cpl.thalesgroup.com

THALES

Sensitive data protection in the retail card payments ecosystem

Contents

Helping to lower the cost of securing payment transactions:

- Providing flexibility to choose the best security technology approach to align with your specific risk strategy
- Offering you the ability to retain complete control of your cryptographic keys
- Simplifying compliance by protecting your data at all times (in transit, in storage and in use)

Overview

Securing sensitive data in a cost effective manner is often one of the biggest challenges in processing payment transactions. Get it wrong and the consequences can be catastrophic in terms of financial loss and business reputation. Year after year the threat landscape is widening as fraudsters conceive of more sophisticated methods to compromise payment credentials for monetary gain. The payment industry invests heavily in onward development of an infrastructure which is often referred to as the 'payment rails' and operated by the various global and regional payment brands including American Express, Mastercard and Visa. Hardware-based security (underpinned by rigorous solution certification schemes) is prevalent at multiple nodes in the infrastructure to protect the numerous cryptographic keys that enable participants to transact securely. Compliance with the formal security standards (developed and managed by organizations including EMVCo and PCI SSC) is a pre-requisite.

Thales with its payShield range of payment hardware security modules (HSMs) is a leading supplier to the various issuing banks, acquirers, processors, payment faciliators and payment gateways who play a major role in securing transactions over the payment rails. Increasingly there is now a fundamental need to introduce more sophisticated solutions to secure the rapidly growing volume of online and mobile remote payments which pose new types of threats as the digitization of the end-to-end shopping journey gathers pace. payShield functionality advances on a regular basis to support the latest security standards, especially those connected with mobile transactions, to help mitigate risks for the participants.

In addition to the mandatory infrastructure security, anyone facilitating payment processing needs to be extremely vigilant in how payment information, most notably the customer primary account number or PAN, is secured at all times. The protection of cardholder data and sensitive authentication data plays a major role in the Payment Card Industry Data Security Standard (PCI DSS) which is the primary global payment security mandate with which everyone who transmits, processes or stores cardholder data must be compliant. Various aspects of compliance rely on the use of encryption, key management and secure processing performed using HSMs which align closely to the payment rails infrastructure. However data security is just as important for any organization that needs to store cardholder data as part of its business activities. In these instances the emphasis is on devaluing the sensitive data so that it becomes worthless to an attacker if stolen. The Thales Vormetric Data Security Platform offers a complete suite of technologies to encrypt, tokenize and mask sensitive data so that businesses can concentrate on their core activities in the knowledge that their customer data is secure against compromise from both external attackers and trusted insiders.

This document provides an overview of how organizations can leverage a mixture of the payShield HSM and Vormetric Data Security Platform solutions to provide complete protection of sensitive data as part of their retail card payment processing activities which are linked to a customer PAN. The technology covered is suitable for protecting transactions made using physical plastic cards (contact and contactless), mobile wallet transactions (in-store and remote) and online/e-Commerce browser-based transactions – the common theme being that the transaction is secured end-to-end using a mixture of hardware and software-based cryptography, raising the bar significantly for fraudsters.

What is meant by sensitive data in the retail card payments world?

Payments made using a credit or debit card at a physical point of sale (POS) terminal, online via the internet or mobile app involve various elements of account data that are considered sensitive and need to be protected to reduce the risk of fraud both now and in the future. Although the main components of cardholder data, including the primary account number (PAN), cardholder name and card expiry date, are printed on the physical payment card, their unauthorized capture especially through large data breaches can provide attackers with the information needed to conduct fraudulent transactions.

The PCI SSC (Payment Card Industry Security Standards Council) is the main industry body established to help improve security for payments and especially in protecting the PAN. The PCI DSS (Payment Card Industry Data Security Standard) is the de-facto approach to data protection for the payment industry and it is regularly updated to address new threats. Through a series of specifications and formal tests on components or overall solutions in the payment industry, PCI SSC helps to establish stronger protection for both cardholder data and sensitive authentication data. Just as important as the PAN, it is critical that card authentication codes or values (for example the three digits printed on the signature strip on the reverse side of a card) and PINs associated with individual payment cards are protected at all times.

Account data as defined in the PCI DSS specifications

Cardholder data includes:	Sensitive authentication data includes:
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

The main challenges in keeping payment data secure

There are two distinct aspects to securing the payment transaction end-to-end. The first relates to the security of the payment rails infrastructure, especially the interactions between the participants as the transaction moves from the point of capture/initiation by the cardholder to its final endpoint where it is approved or declined by the issuer or processor.

The second relates to the ongoing protection of data-atrest which applies to most of the participants such as issuers, merchants, acquirers, processors, payment gateways and even the payment networks themselves. By taking a closer look at each of these security requirements, it can be seen that there are distinct challenges and ultimately different potential solutions involved.

The infrastructure challenges primarily are concerned with ensuring the integrity of the physical HSMs and point of interaction (POI) devices (such as point-of-sale (POS) terminals and ATMs) and their associated installation, configuration, management and monitoring on an ongoing basis. Without effective planning and robust security processes and procedures, some of the most difficult tasks include:

- **Preventing compromise of cryptographic keys shared between participants—**weak key management processes or poor key lifecycle management can lead to inherent system weaknesses, making fraudulent attacks easier to launch and risking exposure of critical keys
- **Ensuring only authorized access to HSMs by trusted applications and personnel—**the ability for a privileged user or rogue application to gain unrestricted access to HSMs without suitable authentication could result in a wide range of security compromises such as loading of untrusted keys and software code or the bypassing of proper PIN validation for card transactions, for example
- **Keeping any downtime of the HSM estate to an absolute minimum—**taking HSMs offline in data centers for prolonged periods to facilitate application and security upgrades necessary to mitigate the latest known threats can have a detrimental impact of payment system availability and the ability to process all transactions securely at scale

payShield, the most widely deployed payment HSM in the world

Leading payment application vendors rely on payShield HSMs to offer enhanced functionality to meet the latest security standards in a timely manner. This enables them to provide the strongest protection for the keys and sensitive data they need to handle as part of their transaction switching and authorization solutions.

The data-at-rest protection challenges primarily are concerned with ensuring that any data permitted to be stored under PCI DSS rules achieves suitable and robust protection consistent with the likelihood of fraudulent exposure and the overall impact on the business. Without a coherent data encryption strategy underpinned by strict access control and monitoring capabilities, some of the most difficult areas in securing data include:

- **Limiting the spread of data within your organization—** not knowing where all your sensitive data is stored and failing to adopt proven PCI DSS scope reduction technologies makes your compliance task much more difficult and raises the risk of a serious data breach
- **Restricting access to sensitive data spread across multiple locations—**it is all too easy to end up with a fragmented approach to security based on multiple proprietary vendor solutions and inadequate technologies that are expensive and complex to operate and likely will lead to compliance gaps
- **Mitigating the risk of data compromise by trusted insiders—**sole reliance on basic operating system or database controls as a means of preventing administrators and privileged users from viewing cardholder data is fraught with security loopholes and is a growing threat for many organizations who just treat data security as a 'check box' exercise

Vormetric Data Security, extensible, centralized data-at-rest security

The Vormetric Data Security Platform provides efficient management and use of multiple data-at-rest security solutions built on a common infrastructure with centralized key and data protection policy management. The platform protects and controls access to databases, files and containers—and secures data residing in cloud, virtual, big data and physical environments.

Typical ways fraud can be carried out if payment data is compromised

The most valuable data is the sensitive authentication data for which storage is prohibited under PCI DSS. The creation of a counterfeit magnetic stripe card is possible if a fraudster did manage to obtain the full track data and the PIN for the card, enabling transactions at point-of-sale (POS) to be made or cash withdrawn from ATMs. The typical method used to obtain such data is via interception of the communications between the merchant POS terminal and the acquirer bank network where in many cases the data captured from the card is being transmitted as cleartext. The associated PIN would need to be compromised using a technique such as 'shoulder surfing' or capture through 'skimming' using a compromised POS terminal or ATM, but fraud can still take place without the PIN. The introduction of the EMV chip card as the replacement for the magnetic stripe card in most countries worldwide now, including the United States, has greatly diminished the opportunities to make use of this counterfeit approach since the transaction data present for the chip card is different from that used for magnetic stripe cards and the physical cloning of an EMV chip card is not deemed feasible for fraudsters based on the amount of time, effort and expense involved.

The fraudsters now are concentrating more on just capturing the PAN and card expiry date (present in the track data) through monitoring of network transmissions or stealing from databases where the data protection methods are insufficient. This enables fraudulent 'card not present' (CNP) transactions over the internet or via mail order/telephone order (MO/TO) to take place where the merchant involved does not force the cardholder to either enter the card security code (the 3 digit value printed on the signature panel on the rear side of most credit and debit cards) or authenticate themselves to their bank as part of the 3-D Secure process before the transaction is approved.

It is imperative therefore that the various components of account data receive the appropriate forms of protection throughout their lifecycles to avoid compromise. One of the fundamental objectives of PCI DSS is to make it as difficult as possible for fraudsters to obtain account data that can be used to make illicit transactions. This is accomplished by promoting a coherent approach to sensitive data protection by all stakeholders in the ecosystem with formal compliance against the standard being enforced by the various payment brands.

As the digital transformation of payments evolves, new methods are being utilized by criminals including account takeover and new account fraud to carry out digital commerce fraud. In these cases the initial capture of personal information about the cardholder (possibly through a payment data breach) provides sufficient information to create rogue payment accounts for monetary gain. The challenge again for the payment industry is to devise effective solutions to address this new type of fraud which is a different proposition from the legacy focus on securing physical cards for use in face-to-face environments.

The technology solutions available to protect sensitive data

The payments industry employs three core technologies to protect cardholder data in a mixture of infrastructure and data-at-rest solutions:

- **Point-to-point encryption (P2PE)—**protecting transaction data in motion especially linked to merchant networks where it is most vulnerable to theft
- **Encryption—**devaluing stored transaction data if stolen as part of a major data breach
- **Tokenization—**segregating payment channels to reduce cross–channel payment fraud and supporting merchants who can maintain business processes using a token as a proxy for the PAN

Point-to-point encryption (P2PE)

P2PE is used to protect vulnerable zones or segments in the payments infrastructure. It is almost exclusively used in POS environments to protect data from the point of capture in the merchant environment to the next point of processing which is normally a payment gateway or acquirer. Traditional POS systems are increasingly adopting P2PE to avoid vulnerabilities relating to magnetic stripe and chip card track data being transmitted in the clear. Mobile point-of-sale (mPOS) solutions have really no choice but to deploy P2PE because they involve untrusted devices (mobile phones or tablets) and untrusted networks (the internet) and the risk of mobile malware having access to clear text account data would be unacceptably high.

P2PE encrypts data at the point of capture (i.e. at the POS terminal or mPOS reader) and this data is maintained in an encrypted state thereafter and is only ever able to be decrypted inside the HSM at a payment gateway or acquirer.

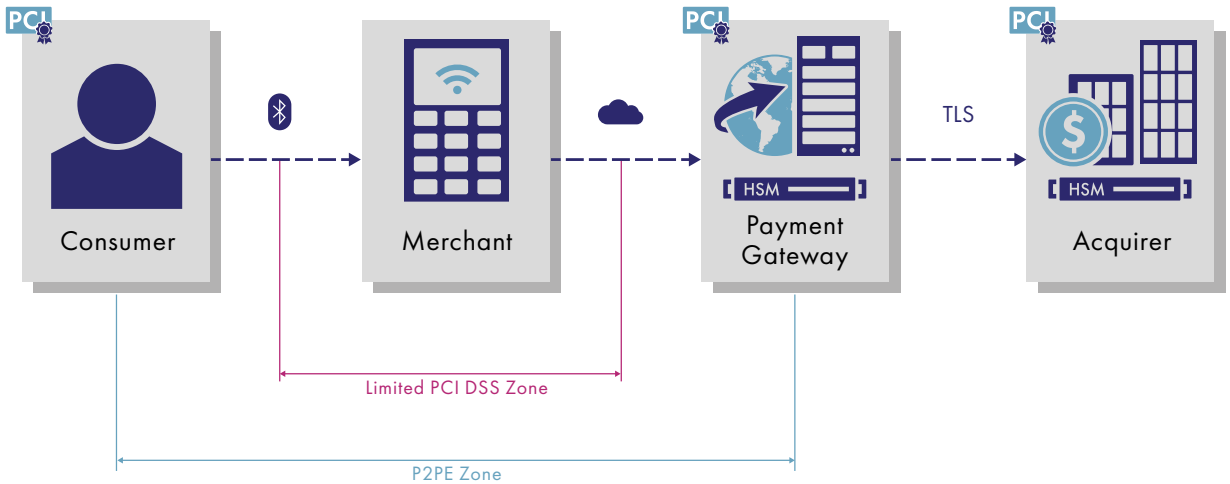
The main point about the use of P2PE is that the merchant has no means to decrypt the data since he does not have access to the necessary cryptographic keys.

P2PE has therefore proved very effective in reducing the scope of PCI DSS compliance for merchants and also devalued data in a segment of the ecosystem where data breaches were becoming widespread and very lucrative for attackers.

Thales payShield HSMs at the heart of POS and mPOS solutions leveraging P2PE

Numerous payment service providers (PSPs) and payment gateways have standardized on payShield HSMs to help improve security, simplify operations and limit liability for their merchants in processing transactions. The HSMs are providing a vital ingredient in increasing their security posture by:

- Reducing the risk of key compromise through proven hardware-based key generation, distribution and management techniques as part of their PCI P2PE implementation
- Helping to meet and demonstrate compliance with stringent PCI key management requirements in a simple and cost effective way
- Facilitating secure PIN processing, compliant with PCI PIN Security requirements, through use of the comprehensive standard PIN management functionality available in the HSM



Encryption

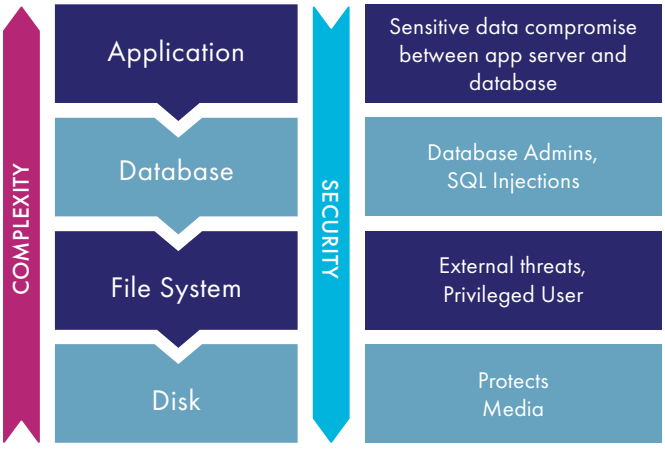
Encryption is used extensively in the payment rails infrastructure as an inherent part of the terminals, ATMs and HSMs deployed by the various participants. Anyone who accepts card payments will be using encryption as part of their system, whether they are aware of this fact or not. The cryptographic algorithms used and the strength of the encryption keys are largely governed by security standards in place linked to the EMV chip card specifications and supplemented by PCI or payment network specifications and guidance. This ensures that any keys shared electronically between participants are protected using strong encryption and any PINs or authentication codes needed to be transmitted through the payment networks for validation are also protected through encryption. The payment processing, switching and authorization applications that are used for transaction processing make use of dedicated functionality in HSMs to achieve their specific encryption requirements which may vary slightly depending on the particular payment brand debit or credit card or mobile device that is being used. Such applications therefore have very tight integration with HSMs and require specific software development efforts. In contrast, general data encryption in the infrastructure automatically takes place using P2PE, TLS or hardware-based network encryption for privacy/confidentiality reasons as part of the connectivity between the various participants without any inherent need for specific application development efforts. In most cases strong key management processes and procedures are essential to underpin the effectiveness of the encryption used in the infrastructure.

Another main use for encryption is to protect data at rest. Its deployment has been accelerated by the increasing demands of the PCI DSS requirements and the desire to devalue data in the event of a data breach. PCI DSS allows merchants to store PANs on their databases as long as they are rendered unreadable by a process such as encryption. Merchants are not allowed to store any sensitive authentication data after authorization, even if it is encrypted. The biggest effort in the industry then is associated with the protection of PANs on databases using an appropriate method of encryption.

PANs can be encrypted at any of the four layers (disk, file, database and application) in the technology stack, each of which provides protection against different threats. The choice depends on your architecture and compliance goals. The Vormetric Data Security Platform offers broad data security options to deliver support across changing architectures and compliance requirements.

Vormetric Data Security Platform data protection products

- **The Vormetric Data Security Manager** delivers operational efficiency with centralized key management and data protection policies for data on your premises or in cloud environments for the following products and others
- **Vormetric Key Management** solutions include cloud- and enterprise key management for Transparent Database Encryption (TDE) keys, KMIP clients, and full key life cycle management for cloud data encryption keys
- **Vormetric Transparent Encryption** offers encryption of structured and unstructured files along with strong privileged user access controls
- **Vormetric Application Encryption** simplifies the process of adding encryption into existing applications



The threats mitigated by encryption on each layer of the technology stack

Tokenization

There are two main types of tokenization used to protect retail card payments. Both methods replace the PAN with a surrogate value (or token) but they have very different objectives and are controlled or used by different participants in the ecosystem:

- **Issuer tokenization—**a payment network initiative for use by issuers based on EMVCo specifications where it is known as 'payment tokenisation'
- **Acquirer tokenization—**a technique used mainly between acquirers and merchants based on guidance provided by PCI SSC as part of PCI DSS scope reduction initiatives for merchants

Issuer tokenization

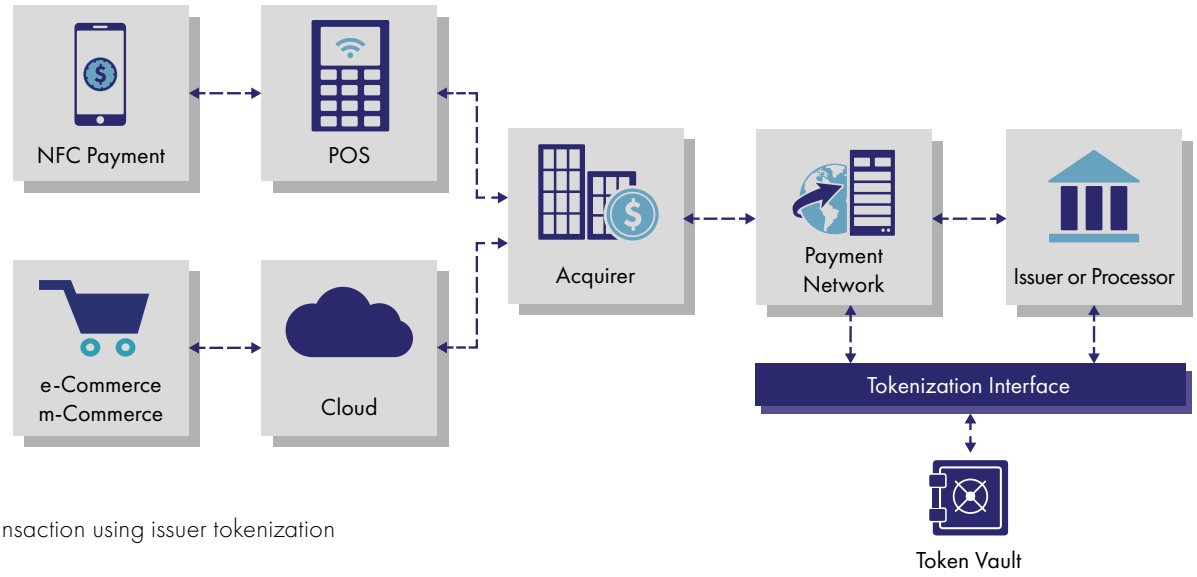
Issuer tokenization is used to segregate payment channels, ensuring that any data breached in one channel is invalid for use in another. Typically, an issuer creates a separate, logically unique token for each payment type or method associated with the same consumer account. Three different tokens, for example, could be assigned to the same payment card account: one for contactless mobile payments in a store, one for use when shopping on the Internet, and one for making payments using consumer devices such as bracelets. The main advantage of using a token rather than the real PAN for the account is that if compromise occurs, only the token needs to be replaced — not the PAN and associated payment card. Individual issuers (or their third-party token service providers) maintain the lookup tables between PANs and tokens for their customers, and protect the PAN in the lookup table by using encryption.

One of the primary benefits is that the tokens created have a similar structure to the original PAN so that the transaction can be routed through the network in the normal manner without the need for any changes to the merchant or acquirer systems. In order to achieve global interoperability, any issuer wishing to deploy tokens rather than PANs in the issuance of their payment instruments (such as mobile applications) need to conform to the detailed requirements in the EMVCo Payment Tokenisation Specification: Technical Framework documentation.

Thales payShield HSMs facilitating secure access to leading payment tokenization services

Issuers and issuer processors can utilize payShield functionality to generate tokens from PANs and retrieve PANs from tokens as part of the secure token service provider (TSP) offerings from major payment brands. Offthe-shelf support for the following solutions is provided:

- American Express Tokenization Service
- Mastercard Tokenization Service as part of the Mastercard Digital Enablement Service (MDES)
- Visa Token Service (VTS)



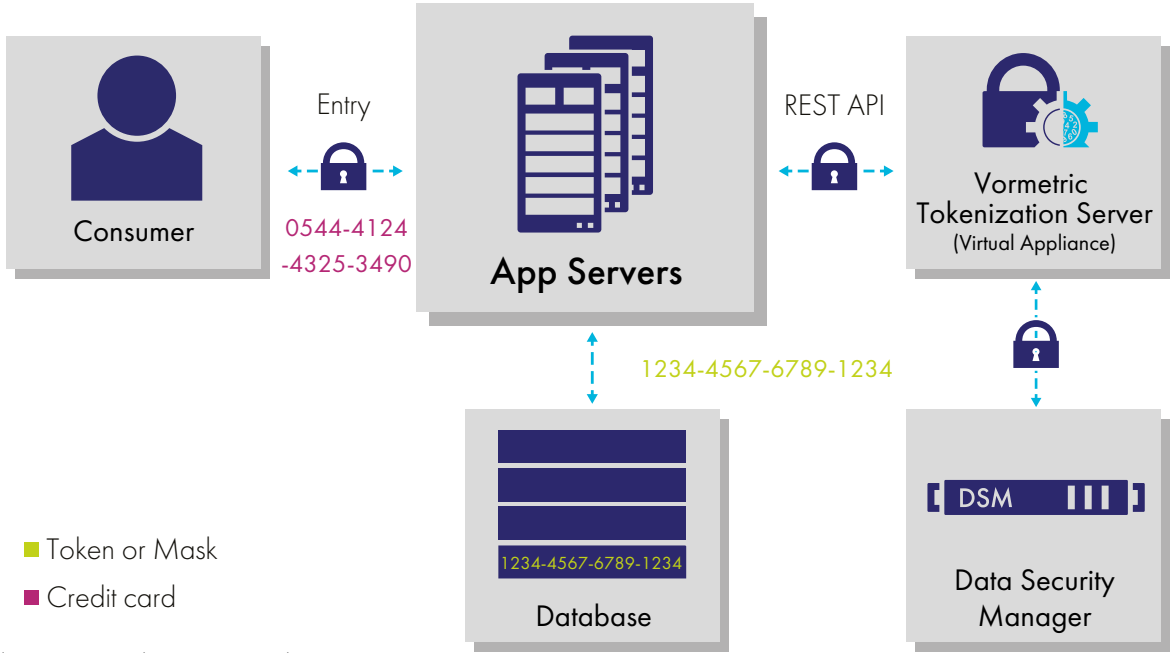
A transaction using issuer tokenization

Acquirer tokenization

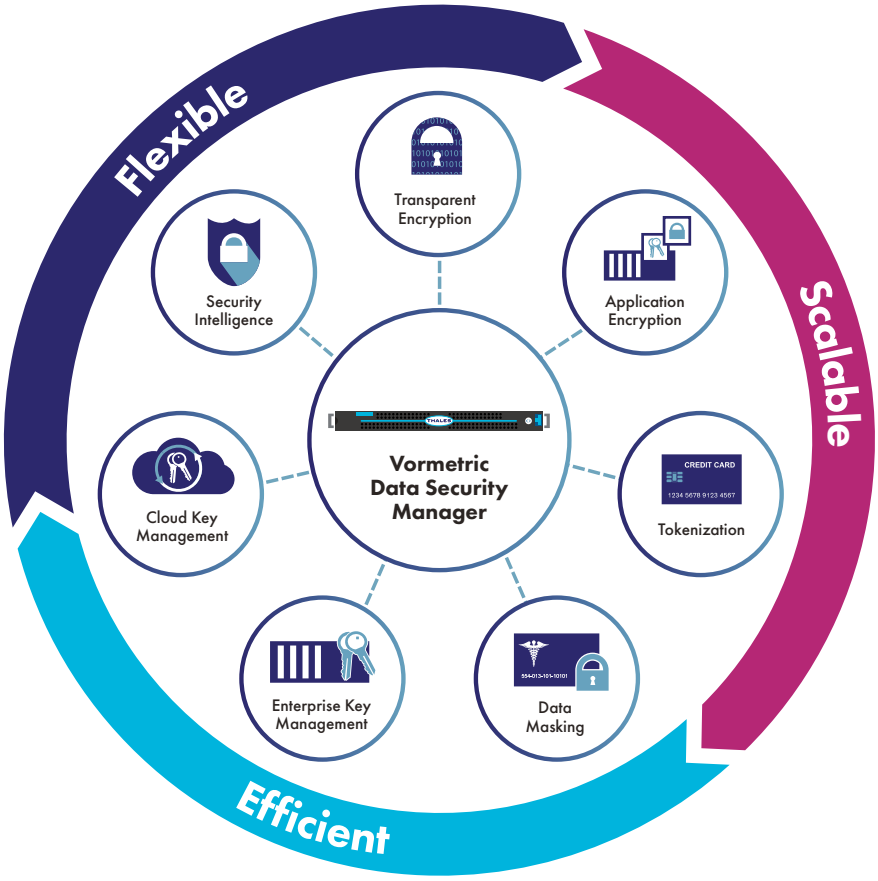
Acquirer tokenization is designed to protect the merchant from data breaches. The merchant doesn't have to store even the encrypted PAN, which reduces its scope for PCI DSS compliance. Typically, the real PAN is used for the payment transaction up to the authorization stage. At the point where the merchant needs to store customer account data to assist with business processes such as chargebacks, after-sales returns, and loyalty programs, a token rather than the real PAN is used. Normally, the token is generated and controlled by the acquirer or the payment network and provided to the merchant as a substitute for the PAN in the authorization response. The main advantages of this system are that merchants reduce their PCI DSS compliance scope, business processes don't have be redesigned, and the risk of exposure of sensitive data is dramatically reduced. Unlike the EMVCo-based payment tokenisation which is a global interoperable standard, acquirer tokenization is not linked to any formal specification or standard (it is just a set of guidelines and recommendations from PCI SSC). As a consequence many different structures and derivation methods will be used throughout the industry – which is not unreasonable considering that it is a distinct service being offered by individual acquirers/processors to their merchant customers and does not need to be interoperable, since the token does not flow through the payment network. The main security focus is in ensuring that only the token service provider (in this case the acquirer or a payment network acting on behalf of the acquirer) can perform the tokenization and de-tokenization processes.

Vormetric Vaultless Tokenization with Dynamic Data Masking efficiently reduces PCI DSS compliance scope

The solution delivers capabilities for database tokenization and dynamic display security. Now you can efficiently address your objectives for securing and anonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments.



Sample Acquirer Tokenization Architecture



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 amount 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.

THALES

Contact us

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

> cpl.thalesgroup.com <