cpl.thalesgroup.com

THALES

Transaction processing using payShield HSMs

Contents

Overview

payShield from Thales is the world's leading payment HSM, helping to secure an estimated 80% of global point of sale (POS) transactions. As the HSM of choice for payment solution providers and payment technology vendors, it delivers proven integration with all of the leading payment applications. It reduces time to market for various participants including issuers and acquirers who rely on robust security when processing retail payment transactions. Since its initial deployment in the early 1980's, the Thales payment HSM family has continued to evolve to support the transaction needs of the payment industry as it moved from magnetic stripe to EMV chip card transactions and then on to proximity payments, based on contactless cards and mobile NFC devices.

Compared with the early Thales payment HSMs, the payShield variant in use today has a more comprehensive command set, contains more sophisticated security mechanisms to prevent fraudulent attacks on the device and delivers significantly higher levels of performance necessary to support the massive increases seen in transaction volumes. Full remote management and monitoring is available to help lower operating costs and provide greater visibility on the HSM estate. Secure host communications offers the ability to deploy devices in more open environments rather than dedicated private network segments.

The growing importance and influence of global standards bodies such as EMVCo and PCI SSC has contributed to significant advances in the cryptographic technology required in payment HSMs and the emergence of more stringent security standards and mandates. payShield has consistently been an early adopter of the latest security methods and offered support for the newest card and mobile applications from the various global payment brands. This document provides an overview of the features and benefits of the payShield transaction processing functionality that is used to help secure the retail payments ecosystem.

The challenges of securing payments end-to-end

Any merchant, acquirer, processor, payment gateway or issuer involved in processing transactions will be very aware of the significant increases in complexity since the days of just having to support face-to-face transactions using initially plastic magnetic stripe cards and then later the chip-based credit and debit cards. There are so many trusted cryptographic zones that need to be established, customer-facing acceptance devices together with HSMs for back-end processing that need to be validated as trustworthy prior to deployment and an increasing range of faceto- face and remote payment methods that need to be supported.

Today we are faced with securing 'card-based' payments from consumer-centric devices (such as smart phones and tablets) that have not been issued by the bank, unlike the case with physical payment cards. Accepting payments originated by IoT devices is a relatively new and fast evolving requirement that introduces new risks and threats. The digitization of cards and their subsequent use in making payments has stimulated much activity recently in the payment security world, impacting everyone who is involved in accepting payments.

The traditional card 'payment rails' managed and operated by the major payment networks (including global organizations such as American Express, Mastercard and Visa) are constantly having to evolve to support more and more sophisticated security and risk management techniques to ensure that the industry minimizes the opportunity for payment fraud and in doing so maintains consumer trust in the payment systems. Processing transactions is a volume business (underpinned by an inherent need for efficiency) but it is important that in facilitating consumer flexibility and a better user experience, the appropriate level of security is enforced which often requires stronger cryptographic algorithms, key lengths and more widespread use of encryption to be implemented.

Some of the top challenges in processing (and ultimately securing) retail payments today include:

- Providing coverage for all the latest applications including both online and offline transaction use cases originating across a range of bank-issued and customer-centric payment instruments—the cryptographic requirements, data to be protected and risk management implications differ even though almost all are based on a consumer account number or PAN

- Ensuring that the infrastructure is robust, protected against fraudulent attacks (especially on sensitive data) and capable of coping with peaks demands in transaction volume—managing necessary changes to keep pace with the latest threats and efficient monitoring that everything is operating smoothly can result in significant effort in trying to achieve 24x7 availability
- Complying with all the latest payment brand security mandates that leverage multiple specifications from organizations including EMVCo and PCI SSC—many now mandate the use of HSMs which require strict key management policies and procedures to be enforced

It is essential that anyone involved in securing the transaction at any stage from its point of initiation or capture until its final authorization by the card issuing bank or issuer processor deploys a flexible, secure, trusted foundation that can evolve as their needs change.

payShield offers processing solutions for multiple types of payment instrument

payShield has helped various participants simplify their integration efforts and lower their operating costs for a wide range of transactions initiated by legacy and emerging payment instruments including:

- Magnetic stripe credit and debit cards
- EMV chip credit and debit cards (both contact and contactless)
- Mobile devices with digitized cards (based on secure elements, host card emulation or native applications)
- eWallets or digital wallets
- Card on file (including tokenised credentials)
- IoT and connected devices used for payments

The off-the-shelf payShield base software contains core functionality that is fundamental to the processing infrastructure, irrespective of the type of payment being processed or payment instrument involved in the transaction:

- Key and certificate management
- Symmetric (DES, TDES, AES), Asymmetric (RSA) keys
- Message encryption/decryption
- Message authentication (MAC, CMAC, HMAC, Hash)
- Digital signatures and verification
- Auditing

This core software is complemented by a range of specific sets of functions that in total cover the full range of card, mobile and IoT payments transactions that apply today. The following list is constantly reviewed and extended as new payment types and security requirements emerge:

- PIN verification and translation
- Card verification codes/values verification
- EMV cryptogram verification and generation
- User authentication
- HMAC and CAP/DPA for 3-D Secure
- Message decryption for P2PE solutions (including FPE)

Key benefits of using payShield for transaction processing

If you are involved in running part of the transaction processing infrastructure, you will know that agility, flexibility, scalability, profitability and security are essential ingredients of your solution. In a conscious effort to meet your needs, payShield continues to evolve, delivering a wide range of immediate benefits including:

- **Early support for the latest card and mobile applications—expanding your payment acceptance**
- **Proven integration with all major certified payment application solutions—reducing your testing time**
- **Performance upgrade without hardware change—supporting your business growth**
- **Comprehensive remote management and monitoring capabilities—lowering your operating costs**
- **Certified to global and regional payment industry security standards—helping you pass your security audits**

Delivering high levels of resilience and availability

payShield has always set the standard for high resilience reinforced by a proven track record of reliability. Some of the main features that help keep your payShield HSM estate up and running include:

- Utilizing dual hot-swappable power supplies and fans and dual host ports for added resilience and redundancy
- Delivering minimal scheduled downtime (through efficient HSM management, configuration and updates)
- Avoiding any client footprint to remove any operating system dependencies which would otherwise result in ongoing updates and security patches
- Minimizing physical interaction with the HSM through a dark data center, no touch approach
- Supporting secure communications between the application and the HSM to ensure only trusted applications have access to its services
- Maintaining secure audit trails of every important security operation to simplify mandatory audit reporting requirements
- Offering payShield Monitor as an optional accessory to assist with capacity planning

Enabling software and performance upgrades to meet new requirements

The processing environment never stands still—both in the increasing number of transactions that need to be processed and the types of payments that need to be addressed. Working closely with the various payment brands, standards organizations and payment security certification bodies, Thales ensures that its payShield platform is kept up to date so that you can process every type of payment possible in the most efficient and secure manner. Some of the major benefits of standardizing on payShield payment HSMs for current and emerging requirements include:

- Software and license upgrades are very simple and quick to apply—you do not even have to visit the data center if you use payShield Manager remote management
- New features are available in a timely manner—we work closely with the various payment brands, obtain their latest specifications and deliver the functionality well in advance to our growing list of technology partners for early integration with their payment application software
- Software license upgrades are available to boost your performance and overall processing capacity—we offer a broad range of performance levels so that you can start low and upgrade later to avoid unnecessary hardware replacement

Offering comprehensive card and mobile application support across all major payment brand

As a volume processor or acquirer of retail payment transactions, you need the broadest possible support of payment applications to maximize your volume and hence profit. payShield HSMs contain functionality that supports the security requirements of payment transactions for all major payment systems across multiple payment instruments. The coverage is always under review and currently includes:

- Contact and contactless card application support for American Express, Discover, JCB, Mastercard, UnionPay and Visa (for both magnetic stripe and EMV chip cards where applicable)
- Secure Element (SE) and host card emulation (HCE) mobile NFC transactions compliant with the proprietary specifications from American Express, Mastercard and Visa
- Payment tokenization services from American Express, Discover, Mastercard and Visa compliant with the EMVCo standard
- Acquirer (or non-payment) tokenization services compliant with the PCI DSS specification and guidelines

Facilitating new services

payShield HSMs live at the heart of the robust payment rails infrastructure, being deployed at many nodes in the various networks including those associated with merchants, merchant processors, payment facilitators, acquiring banks, payment networks, issuer processors and issuing banks.

Different participants often have slightly varying needs as they aim to increase their security posture and minimize risk. The ongoing digitization of retail payments has stimulated innovation in new security approaches in securing the processing infrastructure, with payShield being upgraded regularly over time to support the cryptography and key management requirements of various solutions including:

- Card digitization where the destination could be a mobile device, merchant card on file system or an IoT or connected device for example
- P2PE support mainly for merchant to acquirer/processor segments where the primary driver is to better protect payment data in motion and at the same time reduce scope of PCI DSS compliance for merchants
- Payment tokenization which in addition to being an essential component of some forms of card digitization is also being used as a dynamic way to change the PAN into a token for the bulk of the payment transaction to help protect payment data in motion

In all cases the extensive use of high level functions in the payShield platform has helped remove complexity, both for in-house bank development teams and for integrators offering payment solutions to the market. In addition HSM partitioning (through multiple local master key or LMK support) is an option that has been used successfully by numerous payShield customers to provide secure segregation of applications and tenants.

Simplifying integration

From day one a very important goal for Thales payment HSMs was to simplify the task for anyone who wanted to integrate with them or use them to secure payment transactions. Some of the main things we have done on this journey include:

- Ensuring no host footprint or operating system dependency—we do not want you to have to update any HSM software if your host operating system, application or database for example needs to apply a security patch or enforced functional upgrade
- Supporting all payment system key management methods— making it easy for you to generate, share and use strong cryptographic keys

- Presenting high level functions for integration—eliminating complexity, avoiding you having to read and understand hundreds of pages of complex security specifications while at the same time reducing the number of HSM calls necessary to complete any particular task (and incidentally making the system more secure by avoiding exposure of interim processing steps)
- Allowing cryptographic keys that you need for processing to be stored as cryptograms on external databases under your application control—ensuring that there are no synchronization or scalability issues when you need to support additional HSMs as your processing volume grows
- Maintaining backwards compatibility when we introduce a new payment HSM to our portfolio or expand the command set— ensuring that your existing applications will work seamlessly with both existing and new models of Thales HSMs
- Delivering feature-rich base software that you can use off-theshelf— striving to make our optional customization service the exception rather than the rule

Lowering operating costs

By choosing payShield as your payment HSM platform you will enjoy a variety of benefits that will help reduce your operating costs:

- Configuration is easy when using the payShield Manager graphical interface—we continue to work hard to reduce complexity
- Performance levels can be upgraded at a later stage—we enable you to defer your investment until you really need the extra processing power
- Remote HSM management avoids your need to travel to data centers—we have enabled all functions that you would perform face-to-face to be managed securely from a remote location (at a time convenient to you)
- Background monitoring using payShield Monitor delivers high visibility of all your HSMs 24x7—we make it easy for you to spot potential or real issues quickly and plan more effectively your processing capacity needs
- The payShield HSM is certified against all major global and regional security standards—we help fast track your audit compliance especially the five PCI SSC specifications that mandate use of HSMs (PCI PIN Security, PCI P2PE, PCI TSP, PCI 3DS and PCI SPoC) for which many will apply to you

Thales is in the payments HSM business for the long haul. We have a proven track record of enabling you to maximize the active lifecycle of our HSM product range. This is underpinned by our superior support services, local to you, and covered by our vastly experienced internal team of payment experts complemented by our channel and technology partners. Standardizing on Thales payShield HSMs for all your payment transaction needs is a smart move.

payShield: A flexible, secure platform for all your transaction processing needs

- **Helping you to launch new payment services more quickly**
- **Reducing your ongoing management and security audit costs**
- **Enabling your mission critical environment to run securely 24x7**

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.

THALES

Contact us

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

> cpl.thalesgroup.com <