January 2015

Heartland

Getting Out of PA-DSS Scope and Eliminating the High Cost of EMV:

What you need to know

Mike English
Executive Director, Product Development
Heartland Payment Systems

There are four major concerns every Value-Added Reseller (VAR), Independent Software Vendor (ISV), and businesses with "homegrown" POS systems that accept cards has today:

- *The high cost of achieving and maintaining PCI, specifically PA-DSS validation and compliance*
- *Keeping current with changes in payment technology and mandates*
- *The risk of having your customers' card data hacked/stolen*
- *The high cost and complexity of developing and certifying EMV*

Heartland has solutions for VARs, ISVs and businesses accepting cards that eliminate the risk of stolen data and eliminate a POS system's PA-DSS scope as well as pave a road to seamlessly implementing EMV. This paper offers third-party POS providers, VARs, ISVs, and businesses with "homegrown" payment acceptance the information they need to manage cost and compliance.

EMV Is Here and Is Costly to VARs, ISVs and Businesses with "Homegrown" POS

With EMV[1] timelines quickly approaching for the restaurant, retail, petro and convenience industries, POS system providers, pump providers, merchants and businesses are preparing for the October 2015 liability shift for in-store systems and the October 2017 liability shift for automated fuel dispensers (AFDs). As businesses become acquainted with EMV and the necessary system enhancements to support EMV, they soon learn that EMV can be a time-intensive and costly endeavor.

In a traditional configuration, after integrating EMVCo-certified payment peripherals and updating systems to accept and manage EMV transactions, the merchant or vendor will connect to the acquirer or processor's certification environment, which is linked to the EMV certification test systems for Visa, MasterCard, American Express and Discover. Using an EMVCo-certified Level I and II device, the vendor or merchant will need to run about 120 test transactions for contact EMV and 150 test transactions for EMV contactless to obtain certifications.

For a POS system, costs include the first contact-only EMV POS certification fees, plus any fees charged by a processor to support the certification. This does not include the cost of EMV transaction management code development, POS upgrades, installation, or other necessary expenditures. Optimistically, the time frame to code, test and certify for EMV is more than seven and a half months. However, the initial development and certification will likely take longer because of the intricacies in online and offline PIN management that take time to code and test. Also, many parts of this certification process and cost need to be repeated for each processor and each card brand to which the POS system certifies. To a degree, each POS or AFD configuration must also be repeated. The time frame indicated includes only EMV credit because open questions related to EMV debit haven't been resolved by the industry. The cost for EMV certification is staggering—tens of thousands of dollars.

[1] EMV stands for Europay, MasterCard and Visa, a global standard for interoperation of integrated circuit cards (IC cards or "chip cards") and IC card-capable point-of-sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

There Is a Better Road to EMV

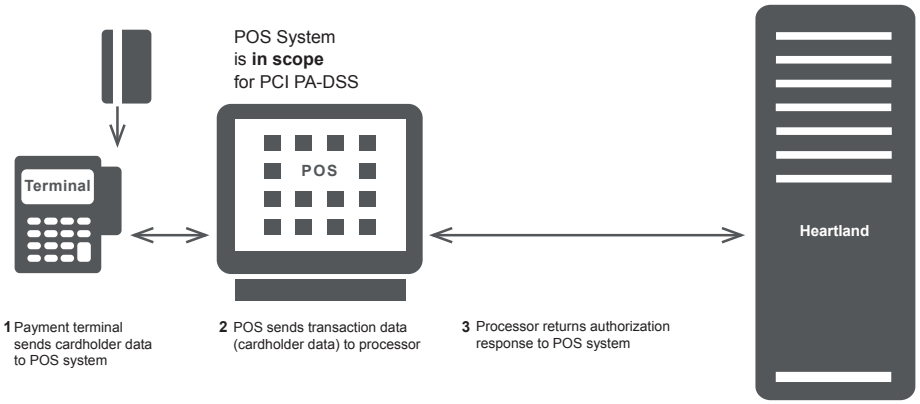
Fortunately, there is a way to eliminate the cost, time and complexity of EMV development and compliance. While not new, an Out-of-Scope approach to in-store payment has taken on new value as a solution for EMV acceptance and as a way to take a POS system out of PA-DSS scope.

In a traditional POS system configuration, the PIN pad is directly connected to the POS system and sends the payment information to the POS for authorization. The POS system receives the authorization back from the acquirer or processor and concludes the transaction. In this configuration, the POS system is in PCI PA-DSS scope and the POS system is responsible for EMV certifications.

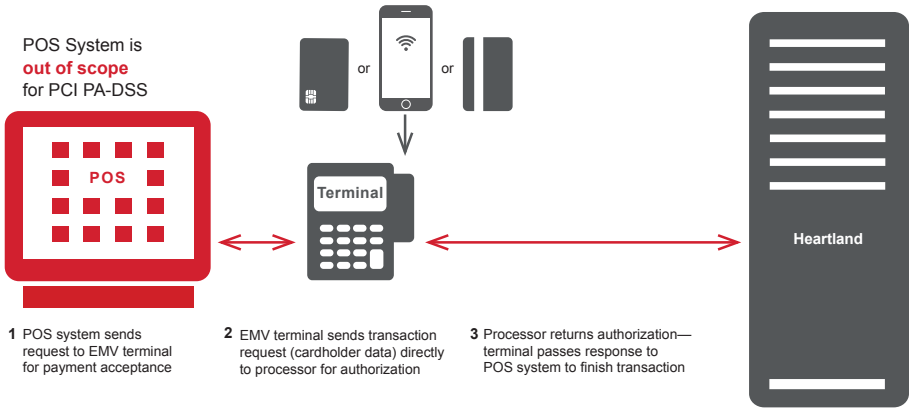
In an Out-of-Scope configuration, the PIN pad or signature capture/PIN pad receives a prompt from the POS system to start payment acceptance, and instead of sending the payment information to the POS, the PIN pad sends the transaction directly to the acquirer for approval. In this configuration, manual entry can be done on the PIN pad to keep the POS system out of PA-DSS scope.

The PIN pad receives the authorization response back from the acquirer or processor and passes it on to the POS system. This configuration takes the POS system out of the payment authorization process. The POS is notified of the transaction, but no cardholder data is sent to the POS, thus taking the POS system out of PA-DSS scope.

Traditional Payment Configuration



Out-of-Scope Configuration



The value of an Out-of-Scope configuration for a POS provider and the merchant is immense. When integrating EMV support with acquirers and processors, third parties and merchants incur a high cost per endpoint to become EMV-certified. The Out-of-Scope configuration eliminates the need for the POS system to code for EMV, as well as removes the need to certify the POS system to the card brands for EMV. Why? Whoever wrote the payment application residing on the PIN pad in an Out-of-Scope configuration is responsible for EMV certification. The POS system may still need to be certified to the acquirer or processor, but the process takes far less time and not for EMV. The POS system simply makes calls to the payment device to begin the payment acceptance process.

Seamlessly Implementing EMV Has Immense Payback

- Our Out-of-Scope offerings eliminate the need for POS systems to develop for EMV acceptance and incur card brand certification costs
- Speeds time to market and greatly reduces development costs associated with EMV support
- Eliminates the POS systems' need to support current and future payment mandates
- Solution can get VARs, ISVs and businesses with a "homegrown" POS system to market with an EMV solution quicker than their competitors

> *"…most PA-DSS certifications cost at least $30,000 or more depending on the complexity of the application and the number of platforms involved…"*[3]

Getting and Staying PCI Out of Scope

An Out-of-Scope configuration eliminates the POS system's PCI scope, specifically PA-DSS[2] scope. When payment services are provided as part of the POS system, the POS system provider incurs costs to become PA-DSS validated as well as continual costs to maintain card brand mandates. In the case of an Out-of-Scope configuration, PCI scope is maintained by Heartland and our solution partners, alleviating that burden from the POS system.

- Eliminates POS system's PA-DSS scope by removing acceptance and management of card data
- The VAR or ISV's scope is eliminated if all card acceptance and processing are completed at the acceptance device
- Without card data, the POS is no longer considered a payment application

Eliminating card data does not take a merchant out of PCI scope, but does significantly reduce their PA-DSS scope. The merchant's PCI scope is reduced when encrypting card data and eliminating PA-DSS. The number of PCI SAQ P2PE-HW questions to which a business need to respond from 230 to 18![4]

For businesses with an in-house POS solution, Heartland Secure and an Out-of-Scope configuration take major portions of your infrastructure out of PA-DSS scope and minimize PCI compliance to the very basics of perimeter security. Providing that the business no longer has access to any clear text card data, overall PCI scope and associated costs are reduced by 70-80%.

---

[2] Payment Application Data Security Standard (PA-DSS) is a set of requirements that are intended to help software vendors develop secure payment applications that support PCI DSS compliance.

[3] http://pciguru.wordpress.com/2010/04/10/open-source-pa-dss-certification/

[4] http://pcisecuritystandards.org/documents/PCI_SAQ_P2PE-HW_v2.pdf

Heartland Secure

At the core of this powerful PCI avoidance offering—and seamless manner of implementing EMV—is Heartland Secure. Heartland Secure consists of E3 end-to-end encryption, EMV and tokenization. It eliminates PCI scope by encrypting card data within a secure acceptance, thus taking the card data out of the transaction and the business's ecosystem.

Heartland Secure is what PCI was meant to be—helping merchants and businesses manage the risk of payment acceptance through the removal of card data from the merchant's network. Heartland Secure. No card data. No risk.

Heartland SECURE

Encryption's Impact on PCI Scope Reduction

Heartland Secure and our Out-of-Scope solutions do not remove a merchant from the requirement to be PCI compliant. A merchant is responsible to validate compliance to their acquirer, often through a qualified QSA or ISA. As stated earlier, the merchant's PCI scope is greatly reduced when encrypting card data and eliminating PA-DSS. These actions reduces the number of PCI SAQ P2PE-HW questions to which a business needs to respond from 230 to 18! It is important to note that PCI DSS always applies to any and all merchants that accept card data. All applicable PCI DSS requirements for card data in scope apply if the following is true:

- If encrypted cardholder data is stored on a system, media or environment that also contains the decryption key
- If encrypted data is accessible to an entity that also has access to the decryption key

The vast majority of breaches occurred at businesses with fewer than 1,000 employees. The average cost per breach for an SMB is up to $500,000, forcing many out of business. Heartland Secure protects a business and their customers' card data from breaches through end-to-end encryption, EMV and tokenization.

When Is Encrypted Cardholder Data Out of Scope?

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable in order to meet PCI DSS Requirement 3.4. The PCI SSC states, "Encrypted data may be deemed out of scope if, and only if, it has been validated by a QSA or ISA that the entity that possesses encrypted cardholder data does not have the means to decrypt it."

If a merchant encrypts cardholder data but does not possess the means to decrypt it, the cardholder data is not considered in scope once it has been encrypted. The best means to encrypt cardholder data is within a terminal or PIN pad that is PCI PIN Transaction Security (PTS) certified.

- An encrypted PAN is still defined as cardholder data and in scope for PCI DSS compliance if the merchant has access to key and ability to decrypt data
- If a merchant has no ability to decrypt encrypted data, the encrypted data is not card data and is NOT in scope of PCI
- Systems that transmit, process and store such encrypted data are not in scope
- Encryption removes clear text card data at point of entry to eliminate PCI scope risk
- By removing clear card data from the merchant's environment, the opportunity for monetization of the card data is also eliminated

Tokenization's Impact on PCI Scope Reduction

Tokenization, which is a way of replacing sensitive data like credit card numbers with tokens, is one of the data protection and audit scope reduction methods that is recommended by PCI DSS.[5] The use of tokens for post-authorization operations such as returns, chargebacks, recurring payments, sales reports, analytics or marketing programs eliminates the storage of the PAN and subsequent use of the PAN. Tokenization takes applications and systems for these business processes out of PCI scope.

However, per the *Information Supplement: PCI DSS Tokenization Guidelines* that were published by PCI in August 2011, "Tokenization solutions do not eliminate the need to maintain and validate PCI DSS compliance, but they may simplify a merchant's validation efforts by reducing the number of system components for which PCI DSS requirements apply."[6]

Per the *PCI DSS Tokenization Guidelines*, PCI Data Security Standard (PCI DSS), Version 2, published in August 2011:

In PCI scope…

- All elements of the tokenization system and tokenization process, including de-tokenization and PAN storage, are considered part of the cardholder data environment (CDE) and are in scope for PCI DSS
- Any system component or process with access to the tokenization system or the tokenization/de-tokenization process is considered in scope

Out of PCI scope are system components that...

- are adequately isolated from the tokenization system and the CDE
- store, process or transmit only tokens
- do not store, process, or transmit any cardholder data or sensitive authentication data
- may be considered outside of the CDE and possibly out of scope for PCI DSS

Heartland's Comprehensive Breach Warranty

Unparalleled in the industry, Heartland is offering merchants the first-ever comprehensive breach warranty. Going beyond breach insurance, Heartland's warranty protects businesses from being financially liable in case of a breach of card information.

To be covered under the warranty, a business must have a Heartland Secure-certified device and process payments through Heartland.

The Heartland breach warranty is straightforward. In the case of expenses incurred due to a data breach of card information, Heartland will reimburse the merchant for all costs, compliance fines and penalties a merchant must pay to the card brands, issuing bank or acquiring bank as well the amount paid for a directly related forensic audit conducted by a Qualified Incident Response Assessor.

Summary

As a leader in secure payment acceptance, Heartland has solutions for VARs, ISVs and businesses accepting cards that eliminate or reduce scope as well as pave the path to seamlessly implementing EMV. We are working with leading hardware vendors as well as strategic third parties to help reduce the cost, complexity and risk associated with PA-DSS compliance and EMV acceptance.

Combined with Heartland Secure, our solutions, and our partners' solutions, we help our customers to be more secure in knowing that Out of Scope is a reality and EMV does not need to be painful.

---

[5] https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

[6] https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf