cpl.thalesgroup.com

THALES
Building a future we can all trust

Quadrac Co., Ltd.: Contactless payment with a credit card-a major step in the convenience of transportation payments

Thales's payment HSM and tokenization technology are behind innovative MaaS services

Summary

As mobility-as-a-Service (MaaS) for transportation and moving services have begun to gain traction in Japan, so, too, have credit card contactless payments. This payment method is common outside of Japan because of its convenience.

All a paying user needs to do is hold a credit card over a dedicated reader terminal at a ticket gate. No signature or PIN number[1] is required for a credit card contactless payment. Passengers can buy tickets and board efficiently.

Kyoto Tango Railway, Keifuku Bus, and Hokuto Kotsu already provide the contactless payment service, and Nankai Electric Railway and Fukuoka City Transportation Bureau conducted verification tests in 2021. Some of the services and verification tests included specially planned ticket services combining Visa contactless payments[2] and a MaaS app installed on a smartphone. Both cases use Quadrac's Q-move SaaS platform for railway companies to execute authentication and processing payments. Q-move is highly secure and cost-effective and uses Thales's payment hardware security module (HSM) and the CipherTrust Tokenization solution. These are key to safeguarding advanced MaaS sevices.

Key Points for Selection

For easy-to-use contactless payments, it is essential to use stronger methods of protecting credit card information than conventional methods using a signature or PIN code. Quadrac decided to use DUKPT[3] and obtained Payment Card Industry Data Security Standard (PCI DSS) certification[4] to design and develop a payment and authentication center.

DUKPT is a protocol for using encrypted communications between a reader terminal at a ticket gate and the center. To maintain the security level of DUKPT, dedicated hardware (an HSM) is required to protect and manage the cryptographic keys retained by the server.

[1] Payments exceeding a certain amount require a PIN code or signature.

[2] Although there are different kinds of contactless payment services, including Mastercard® Contactless and JCB Contactless, Visa contactless payment services are currently ahead of the others in Japan.

[3] DUKPT Delivered Unique Key Per Transaction

[4] PCI DSS Payment Card Industry Data Security Standard

> " By aggregating the common functions for transportation fare payment in the cloud, we succeeded in starting Q-move at a much lower initial cost than the existing fare collection systems that use IC cards or other media. We are confident that it will play a key role in providing MaaS seamlessly across a variety of transportation institutions. In particular, it is likely that inbound visitors will find it convenient. All they need to do is hold a credit card over the reader, and they can ride an airport bus, shop, stay in hotels, and visit tourist sites. We expect this will contribute to expanding inbound tourism."
>
> – Hirotaka Ito, Cloud Instructure Manager, Quadrac Co., Ltd.

Quadrac compared HSMs from different companies and selected Thales's payment HSM because of its:

- Proven track record of accomplishments in Japan
- Cost effectiveness with the necessary functions provided
- Ability to start small and then upgrade performance after installation

The PCI DSS is the information security standard for organizations that handle credit cards, and a wide range of issues come under scrutiny for PCI DSS compliance. Quadrac wanted not only to achieve PCI DSS certification, but also to minimize potential costs in system development, operation management, and labor to fully prepare for annual audits. Quadrac worked with consultants specializing in PCI DSS compliance to meet these objectives.

The primary focus was to save the raw data decrypted at the center after being received via DUKPT. Re-encrypting and saving data increases the operational load for managing cryptographic keys.

To address these issues, Quadrac decided to tokenize[5] the data. Tokenization is a highly secure method of protecting data, and it contributes to a reduction in both the scope of scrutiny for PCI DSS and the operational load.

Quadrac compared tokenization solutions from several companies and chose Thales's CipherTrust Tokenization because of its:

- Proven track record in solving similar problems
- Cost effectiveness
- Ease in starting small

Moreover, while tokenization has two architectures, vaulted and vaultless, CipherTrust Tokenization is flexible enough to support both. Quadrac chose the vaultless type, which enabled them to reduce both the audit scope and costs.

Solution

Q-move acquired PCI DSS certification as planned and started commercial services in 2020. Railway companies have since been using the high-speed, highly secure payment and authentication functions without worrying about the number of reader terminals required. Another feature of Q-move is it provides Web service that allows public transportation users to see boarding history on their smart phones. And also it provides common functions to implement individual services combined with QR codes.

Having gotten off to a good start on a small scale, Quadrac's cloud service is expected to scale up as an infrastructure for MaaS.

Issues

- Build a highly secure, low-cost cloud service infrastructure for a transportation payment system using the contactless payment function of a credit card.
- Securely use DUKPT for cryptographic communication between a dedicated reader terminal and the payment and authentication center. An HSM is necessary to store the system key securely.
- The payment and authentication center needed to obtain PCI DSS certification.
- Reduce the scope of PCI DSS audits and the operational load by implementing tokenization of raw data.

Solutions

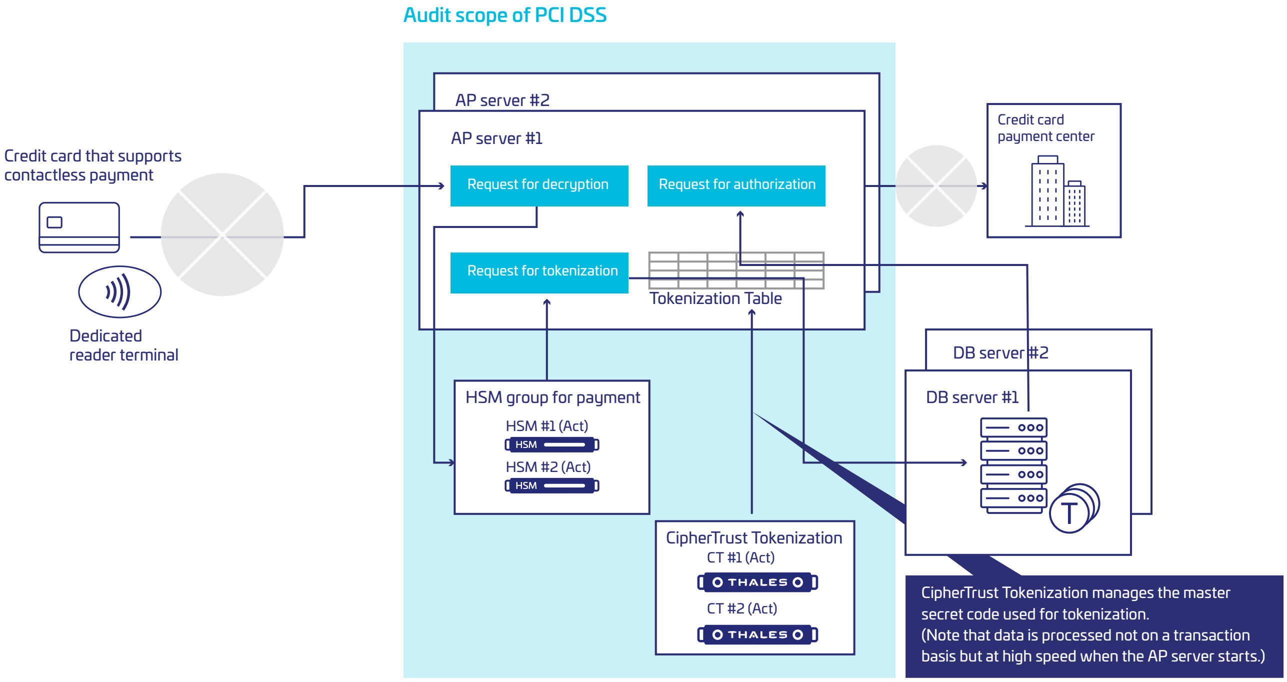
- Thales's payShield HSM was selected to manage the DUKPT system key.
  —Proven track record of accomplishment in domestic cases
  —Cost-effectively provides necessary functions
  —Possible to upgrade performance after initial use, making it easy to start small
- Thales's CipherTrust Tokenization was selected for the tokenization of raw data.
  — Proven track record of accomplishment and cost effectiveness
  —Easy to implement with minimum resources, such as CPU and memory
  —Flexible enough to support both architectures: vaulted and vaultless. For Q-move, vaultless was selected to simplify the auditing of PCI DSS and reduce the initial investment.

Advantages

- Q-move supports DUKPT and has obtained PCI DSS certification. We built a highly secure system infrastructure that allows users to reliably use the contactless payment function of a credit card.
- Credit card data is tokenized before being stored, which reduces the audit scope of PCI DSS. Reduces the initial investment and future operational costs.
- Q-move reduces costs and enables high security operation, which makes it easy for railway companies to introduce the system. Many cases of practical use and demonstration tests are in progress.
- The development engineers at Quadrac had never worked on the system key management of DUKPT and tokenization in compliance with PCI DSS. From the pre-sales stage, Thales's Japan team provided extensive support for Quadrac, including product training for operation managers and attendance at the first audit.
- Thales's broad product portfolio can also support the future development of Quadrac's mobile payments business.

[5] Tokenization is a technology that replaces confidential data, such as credit card numbers, with a random number string, and then saves or uses the string. Tokenized data corresponds only to the original, and thus the original data can be retrieved. On the other hand, tokenized data is not mathematically related to the original data, so even if tokenized data is leaked, it cannot be used in fraudulent ways. This enables tokenized data to fall outside the scope of PCI DSS audits.

The database server storing tokenization data was removed from the scope of the audit by PCI DSS, significantly reducing the load on operational management.



CipherTrust Tokenization manages the master secret code used for tokenization.
(Note that data is processed not on a transaction basis but at high speed when the AP server starts.)

Thales's CipherTrust Tokenization

CipherTrust Tokenization, provided in both vaulted (with a token vault) and vaultless, can reduce the cost and complexity of compliance with the data security requirements of PCI DSS or other standards. Tokenization protects confidential data by replacing the information with substitute tokens and isolating the confidential data from the database or unauthorized users or systems. The vaultless solution has a dynamic data masking function. With either solution, tokenization can be easily added to any application. CipherTrust Tokenization is part of the CipherTrust Data Security Platform. The CipherTrust platform unifies data discovery, classification, and data protection, and provides unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations, and reduces risk across your business.

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.

> cpl.thalesgroup.com <

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