cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales ProtectServer HSMs Used as a Root-of-Trust for an IoST (Internet of Secure Things) Platform

Summary

The Internet of Things (IoT) is rapidly expanding. During 2022, the number of IoT devices in the world surpassed 30 billion.[1]

This expansion led to an increase in the number of cyber-attacks targeting IoT devices. To adequately benefit from new business models enabled by the shift to IoT, businesses must ensure they incorporate the appropriate security requirements. One of these requirements is securely managing the keys used for data encryption, authentication, and other tasks. Key management can be quite complex and challenging to implement, into existing technology / IoT systems, and requires technical expertise.

To help address these challenges Dai Nippon Printing Co.,Ltd., (hereinafter "DNP") provides the Internet of Secure Things (IoST), a platform that allows for the easy integration of encryption key management into the IoT systems of customers.

The IoST platform implements Secure Application Modules[2] (SAMs) into IoT devices with the encryption keys pre-configured in the SAMs in advance. This ensures safe, end-to-end communication and the sharing of information in IoT environments through encryption key protection and data encryption. SAMs serve as a root-of-trust for assuring the reliability of IoT devices, and they contain information that acts as a trust anchor. To use this system, SAMs need to be implemented into IoT devices and, on the cloud side, a system is required to manage the trust anchors.

Thales HSMs play a critical role in the management systems of these trust anchors. Thales ProtectServer HSM completes the encryption processing inside the hardened, tamper-resistant hardware device. This system also achieves a high degree of reliability in encryption key management on the IoST cloud side.

Business Needs

Since its founding in 1876, DNP has carefully protected the critical information entrusted to the company by its customers. As the basis for the business as a printing company, DNP has independently achieved the three elements of information security: confidentiality, integrity, and availability.

Since 1981, the company has developed IC cards and has accumulated highly advanced security technologies and expertise through the achievements of the certification of credit card brands both inside and outside Japan and ISO/IEC 15408 (Common Criteria) certification.

In order to achieve customer satisfaction, technological requirements at a high level were established for the management of encryption keys, which are required for security, even in the construction of an IoST platform system.

Thales ProtectServer HSMs were selected for the flexibility and customization abilities that the functionality module toolkit provided when developing proprietary firmware needed to be built into the SAM for complex encryption processing. Thales HSMs are FIPS 140-2 Level 3 certified and provide a physical tamper-resistant device as required by industries that handle critical, sensitive information, such as financial services. Additionally, HSMs support elliptic-curve cryptography (ECC) and enable the construction of highly available redundant configurations due to the features of employing dual swappable AC power supplies and automatic isolation of faulty units.

DNP integrated the Thales HSM into its IoST platform, providing a lower total cost of ownership (TCO) than some of the other competitors on the market, without compromising on performance or quality while meeting the most stringent technology requirements.

This became an important selection factor for DNP wanting to implement a redundant configuration. As a result, after passing strict technological requirements, Thales ProtectServer HSMs, which boast outstanding cost superiority, were adopted.

Solutions

DNP worked with Thales systems engineers to develop firmware that would be implemented into the IoST platform, making it easy to integrate, manage and configure the HSMs.

Because of the ability of the IoST platform of DNP to safely manage encryption keys using HSMs, the company has received praise from such industries as finance and automotive, which require tamper-resistant devices, and the number of customers using this system is steadily increasing.

One example includes the secure remote monitoring maintenance service for automatic teller machines installed at the branches of a financial institution. Conventionally, financial institutions have avoided using network communications with external parties. However, authentication and encrypted communications using secure IoT gateways embedded with SAMs made it possible to securely collect highly confidential information via the Internet and then enabled the external communication needed for remote maintenance.

For credit card payment terminals, using the installed SAM modules to encrypt the credit card information and payment messages and sending it via the IoST platform to the payment infrastructure achieved compliance with PCI DSS, which is an information security standard in the credit card industry.

The system also supports digital key platforms in the automotive industry. The software-based SAM embedded in a smartphone application allows the safe transmission and storage of digital keys on the smartphone, and this level of security prevents the hacking of applications and the exploitation of digital keys.

For more than 25 years, Thales has been the market leader with innovative, high-assurance, FIPS 140-2 Level 3-validated HSMs to meet evolving risk and compliance needs, such as FIPS 140-3. Thales HSMs provide a crypto agile solution, enabling quantum safe algorithms to secure users and data today and into the future.

The IoST platform supports the growth of IoT businesses by providing customers with an environment that allows the achievement of security-by-design in which security measures are implemented from the planning and design stages of the device.

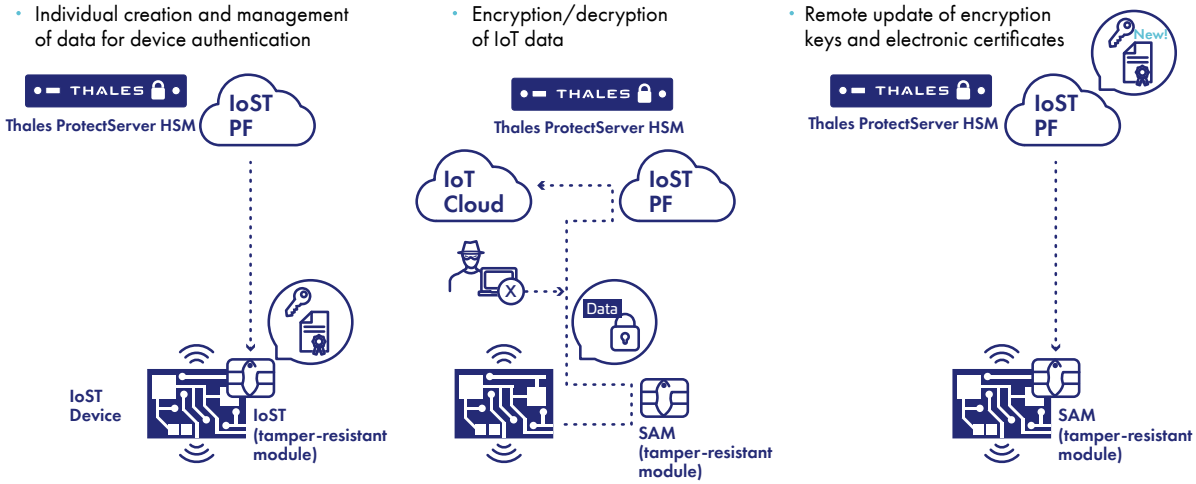
1 Source: Ministry of Internal Affairs and Communications Information and Communications White Paper (2022 Edition)

2 SAM: Secure Application Module. The module is tamper-resistant and used in secure IC chips, and it is equipped with functions that provide safe communication of data with servers through encryption key protection and data encryption. For devices in which secure elements cannot be embedded, tamper-resistant encryption modules are provided in software form.

Three functions of the IoST platform

Functions

- Individual creation and management of data for device authentication
- Encryption/decryption of IoT data
- Remote update of encryption keys and electronic certificates



Results of deployment

- Safe protection of device ID's and encryption keys using tamper-resistant devices
- Realization of secure-by-design

Use Cases

- Financial device remote monitoring service
- Payment terminal remote maintenance service
- Digital key platform

Challenges

- The platform needed to be able to manage encryption keys in the cloud for enhanced security to IoT services.
- The solution needed to meet FIPS 140-2 Level 3 compliance or higher for those operating in highly regulated industries.
- The HSM solution needed to be highly customizable in order to meet the complex encryption processing needs.

Solutions

- The selection of Thales HSMs makes it easy to achieve a redundant configuration to meet FIPS 140-2 Level 3 and ECC compliance and certification requirements.
- Thales ProtectServer HSMs ensured the secure management and storage of encryption keys, including the decrypt / encrypt functions to secure communication to IoT devices.
- The use of Thales ProtectServer HSMs is a cost-effective solution that facilitates the development and implementation of proprietary firmware.

Benefits

- All encryption key processing are performed in hardware with FIPS certification that has robust tamper-resistant capabilities against attacks, which achieves a secure encryption infrastructure.
- Installing Thales HSMs, which have a track record in a variety of fields that require a high degree of security, as a root-of-trust in the cloud provides customers with peace of mind and gains their trust.
- Extensive toolkits in the form of functionality modules made it easy to develop and implement proprietary firmware. It is also easy to modify the firmware after operation has started.
- Highly available redundant configurations are constructed by using dual swappable AC power supplies and automatically isolates faulty units.
- With a guarantee to support the latest technologies, such as FIPS 140-3 and post quantum cryptography, a platform has been built to sufficiently support customer businesses into the future.

"The future plans for the IoST platform are to expand into the fields of industrial equipment, industrial robots, and medicine, while complying with the different standards and guidelines, such as IEC 62443 (which is becoming a substantial security guideline in critical infrastructure fields in Europe and the United States) and IMDRF (which provides cybersecurity guidance for medical equipment). Eventually, the company would like to expand into the social infrastructure that covers the entire supply chain. To that end, the company looks forward to working with Thales in even more fields."

– Takeshi Ohno
Planning & Sales Promotion Group
1st Service Development Department
IoST Platform Division
PF Service Center
Information Innovation Operations
Principal Planner
Dai Nippon Printing Co.,Ltd.

DNP
Dai Nippon Printing Co., Ltd.

About Thales ProtectServer HSMs

Thales ProtectServer Hardware Security Modules (HSMs) protect encryption keys and provide encryption, signing, and authentication services.

Users and developers can seamlessly integrate cryptography and HSMs with a large array of pre-integrated third-party solutions or custom applications. Software development kits (SDKs) for customization make it possible to develop, download, and save customized and unique functionality modules within the secure boundaries of the HSM.

ProtectServer HSMs contain a FIPS 140-2 Level 3 validated cryptographic module to perform secure cryptographic processing in a high-assurance fashion. Built for industry standard security applications, ProtectServer HSMs function within a tamper-protected environment, providing secure storage for highly sensitive information, cryptographic keys, PINs, and data.

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us