Case Study

Mitsubishi Electric Sanda Works: Encryption management using Thales Luna HSMs that yield significant improvements in security during the software writing process

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Cars continue to evolve.

Electric vehicles, automatic driving (AD), and advanced driver-assistance systems (ADAS) are now common in society. Companies are also producing software-defined vehicles (SDVs) that conduct over-the-air (OTA) bidirectional communication between the vehicle and an external source for maintenance and to improve the functionality of the vehicle.

However, vehicles controlled by software that can be updated via data communications are subject to the risks of external hacking or information leakage; they require a new level of sophisticated security.

Sanda Works of Mitsubishi Electric in Hyogo Prefecture has made significant innovations by deploying Thales Luna Hardware Security Modules (HSMs) into the process for writing software into microcomputers called Electric Control Units (ECUs), which are used for electronically controlling ADAS products. Sanda Works successfully created and implemented a system for robust protection of the entire lifecycle from the development of ECU software to production.

Business Needs

Under the concept of "Realize a safe, secure, and comfortable society", Sanda Works produces a variety of different vehicle control products for ADAS/AD, which are essential elements of automobiles as they become more sophisticated and diverse.

One product that is gaining attention is the driver monitoring system (DMS). These systems help drivers drive safely. For example, the systems use an on-board camera to monitor the driver and issue warnings when the system has detected that the driver is falling asleep or not focusing on the road.

ADAS products are electronically controlled by ECUs. The core of a DMS is an ECU that is integrated into the on-board camera and that contains software (firmware).

The cybersecurity of ECUs has become an important issue in recent years, and Japanese companies are proactively adopting the international standards UN-R 155/UN-R 156 and ISO/SAE 2134.

In the autumn of 2022, an OEM (an automobile manufacturer that is a customer of Sanda Works) that uses DMSs in their vehicles asked Sanda Works to make improvements to the ECU design and production process.

The requirements of the OEM were multifaceted and included compliance with NIST FIPS 197, Advanced Encryption Standard (AES). Specifically, the requirements of the OEM were that the software under development should not be stored on a server that can be accessed via an external network, that encryption be used for software communications between design and the production line, and that encryption must be used when saving encryption keys.

Sanda Works promptly improved their processes.

The company had already implemented security measures. However, Sanda Works was concerned that internal servers did not conform to the standards, so the company decided not to use them.

Sanda Works rebuilt the security process to be based on PCs and encryption processing.

After an investigation of a variety of methods for encryption processing, the company ultimately decided to manage the entire lifecycle of encryption keys using robust keys issued and managed by HSMs.

MITSUBISHI ELECTRIC
Changes for the Better

The reason Thales HSMs were selected was the superior functionality of their advanced protection capabilities compared to that of the solutions of competitors. They provide a much higher degree of security over other solutions in the same price range, and they allow customers to construct much better systems with relatively low investment.

Also, the biggest factor in their decision to adopt Thales HSMs was that Thales provided HSMs to other Mitsubishi Electric factories that also produce automotive components. Other factories praised the HSMs, mentioning the results they received from using them in encryption key management on their production lines.

The device they selected was the Luna USB HSM, a small-form-factor, easy-to-deploy device that has achieved FIPS 140-2 level 3 certification and complies with UNR 155/156.

Solutions

The software completely encrypts all processes between the design area and production line. Encryption keys are created in the HSM, and the keys are saved in an encrypted format. The OEM supported their process improvements. The new DMS production system has been in operation steadily since the autumn of 2023.

The design area constructed a key generation device using the Luna HSM and a PC. The software is encrypted and then sent via LAN at the works to a key management server on the production line.

The production line key management server consists of a Luna HSM and PC. This server decrypts the data, transfers the data to a PC that writes the software, and then the software is written to the ECU.

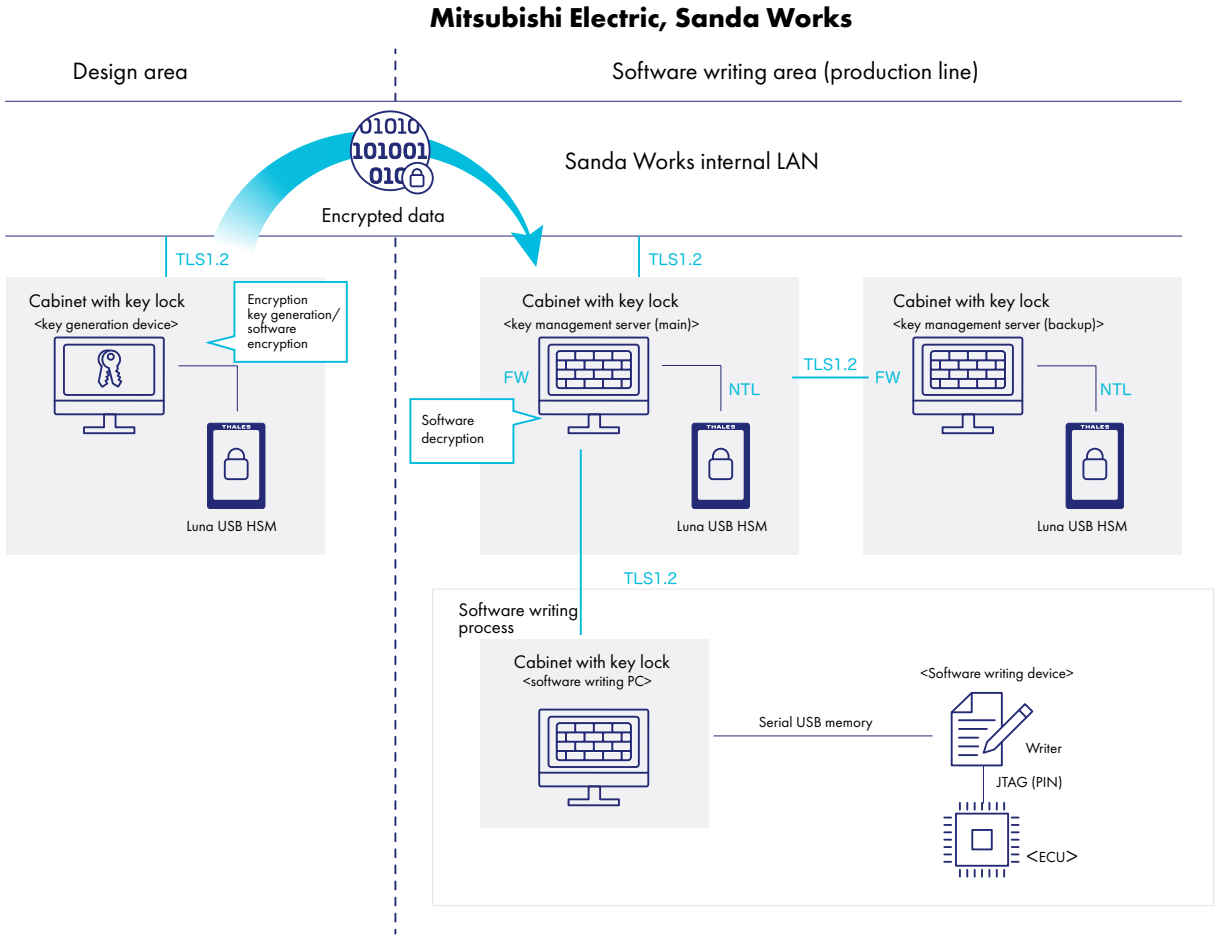
The key management server has a redundant configuration and is linked to a backup server. One characteristic of the Luna HSMs is the ease with which a redundant configuration can be created.

By using HSMs, Sanda Works was able to achieve the high level of process improvements required by the OEM within a short period of time. With the approval of the OEM, the company started full-scale operation of the system in a timely manner.

The DMS market is expected to grow rapidly in the future.

Sanda Works will continue to lead with technological innovations in the DMS market and contribute to expansion of the overall ADAS market by flexibly responding to the security management requirements of each OEM and proactively adopting the latest security technologies.

> " A major trend in the automotive industry is the need to improve security in line with increased convenience. Thales will continue to develop products that can satisfy the needs of OEMs for higher levels of security. In addition to HSMs, we look forward to Thales providing more comprehensive and robust security solutions."
>
> **Mitsubishi Electric, Sandra Works**
>
> **DMV Software Design Department Security team**



About Thales Luna USB HSM

Luna USB HSM delivers industry leading key management in a portable appliance with an USB interface. These devices provide high assurance key protection, maintaining all key materials encrypted within the confines of the tamper-resistant hardware. These devices are characterized by a small form factor and offline key storage function. They are suitable for applications that require protection of business-critical keys in a secure offline environment; therefore, they are widely used in manufacturing industries, government institutions, financial institutions, and large enterprises to protect data, applications and digital identities in order to reduce risk and ensure regulatory compliance.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Challenges

- Car electronics products are electronically controlled by ECUs. Assuring the security of the software (firmware) embedded in ECUs is becoming ever more crucial.
- An OEM requested reforms to the process for writing the software in ECUs.
- The OEM had specific high-level security requirements, including both data encryption and encryption of encryption keys.

Solutions

- HSMs were adopted to manage the entire lifecycle of encryption keys using keys that are issued and managed on dedicated hardware without the need to be sent over a network.
- They considered adopting Thales HSMs because of the superior tamper resistance and high level of protection. The level of security was higher than other products in the same price range.
- The devices that were selected were small-form-factor Luna USB HSMs. These devices are easy to deploy, have achieved FIPS 140-2 level 3 certification, and comply with UN-R 155/156.

Benefits

- These devices allowed Sanda Works to satisfy the requirement that software communication between design and the production line use encryption and that encryption must be used for storing encryption keys. Within a relatively short period of time, the company was able to easily construct a security process that conformed to NIST FIPS 197 of AES.
- All encryption processing takes place inside the FIPS-certified, tamper-resistant hardware to realize a secure lifecycle from software development to deployment.
- The OEM acknowledged the high level of security made possible by using HSMs.
- The timely improvements in processes allowed Sanda Works to smoothly develop and produce DMSs without delay.