Thales e-Security

mPOS
Secure Mobile Card Acceptance

More cards, more volume, less cash

White Paper
November 2013
Contents

Scope and Target Audience .................................................. 2
About Thales e-Security .......................................................... 3
   Our payments pedigree ....................................................... 3
The revolution at the point-of-sale .......................................... 4
   Mobility and flexibility ......................................................... 4
   Innovation at the front-end .................................................... 5
   Reducing friction and cost for merchants ................................. 7
mPOS in action ................................................................. 9
   Roles and responsibilities ..................................................... 11
   How it works ................................................................ 12
   Why PSPs need HSMs for mPOS solutions ............................ 13
Thales and its partners driving innovation ............................... 14
   CreditCall ................................................................. 15
   MagTek ................................................................. 17
   Miura Systems ............................................................. 19
   Spire Payments ............................................................. 21
Looking ahead ................................................................... 23
   Scaling to meet increasing transaction demand .................... 23
   Maximizing the value of the HSM ......................................... 23
Conclusion .................................................................... 24
Further information ............................................................ 25
Glossary ........................................................................ 26
Scope and Target Audience

Today there is increasing excitement in the payments industry regarding a new card acceptance solution, providing a compelling combination of flexibility, portability and comprehensive security, all at lower cost than the traditional approach.

The features and functions of point-of-sale terminals used by merchants in ‘bricks and mortar’ stores have evolved gradually over many years with magnetic stripe card acceptance remaining as the baseline. Many countries have already introduced enhancements to support EMV chip card technology and contactless transactions for fraud reduction and consumer convenience reasons respectively. One aspect that remains constant is the strict payment card industry security audit compliance that must be met before any terminal can be used to process card transactions – a highly controlled, complex and costly environment for the participants.

However, outside of the store environment, many merchants are still reliant on cash and do not accept cards at all. Today there is increasing excitement in the payments industry regarding a new card acceptance solution, providing a compelling combination of flexibility, portability and comprehensive security, all at lower cost than the traditional approach. Mobile point-of-sale (mPOS) is the preferred option of numerous micro merchants who are accepting card payments for the first time, opening up significant new opportunities for payment service providers (PSPs) to increase revenue through additional transaction volume. Significantly, existing card acceptance merchants are also adding mPOS to their payment options, mainly because it creates a better interaction experience with the consumer.

The primary goal of this white paper is to outline the significant business opportunity that mPOS represents for PSPs. Based on experience with solutions that are live today, it describes the steps PSPs can take to construct, configure and deliver an mPOS solution to their existing and new customer base of merchants and the associated benefits. Thales e-Security is very active in this market, working with leading card reader vendors to integrate hardware-based key management and encryption technologies. This enables PSPs to get to market quickly with a proven security solution for installation at the payment gateway that supports a wide variety of card readers and their preferred encryption methods. The ability to create a secure infrastructure for mPOS, which uses untrusted devices (mobile phones and tablets) across untrusted networks (cellular, Wi-Fi or Internet), is one of the critical security challenges solved by Thales technology.
About Thales e-Security

Thales e-Security is a leading global provider of data protection solutions with more than 40 years of experience securing the world’s most sensitive information. Our customers – businesses, governments, and technology vendors with a broad range of challenges – use Thales products and services to improve the security of applications that rely on encryption and digital signatures. By protecting the confidentiality, integrity, and availability of sensitive information that flows through today’s traditional, virtualized, and cloud-based infrastructures, Thales is helping organizations reduce risk, demonstrate compliance, enhance agility, and pursue strategic goals with greater confidence.

Our payments pedigree

Designed specifically for payments applications, payShield 9000 from Thales e-Security is a proven hardware security module (HSM) that performs tasks such as PIN protection and validation, transaction processing, payment card issuance, and key management. payShield 9000 is the most widely deployed payment HSM in the world, used in an estimated 80% of all payment card transactions. The payShield 9000 design benefits from over 25 years of Thales experience with payment system security, giving organizations confidence in a state-of-the-art solution that delivers an ideal combination of security and operational ease. The payShield 9000 device is deployed as an external peripheral for mainframes and servers running card issuing and payment processing software applications for the electronic payments industry — delivering high assurance protection for Automated Teller Machine (ATM) and Point of Sale (POS) credit and debit card transactions. The cryptographic functionality and management features of payShield 9000 meet or exceed the card application and security audit requirements of the major international card schemes, including American Express, Discover, JCB, MasterCard, Union Pay, and Visa. payShield 9000 is certified to FIPS 140-2 level 3 and is also available in configurations certified to the PCI HSM v1.0 specification as published by the PCI Security Standards Council.

Through a diverse range of close technology and business relationships, many of them long-standing, Thales e-Security fosters the creation of new solutions and ensures that Thales products can be deployed seamlessly in a wide range of customer environments. Technology partners include solution and application providers, system integrators, and original equipment manufacturers. Partners working in conjunction with Thales on mPOS solutions include CreditCall, MagTek, Miura Systems and Spire Payments.
The Revolution at the Point-Of-Sale

Not many people in the payments industry anticipated the type of disruption that is all too evident at the point-of-sale today. There is now a rapid expansion in choices for paying at the point-of-sale. A key technology behind this innovation is the use of encryption. Although encryption has been used to protect PINs for many years it is now being deployed more broadly to ensure that payments data is protected right from the moment of capture. This opens up a new level of flexibility for both merchants and PSPs because data can now be routed through untrusted devices such as mobile phones and across untrusted networks. The combination of new payments technologies and the ubiquity of the smart phone and tablet are set to change the payments landscape forever.

Mobility and flexibility

Both merchants and PSPs have operational and logistical issues with traditional POS terminals associated mainly with the highly controlled and certified environment in which they must be used. Some of the reasons that traditional POS terminals are either limiting or excluding card acceptance by a wide range of the merchant community include:

• POS terminals generally only work in fixed locations within a store or in limited areas outside where secure wired or wireless network connectivity is available

• Complete POS systems need to comply with payment system rules (including merchant servers, in-store and at head office and the associated software applications that handle transaction data) – the ability to make simple changes is problematic and incurs significant time and materials costs to remain in compliance

• PSPs are responsible for ensuring merchant compliance of a very large and complex system with multiple components, many of which are supplied by the PSP - this results in high cost of entry, preventing tens of millions of micro merchants globally from accepting cards
The complementary mobile option has simple, effective and lower cost attributes that deliver the type of mobility and flexibility that PSPs and merchants crave, but very importantly without degrading security. mPOS enables:

- **Merchants to accept cards for payments any place, at any time where there is internet or mobile connectivity** – the network does not need to be trusted because the data is secured at the time of capture
- **Commercial off-the-shelf smart phones or tablets replace the traditional terminal to offer a rich and flexible user interface to process the payment transaction** – the merchant can now be as creative as desired and integrate with other applications without impacting any payment system compliance
- **Compliance with payment system rules is focused solely on the card reader** – everything else on the communications path between the merchant and the PSP is out of scope for security audits, enabling PSPs to on-board new merchants at minimal cost

### Innovation at the front-end

Components of the mPOS system
Accepting card payments is a complex process involving many participants in the value chain. The whole environment historically has been designed and implemented to manage risk, clearly establish roles, responsibilities and liabilities for fraud with a very stringent approach to the devices and applications that can be used by the merchants. mPOS through its innovative way of redefining the front-end part of the card acceptance process enables merchants to run value-added applications on the mobile device to control and manage things important to them (such as discounts, loyalty points and targeted promotions) while being isolated from any card scheme payment data protection requirements.

PSPs get the best of both worlds with mPOS. Their cost and complexity of equipment supply, security infrastructure overhead and PCI DSS compliance logistics associated with supporting their merchant customers are greatly reduced, leaving them to concentrate on generating new business and handling higher transaction volumes. An added benefit is that the PSP interface to the acquiring network is unchanged. mPOS enables face-to-face card present transactions to be conducted in a highly secure manner. Once the encrypted transaction data is decrypted securely by the PSP using a Thales HSM at their payment gateway, the onward presentation of the data into the acquiring network is the same as it is today for any other transaction originating from a traditional POS terminal. That is one of the key benefits of mPOS for multiple payment stakeholders – mPOS enables higher card volumes from a larger merchant community, significantly improving the often compromised merchant to PSP link, while leaving the proven, low fraud segment unchanged.

Another key advantage of mPOS is that it can support both magnetic stripe and EMV cards. The mPOS revolution started with Square in the United States with a simple low cost plug-in magnetic stripe card reader for a smart phone that enabled micro merchants (such as taxi drivers) an easy entry into the world of card acceptance, offering customers an alternative to paying by cash. Europe followed with slightly more complex and higher cost card readers due to the need to facilitate EMV chip and PIN transactions. For PSPs, operating globally, it means that mPOS can address the needs of all merchants and supports all payment card technologies in use.
Reducing friction and cost for merchants

Merchants dislike the cost and complexity of dealing with PCI DSS compliance – their business is selling goods to make profit, not incurring significant costs to protect payment data owned by card issuers. They need to support all the ways their customers wish to pay to avoid losing business to competitors – card acceptance today is largely a pre-requisite. With traditional POS solutions they are always involved in ensuring that the terminals they use, the software applications they run on their servers and the process they use to transfer data into the acquiring network, directly or via a PSP, meet all the various PCI and card scheme rules and certifications. Card acceptance would be much simpler and less costly if:

- **Merchants had a card acceptance solution that never brought them into scope of PCI DSS in the first place**
- **Merchants already accepting card payments (and hence compliant with PCI DSS) could add a new flexible POS offering to complement their existing infrastructure without adding to their PCI DSS compliance burden**
mPOS enables micro merchants to accept cards for the first time with the benefit of never bringing them into scope for PCI DSS. Since all cardholder data is securely encrypted within the mPOS card reader merchant systems are only exposed to encrypted payment data, which therefore can travel through unsecured devices and unsecured networks. Since the merchant has no access to any keys to decrypt the payment data (they are managed securely by the PSP), the mPOS application running on the merchant smart phone or tablet is not subject to compliance scrutiny and can therefore provide a rich user experience and be tailored to suit individual merchant needs without any restrictions. This is not possible with traditional POS since the user interface is constrained to what is supported by the relatively simple terminal prompt-style interface. Compare traditional POS devices with the latest high-tech graphic capabilities of a modern tablet and it is easy to see why merchants are demanding mPOS now.

Merchants without card acceptance devices that currently phone through card details to their PSP (captured from a face-to-face transaction) gain even more benefit from the use of mPOS. Those ‘card transactions’ are currently treated under card scheme rules as card-not-present (CNP), resulting in higher fees paid by the merchants. The merchants in question when they deploy mPOS will see an immediate financial benefit since the transactions are classified as card-present transactions.
mPOS in Action

Point to Point Encryption (P2PE) Zone

P2PE securing the data from the point of capture to the payment gateway
The mPOS acceptance infrastructure involves three distinct components located between the merchant and the PSP, namely:

1 A card reader owned by the merchant into which the consumer credit or debit card is placed or swiped to initiate the payment transaction

2 A smart phone or tablet owned by the merchant which runs the mPOS payment application which communicates with both the card reader to capture the transaction data and the payment gateway to send the transaction for authorization by the issuer

3 A payment gateway server owned by the PSP which uses a Thales HSM to perform the remote key management for the mPOS card readers and the secure decryption of transaction data received from the merchant before sending to the acquirer for processing

### Roles and responsibilities

<table>
<thead>
<tr>
<th>Participant</th>
<th>Role(s)</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant</td>
<td>Provides a convenient card acceptance method for consumers, leveraging a low cost secure card reader</td>
<td>Install POS payment application on merchant-owned smart phone or tablet&lt;br&gt;Enable card reader to be used by consumer during payment process&lt;br&gt;Adopt best practices to prevent card reader compromise or theft</td>
</tr>
<tr>
<td>PSP</td>
<td>Provides an mPOS acceptance capability for merchants, keeping merchants new to card acceptance out of scope for PCI DSS</td>
<td>Generate and load unique keys into each card reader&lt;br&gt;Secure decryption of transaction data received from merchant&lt;br&gt;Ensure merchant has no access to decryption keys</td>
</tr>
</tbody>
</table>
How it works

Installation and operation of an mPOS system relies on three critical security-related processes:

1. Protecting keys installed in the card reader using strong hardware-based security techniques

2. For PIN-based card transactions, ensuring that the PIN entered by the consumer at the card reader is never available in cleartext form outside the tamper-resistant area of the card reader or an HSM

3. Ensuring that the encrypted transaction data when returned to cleartext by the PSP is not accessible to any unauthorized third party, especially the merchant

The simplest and most cost effective method for a merchant to become equipped to accept mPOS transactions is to source the components from the PSP – the one-stop shop. The PSP supplies the merchant with the card readers, followed by details of how to download the POS payment application from the appropriate web site to the merchant-owned mobile device. There is a separate step to ‘register’ the card readers with the PSP to enable them to process card transactions. Depending on the implementation model adopted by the PSP, the cryptographic keys may already have been generated and loaded into the card readers at the factory prior to secure delivery to the merchant and no more key management is required. Alternatively, the more common approach by PSPs is to ship the card readers without any additional encryption keys loaded – typically just the public key certificates associated with the device manufacturer and the PSP. This enables the merchant device and the PSP to establish a secure session during the merchant registration process. The result is that the initial encryption/decryption key to be used to secure payment transaction data is present within the HSM at the PSP and inside the tamper-resistant card reader device, ready for use by the merchant. The main benefit, whatever method is deployed, is that the process is simple, fast and secure requiring no manual encryption key loading processes.
From the consumer’s perspective, the mPOS transaction looks very much like the traditional POS terminal transaction (except that the experience may be somehow richer) which is important because any requirement to change consumer behavior might negatively impact adoption:

- The card is swiped or inserted into a card reader
- Optionally a PIN is entered
- Visual confirmation of transaction success or failure is displayed on the card reader or the merchant smart phone or tablet

The core differences lie behind the scenes and are invisible to the consumer:

- The card reader communicates wirelessly (or for plug-in variants via the audio port) with the smart phone or tablet – this means that the POS application is no longer loaded inside the card acceptance device, reducing complexity, simplifying EMV/PCI certification and most significantly reducing infrastructure costs for both merchants and PSPs
- The POS application (and by implication the merchant) never sees any cleartext transaction data – point to point encryption (P2PE) is permanently active as the card data is encrypted at the point of capture using the hardware-based cryptographic capability of the card reader
- The P2PE ‘zone’ established between the card reader and the PSP gateway uses payment industry best practices for protecting data – the HSM at the gateway underpins the key management scheme for the P2PE ‘zone’ and ensures that the encryption keys deployed are generated, distributed and used securely, meeting the card scheme rules for unique keys per card reader

Everything from the PSP payment gateway onwards to the issuer stays the same – no need for acquirers, card networks, switches or issuers to make any changes. A transaction originating from an mPOS card reader looks exactly like a card transaction from a traditional POS terminal when it reaches the acquirer. mPOS therefore offers significant benefits in increasing card acceptance with low impact.
Why PSPs need HSMs for mPOS solutions

Many PSPs are involved in the processing of POS card-present and e-commerce card-not-present transactions today and although the use of HSMs is a best practice there is no specific mandate for their use. What is so different about mPOS that makes HSMs now essential?

There are three main reasons why HSMs are needed:

1 **Hardware-based security significantly reduces the risk of key compromise** – the core security value proposition of mPOS is that it uses P2PE (which relies inherently on strong key management) to secure all payment data between the merchant and PSP. HSMs are the only proven method of securing critical keys and cryptographic processes from physical and logical tampering. They are used extensively throughout the payments chain since software-based security is unacceptable.

2 **Managing keys using HSMs is the simplest and most cost effective way of meeting and demonstrating compliance** – keeping the mobile device and merchant environment in general outside the scope of PCI DSS auditing requirements relies primarily on the inability of the merchant to decrypt the encrypted card holder data. If the keys are not generated and protected by HSMs throughout their lifecycle (and instead rely on the properties of software-based systems), the task of proving that the keys are not accessible to the merchant or easy to defeat by a fraudster can be extremely time-consuming, complex and costly. HSMs are mandatory components for payment gateways relying on P2PE for PCI DSS scope reduction – software cryptography is not permitted as part of a PCI P2PE certified solution.

3 **Supporting PIN capability in the card reader automatically means compliance with PCI PIN Security Requirements is necessary** – put simply you cannot meet PCI PIN Security requirements without an HSM (or secure cryptographic device (SCD) or tamper resistant security module (TRSM), as the HSM is sometimes known). Hardware security techniques to generate and manage keys throughout their lifecycle underpin all of the requirements for secure PIN handling. A PSP will be managing the keys installed in the mPOS card reader to perform the initial PIN block encryption and will need to translate the PIN block at the payment gateway before transferring to the acquiring network – it needs access to the keys and hence an HSM to perform this task to meet card scheme rules for handling PINs. Any PSP that translates PIN blocks for traditional POS transactions is already required to use an HSM to satisfy card scheme rules.
In summary, using HSMs as part of the core infrastructure delivers clear benefits for PSPs in three distinct ways.

| Improves security | • Reduces the risk of key or data compromise at the PSP payment gateway  
|                   | • Minimizes the possibility of transaction replay attacks by deploying hardware-generated unique keys per transaction |
| Simplifies operations | • Establishes a central device of trust, the HSM, that can also protect other critical keys and data used elsewhere by the PSP |
| Limits liability | • Removes access to cleartext transaction data for merchants keeping them out of scope for PCI DSS for mPOS transactions and hence reducing PSP risks  
|                  | • Enables PSPs to isolate the merchant domain (the vulnerable part) from the acquirer domain |

**Thales and its Partners Driving Innovation**

Proven solutions incorporating Thales HSMs at the payment gateway help PSPs launch mPOS solutions quickly with the added flexibility of supporting multiple secure card reader options from a wide range of Thales partners. The HSMs are available off-the-shelf, pre-integrated with the specific encryption and key management schemes supported by the different types of card reader available, covering all micro merchant needs and budgets. This ensures easy, flexible, low risk integration at the gateway, shielding the PSP from unnecessary technology complexity. The following pages provide a summary of some of these partners, both white label solution providers and card reader vendors, who are working closely with Thales as part of the rapidly evolving mPOS ecosystem.
CreditCall – Card Acceptance in Store and On The Go

About CreditCall
CreditCall is an award-winning payment services provider with a global reputation for enabling card acceptance in complex and diverse terminal environments. Founded in 1997, the company has a proven track record in creating innovative, reliable and secure card payment solutions that lie at the heart of the payments ecosystem. CreditCall’s product suite covers mobile payments, ecommerce, EMV migration, and unattended payment gateway services.

Solution overview
The CreditCall CardEase Mobile application (www.cardeasemobile.com) enables merchants to use a smart phone or tablet together with a low cost card reader (from leading card reader vendors including MagTek, Miura and Spire) to accept both EMV chip and PIN and magnetic stripe credit or debit card payments on-site. Thales payShield 9000 HSMs are critical components in securing the CardEase Mobile solution by enabling a point-to-point encryption (P2PE) zone to be established between the card acceptance point and the internet-based payment gateway. CardEase Mobile works in conjunction with a merchant account which can be obtained from payment processors such as Elavon and Sage Pay. It is widely sold as a white label solution to banks, acquirers, payment processors and mobile network operators (MNOs), who in turn sell the products and associated services to their merchant customers. The distinct advantage is that CreditCall has full flexibility to support all card readers and all payment processors – no exclusive relationships.

“Thales was an obvious choice for us – best-in-class HSM solutions with wider support and recognition in the payments security arena than any other provider. Hardware solutions are pivotal in making security viable in mobile environments.”

Jeremy Gumbley
Chief Technology Officer – CreditCall
Benefits

- Enables PSPs to support a broader community of merchants in a highly secure manner with low onboarding costs
- Provides merchants a choice of pre-integrated and approved card readers from all leading vendors to satisfy individual requirements and reduce implementation timescales
- Removes costly pre-personalization at the factory or manual installation on the merchant site by using Thales HSMs to deliver secure remote key injection for the card readers
- Keeps mPOS merchants out of scope for PCI DSS compliance by ensuring that all sensitive data is encrypted using proven and certified hardware-based techniques
- Thales payShield 9000 HSMs provide CreditCall with more robust protection and management of encryption keys than competitive solutions
MagTek – Open Source P2PE terminals for independent Payment Gateways

About MagTek

Since 1972, MagTek has been a leading manufacturer of electronic devices and systems for the reliable issuance, reading, transmission and security of cards, cheques, PINs and other identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Its products are used worldwide by financial institutions, retailers, hotels, law enforcement agencies and other organizations to provide secure and efficient electronic payment and identification transactions.

Solution overview

DynaPro®Mini, along with the appropriate application supplied by the PSP, turns the merchant smart phone or tablet into a highly secure mobile payment system allowing acceptance of credit or debit card payments anywhere. Certified to the latest PCI PTS 3.1 specification, DynaPro Mini is a highly secure multi-functional mobile device supporting both magnetic stripe and EMV Chip & PIN card transactions. DynaPro Mini meets PCI P2PE requirements and is compatible with Apple iOS, Android and Windows devices, connecting via Bluetooth or USB HID. A version is also available with a direct connection to Apple devices via the Apple connector and, through a range of brackets, fits all Apple mobile devices including the iPod Touch, iPhone3, iPhone4, iPad, etc. All communication both internally and externally is highly secure, using 3DES and DUKPT key management, exceeding the requirements of PCI DSS. DynaPro Mini enables low cost terminal deployment with remote terminal configuration during installation. The business model is such that there are no ongoing costs of terminal ownership.

“The industry is migrating towards P2PE and PSPs are busy defining their roadmaps. MagTek’s next generation, Open Source P2PE hardware devices along with Thales payShield 9000, provides independent PSPs with a comprehensive proven P2PE solution.”

Steve Poulston
Managing Director – Europe at MagTek
Benefits

• Meets PCI P2PE encryption requirements, bringing many operational, security and cost of ownership benefits both to merchants and PSPs

• Works in a consistent way with other MagTek merchant solutions enabling all transactions to be routed via a single payment gateway

• Removes the need for initial loading of cryptographic keys into the terminals at the merchant site due to pre-installation at the MagTek PCI-certified key loading facility

• Reduces the time to market for PSPs to deploy an HSM at the gateway when using Thales payShield 9000 which is plug and play compatible with Dynapro® data formats

• Enables merchants to sign multi-country acquirer contracts and deploy the terminal into any country safe in the knowledge P2PE keeps them out of scope for PCI DSS certification
Miura Systems – Powering Payments

About Miura Systems

Miura Systems is a leading provider of secure mobile electronic payment hardware with core competency in design, certification and manufacture. Its card-based mobile payment solutions are revolutionising the way consumers pay for goods and services by replacing the need for traditional static POS terminals with secure portable card readers. Miura partners with Independent Software Vendors and Systems Integrators to provide rich and flexible payment solutions for global retail, hospitality, financial, government and healthcare markets.

Solution overview

The flagship product of Miura Systems is the Shuttle device which is an innovative mPOS PIN Entry device (PED) connecting securely via Bluetooth to all types of smart phones, feature phones and tablets. The Shuttle range of devices is certified to the latest payment industry and card scheme security requirements, providing EMVCo Level 1 and Level 2 certified components in addition to a flexible mobile-centric API for integration with partner solutions. The Shuttle delivers a familiar secure payment experience within a small form factor with portability benefits suitable for market sectors ranging from the micro-merchant all the way up to enterprise and traditional retail. Miura supplies its solutions via both traditional merchant acquiring and PSP/Gateway solution providers in addition to new market entrants such as PSPs experienced in e-commerce wishing to add face-to-face payments to their merchant offering. In conjunction with Thales, Miura has developed simple plug-and-play approaches to remote key injection and P2PE implementations using payShield 9000.

“Miura has developed an innovative approach to delivering the highest levels of card payment security for its partners. By working with Thales, Miura has been able to simplify and remove the complexity of delivering leading P2PE and Remote Key Injection services for mPOS solutions.”

Andrew Hodges
Chief Technology Officer – Miura Systems
Benefits

• Supports a wide range of mobile devices and operating systems through its Bluetooth connectivity feature, leveraging P2PE for security

• Minimizes cryptographic knowledge requirements for PSPs by providing proven sample code and a test environment to simplify integration effort

• Reduces time to market through pre-integration with Thales payShield 9000 for encryption, remote key injection and PIN processing services

• Complies with card scheme security audits through certification to PCI PTS 3.x, SRED and Open Protocols

• Delivers future-proofing and expandability enabling PSPs to address multiple tiers of merchants with different hardware offerings based on a single integration investment

About Spire Payments

Spire Payments is an independent provider of point-of-sale hardware and software solutions, supplying a comprehensive range of fixed, portable and mobile payment terminals, together with PIN pads and unattended devices for integration with cash register systems and self-service kiosks. With many of Europe’s top financial and retail organisations among its customers, Spire Payments has been at the forefront of electronic payments for over 30 years. Ranked the third largest POS vendor in Europe (Nilson Report 2012), Spire Payments is committed to delivering best-in-class products and services, with the highest levels of security at a competitive total cost of ownership.

Solution overview

PosMate®Smart, the world’s first fully-certified chip and PIN mPOS terminal, allows merchants to accept card payments securely in a mobile environment. Designed to complement recognized payment applications residing on compatible mobile devices (smart phones, tablets or PDAs), the PosMate®Smart solutions are both robust and simple to use. Solution providers benefit from reliable and secure payment processing through the use of encrypted Bluetooth technology to interface to the merchant mobile device of choice. To ensure maximum security against possible data fraud the PosMate®Smart terminal is equipped with the highest standard of hardware and software security features compliant to PCI PED 2.0 and is EMV level 1 and 2 certified. There are active deployments in multiple geographical regions, supported by central gateways utilizing hardware security modules including the Thales payShield 9000.

In addition to transaction processing, Spire Payments works with its integration partners to deliver a gateway infrastructure providing terminal management, merchant on-boarding capabilities and merchant portals to view financial data.

“mPOS is a significant disruptor within the electronic payments space. Forward thinking, nimble businesses such as Thales e-Security and Spire Payments see this as a perfect opportunity to form strategic relationships to deliver secure, trusted and reliable mPOS solutions.”

Nigel Dean
International Marketing Manager – Spire Payments
Benefits

• Incorporates traditional PIN Pad design together with backlit keys and a graphic display to enhance the ease of use for consumers

• Delivers a robust certified card reader solution with long battery life creating greater flexibility for merchants

• Supports an open SDK for rapid third party development with associated consultancy and training services available from Spire Payments to reduce risk and implementation costs

• Provides multiple options for receipts, supporting hard copy printing, email and SMS text delivering maximum flexibility for merchants and consumers

• Minimizes time to market through comprehensive experience with proven mPOS solutions involving multiple integrators and merchants
Looking ahead

Scaling to meet increasing transaction demand

Globally mPOS is expected to bring tens of millions of new merchants into the card acceptance market. The thousands of PSPs involved each need to be ready to support hundreds if not thousands of merchants. How can this be achieved in a secure manner and without any performance bottlenecks?

For the merchant, the mPOS card reader and the associated smart phone or tablet are very much personal devices with a one-to-one relationship. Both scalability and performance are not issues that the merchant community can control directly in terms of processing an mPOS transaction. It is the responsibility of the PSP to ensure that transaction processing is not degraded as more and more merchants are added to the system. There are two main challenges for PSPs in this respect: ensuring that the HSM at the payment gateway has sufficient capacity to process additional encrypted transactions and avoiding system downtime as new merchants are added.

Thales payShield 9000 HSMs have performance levels that can be upgraded under software license control – this has the distinct advantage of enabling the PSP to reduce initial system costs and defer introducing higher performance processing capability until transaction volumes increase. payShield 9000 has in-built diagnostic facilities that provide clear indications of the spare processing capacity of the HSM, enabling timely upgrades to take place which can be installed remotely without any system downtime.

Maximizing the value of the HSM

The mPOS revolution is only just beginning and PSPs can build on their use of HSMs at the payment gateway for mPOS to secure other parts of their payment infrastructures, improving security and often lowering operating costs.

One area stimulating interest is in securing all transaction data – not just the basic card holder data between the card reader and the PSP. Early mPOS solutions typically just encrypt the primary account number (PAN) and create a hash of the overall message – simply because this is the bare minimum necessary for PCI DSS compliance. Since the PSP is in control of the POS application and the corresponding code running on the card reader device to handle the encryption and key management, an opportunity exists to use stronger message authentication codes (MACs) to ensure the message is not altered during transmission and hardware-based encryption of the overall message to provide additional privacy. The core infrastructure to provide the additional cryptographic capabilities is easy to achieve using proven security methods similar to those used to create and load the initial P2PE encryption key.

Another area where PSPs can derive additional value from their use of the HSM is in protecting stored data, in particular the cardholder data that has been decrypted from the merchant. Typically this data is subject to PCI DSS compliance and historically PSPs involved mainly in e-commerce transactions use software-based encryption to protect it. When rolling out an mPOS solution many PSPs will be deploying HSMs for the first time and will be able to take advantage of the device to protect these other cryptographic functions, dramatically increasing their security posture and simplifying their compliance reporting obligations.
Conclusion

mPOS is revolutionizing the consumer’s point-of-sale experience. Micro merchants are now able to accept cards for the first time at any place, removing dependency on cash transactions while meeting customer expectations and avoiding lost sales opportunities where the customer wants to pay by card. Established ‘bricks and mortar’ merchants are now able to add new low cost and flexible card acceptance options to their in-store experience, helping to enrich the customer shopping experience.

mPOS helps PSPs to increase their revenue through expansion of the merchant base who accept cards for face-to-face transactions. The inherent need to secure the payment data is no longer constraining the solution or dominating the costs. Merchants get the POS interface they need, with the flexibility to enhance or change at will. The PSP obtains a secure, low cost, fast track method for on-boarding new merchants. The threat of a security breach threatening to destroy the organization is significantly reduced.

Hardware-based security underpins the whole mPOS ecosystem. Secure card readers encrypt the card data at the point of capture for both magnetic stripe and EMV chip cards. Hardware-based point-to-point encryption keeps micro merchants out of scope for PCI DSS and does not add to the PCI DSS burden for merchants already accepting cards using traditional POS terminals. HSMs improve security, simplify security audit compliance and limit liability for PSPs.

Thales has significant experience in supporting both pre-integrated packaged mPOS solutions leveraging its payShield 9000 HSM family of devices and in-house PSP proprietary solutions based on its general purpose nShield HSM product line. Thales and its numerous global partners are available now to help PSPs enter this exciting new world. mPOS is here, now and is proven. The opportunity for PSPs is immense.
Further information

Content relating specifically to mPOS can be found on the Thales e-Security web site at locations including:

- mPOS solution page
  www.thales-esecurity.com/solutions/by-technology-focus/mpos-security
- payShield 9000 product page
- nShield product page
- Security blog
  www.thales-esecurity.com/blogs
- Technology partner section
  www.thales-esecurity.com/partners/technology-partners
- Case studies
  www.thales-esecurity.com/knowledge-base (keyword: mPOS)
- Press releases
  www.thales-esecurity.com/company/press

Thales partners working in the mPOS market have various useful articles and documents including:

- CreditCall
  www.creditcall.com
- MagTek
  www.magtekeurope.com
- Miura Systems
  www.miurasystems.com
- Spire Payments
  www.thyron.com and www.spirepayments.com/home.html

Industry organisations and standards bodies provide good sources of information at the following locations:

- Visa Ready mPOS program
  www.technologypartner.visa.com/mPOS
- MasterCard mPOS Best Practices program
  www.mastercard.com/corporate/mpos.html
- MasterCard Mobile POS Best Practices document

There are various portals and blog sites that regularly cover mPOS activities including:

- Finextra
- The PAYPERS
  www.thepaypers.com/voice-of-the-industry
- mPOS tracker on PYMTS.com
  www.pymnts.com/briefing-room/mobile/MPOS-Tracker
- Consult Hyperion blog
  www.chyp.com/media/blog
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNP</td>
<td>card not present</td>
<td></td>
</tr>
<tr>
<td>DUKPT</td>
<td>derived unique key per transaction</td>
<td></td>
</tr>
<tr>
<td>EMV</td>
<td>Europay MasterCard Visa</td>
<td></td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
<td></td>
</tr>
<tr>
<td>HSM</td>
<td>hardware security module</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>message authentication code</td>
<td></td>
</tr>
<tr>
<td>mPOS</td>
<td>mobile point-of-sale</td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>near field communications</td>
<td></td>
</tr>
<tr>
<td>P2PE</td>
<td>point-to-point encryption</td>
<td></td>
</tr>
<tr>
<td>PAN</td>
<td>primary account number</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>payment card industry</td>
<td></td>
</tr>
<tr>
<td>PCI DSS</td>
<td>payment card industry data security standard</td>
<td></td>
</tr>
<tr>
<td>PCI P2PE</td>
<td>payment card industry point-to-point encryption</td>
<td></td>
</tr>
<tr>
<td>PCI PA DSS</td>
<td>payment card industry payment application data security standard</td>
<td></td>
</tr>
<tr>
<td>PCI SSC</td>
<td>payment card industry security standards council</td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>personal identification number</td>
<td></td>
</tr>
<tr>
<td>POS</td>
<td>point-of-sale</td>
<td></td>
</tr>
<tr>
<td>PSP</td>
<td>payment service provider</td>
<td></td>
</tr>
<tr>
<td>RNG</td>
<td>random number generator</td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td>secure element</td>
<td></td>
</tr>
<tr>
<td>SRED</td>
<td>secure reading and exchange of data</td>
<td></td>
</tr>
<tr>
<td>TRSM</td>
<td>tamper resistant security module</td>
<td></td>
</tr>
</tbody>
</table>
About Thales e-Security

Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United Kingdom and United States.

For more information, visit www.thales-esecurity.com