near future of electric and self-driving trucks, the innovative company aimed to connect their vehicles for secure communication and over-the-air updates. In accordance with internal security policies, the company needs to deploy digital certificates in the vehicles and therefore was looking to deploy a trusted PKI environment.

As a forward-thinking organization, the company sought a scalable security investment that would enable the company the crypto-agility to expand to other use case cases such as personnel IDs, document signing, and V2X solutions. With all the advances in transportation industry, especially around digitization and automation, it was essential that the manufacturer's security solution provides the flexibility required to adapt to dynamically changing environments.

Customer need

The manufacturer is working on a new generation of electric vehicles and self-driving trucks and needed a certificate-based security solution to support the new environment. They initially considered buying HSMs for an on-premises PKI solution, and also

evaluated a 3rd party hosting service, but they preferred a cloud-based PKI hosting and certificate solution they could implement quickly and wouldn't require any up-front investment or in-house hardware management.

Because they were changing from vehicles powered by diesel engines to ones enabled by batteries and software, they were challenged to implement an entirely new system. They needed a certificate-based solution that would provide a secure ID to every vehicle. The organization's IT department, would be responsible for managing and hosting the PKI for their development department, which will make it easy for developers to request certificates from their IT department.

One of the requirements of the manufacturer was to have the ability to do over-the-air (OTA) updates, which will be the first use case in their PKI rollout. While most vehicles besides Tesla are brought into centralized locations for software updates, the manufacturer wants to be able to run updates while the vehicles are in the field. Because they will be connecting to the vehicles long-range, this makes having a secure ID for each vehicle imperative. And anyone working on a vehicle or remotely sending an update, must have a certificate based access. This will also be true with any third-party vendor or vehicle enhancements, such as GPS or infotainment. Everything is certificate-based. Nothing can be connected to the vehicles without approval from the manufacturer. Eventually, each vehicle in the fleet will have an ID issued by the manufacturer, so drivers, loaders, mechanics, etc., will not be able to enter the vehicle without a certificate-based ID.



The Solution

The manufacturer chose the combined solution of PrimeKey's EJBCA Cloud as the certificate authority and Thales Data Protection on Demand's Luna Cloud HSM service as the root of trust for the PKI. The IT department provides the hosted PKI, and this enables the engineering teams to request certificates and manage them throughout their lifecycle simply and effectively.

The main drivers that pushed the manufacturer to have a cloud IaaS based certificate authority from PrimeKey were quick time to market, cost and convenience. Other solutions that were evaluated that offeredaaS certificate services are priced per certificate. The per certificate model could result in significantly increased costs, as well as budgetary planning challenges, per vehicle and along the chain of trust such as mechanic, driver, loader etc. In comparison, having the CA as cloud IaaS made more sense when they evaluated the volume of certificates they would need. Also, having the IT department issue certificates made the process faster and easier. With Thales Data Protection on Demand (DPoD) Luna Cloud HSM as the root of trust, there is no question of the security of the PKI.

Benefits of the new PKI service

While the manufacturer is in the midst of rolling out an aggressive plan to deploy smart, energy efficient fleet of vehicles, they have already experienced benefits of the joint Thales and PrimeKey solution.

- Simplified cloud solution that can be quickly implemented
- Predictable costs for easy budgeting
- Robust technologies with high availability deployment to ensure hassle free production
- Thales and PrimeKey's hosted Luna HSMs and PKI service means no upfront costs or hardware to be managed
- Both the PKI and HSM can be migrated from the Cloud to an on-prem solution, which helps keep the flexibility and not get locked in.
- Combined solution means the manufacturer doesn't have to work with multiple vendors. One supplier can help them throughout the implementation

Next Steps

The company plans to roll out the fleet in 140 countries across the globe, with secure certificates needed for every vehicle throughout their lifecycle.

About PrimeKey

PrimeKey is one of the world's leading PKI and signing solutions providers and has developed several innovative products, including EJBCA® Enterprise, SignServer Enterprise, PKI Appliance, PrimeKey SEE and Identity Authority Manager.

As a pioneer in open-source security software, PrimeKey provides global businesses and organizations the ability to implement vital security solutions, such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation. PrimeKey products are Common Criteria and FIPS-certified, the company's internal processes are ISO 9001, 14001 and 27001 certified and it has numerous Webtrust/ETSI and eIDAS-audited customers.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.