cpl.thalesgroup.com

THALES

Thales to help leading Indonesian financial technology and service provider with PCI compliance

Summary

A leading financial technology and service provider in Indonesia required a data protection solution to comply with the Payment Card Industry Data Security Standard (PCI-DSS) to securely exchange data with its customers.

The Organization

A leading financial technology and service provider in Indonesia with 24 years' experience in developing research and analysis software. The company provides products that combine their expertise in capital and money markets together with software development to cater to a wide range of users such as retail investors and sector professionals.

The company runs three lines of business: that of a bill payment aggregator, an electronic payment platform and online payment solutions.

Business Need

The company needs a data protection solution to comply with the payment card industry (PCI-DSS) and to securely exchange data with its customers from the e-commerce, banking, and insurance fronts. Auditors mandate FIPS (Federal Information Processing Standards) 140-2 validation to meet encryption and key management requirements in the PCI-DSS for data protection.

Being a leading financial technology company, it is important that customers are compliant with certifications and financial services. An inability to meet compliance can lead to security incidents that could then lead to data breaches and heavy fines, damaging brand reputation and putting the entire business at risk.

Most importantly, the customer requires a solution that enables them to expand and scale as more partners engage their services, processing sensitive financial data for analysis.

Potential Liabilities of Non-Compliance with PCI Data Security Standards

According to the PCI Security Standards Council, companies that are non-compliant may face the following consequences:

- Diminished sales
- Cost of reissuing new payment cards
- Fraud losses
- Legal costs, settlements and judgments
- Termination of ability to accept payment cards
- Lost jobs (CISO, CIO, CEO and dependent professional positions)
- Going out of business

Furthermore, the average cost of a data breach is $150 per record, according to the 2019 "Cost of a Data Breach" report by the Ponemon Institute.

Solutions

In Phase 1, the requirement is to deploy a solution to provide encryption services for data within the customer applications. Thales propose using CipherTrust Token Server (CTS) where the application can invoke crypto services using Rest API.

Keys used for encryption are managed and protected securely within the Thales CipherTrust Data Security Manager (DSM).

As part of the auditor requirement where the solution must be validated to FIPS 140-2 Level 3, the customer uses its existing Thales Luna General Purpose Hardware Security Module (GP HSM) as the root of trust (ROT) for the DSM.

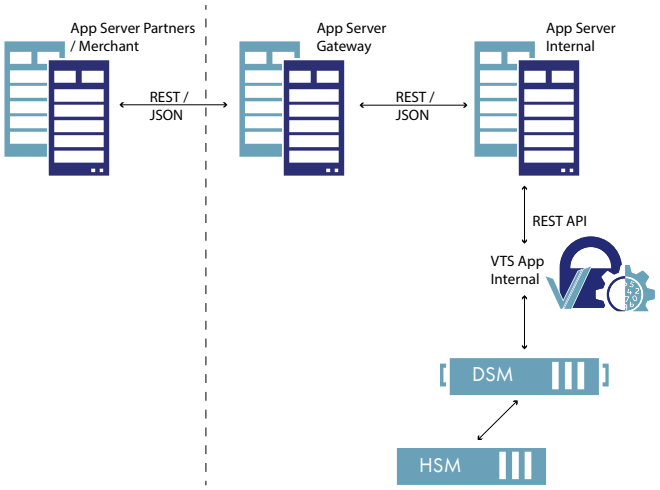

Image above shows Phase 1 deployment

The complete proposed solution will have the ability to encrypt unstructured data before sending it through FTP between a gateway server to their internal server.

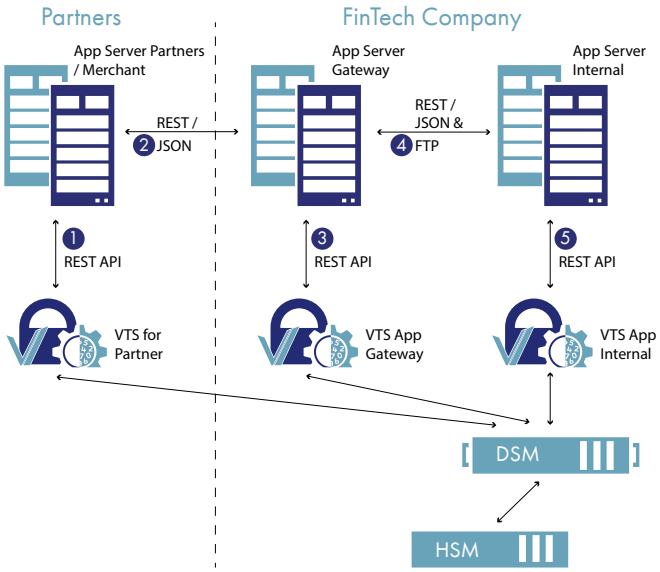

Image above shows the overall tokenization architecture

1. Tokenization stage: Partner tokenise the data before sending the data.
2. To Gateway Server: Partner sends the tokenise data to Fintech customer's gateway server.
3. Detokenization: Fintech customer's gateway server decrypt the data for internal processing.
4. To Internal Server: The processed data is encrypted before sending to the internal server.
5. Data Analysis stage: The internal server decrypt the message for analytics, processing, and storage.

*All 'Vormetric' and 'Keysecure' naming conventions will rename to 'CipherTrust' from September 2020.

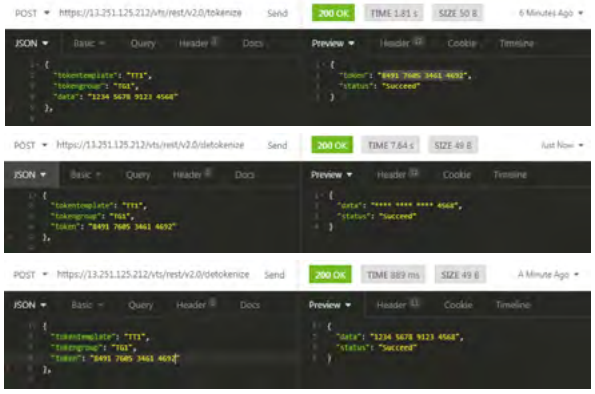

Image above shows the different tokenization stages

Meet Compliance Requirements

Maintaining compliance is an important business need for financial technologies to build and keep trust with customers. Compliance is not a one-time annual event. Upholding and maintaining compliance should be treated as an ongoing challenge to fulfill regulatory requirements in accordance with PCI best practices.

Using Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) is the common centralized management environment for all Vormetric Data Security Platform products. It provides policy control as well as secure management and storage of encryption keys, includes a Web-based console as well as CLI, SOAP and REST APIs.

Leveraging Tokenization Solutions

Vormetric Data Security Manager has Tokenization solutions that aid in financial services and is the next sought after solution to tackle increasing data breaches and growing cases of fraud. Tokenization protects the data itself by making it unusable and substituting it with non-sensitive data, should it be stolen. It creates an unrecognizable tokenized form of the data that maintains the format of the source data.

In financial services, anti-money laundering initiatives require analyzing data while maintaining privacy and security for personally identifiable information (PII).

Tokenized data can be used in place of the original data without destroying the database schema, making it a great advantage for organizations that want to stay with applications and systems already in place.

The Vormetric Data Security Platform from Thales simple one-stop, data-at-rest security

About HSM

Hardware Security Modules

Thales offers the industry leading product family of hardware security modules (HSMs), which are the highest performing, most secure and easiest to integrate in the market today. They act as trust anchors to protect the master keys that encrypt your data and digital identities in a high assurance FIPS 140-2 Level 3-certified, tamper-resistant appliance. Thales offers the following types of purpose-built HSMs.

General Purpose HSM

Luna HSMs come in several form-factors — a network attached appliance, an embedded PCI module, and a portable USB appliance. They can be easily integrated with a wide-range of applications to accelerate general cryptographic operations, secure crypto key life cycles and act as a root of trust for your entire crypto infrastructure. Crypto Command Center is available to centrally monitor and manage multiple Luna HSM crypto resources on-premises, virtual and hybrid cloud environments.

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.