Payment Card Industry (PCI)

Point of Interaction (POI)

Frequently Asked Questions

May 2013

Table of Contents

PCI and POI Security Requirements

Q What part of the payment transaction is addressed by the PCI POI Security Requirements?

A *PCI POI Security Requirements are primarily concerned with device characteristics impacting the security of the POI device used by the cardholder during a financial transaction. The requirements also include device management up to the point of initial key loading, but the evaluation process only addresses device characteristics.*

- ***Device characteristics*** *are those attributes of the POI that define its physical and its logical (functional) characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device—for example, the penetration of the device to determine its key(s) or to plant a PIN-disclosing "bug" within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a clear-text PIN-encryption key.*
- ***Device management*** *considers how the POI is produced, controlled, transported, stored, and used throughout its lifecycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.*

Q What mandates does PCI SSC have for PCI POI compliance?

A *PCI SSC only publishes the PCI POI Security Requirements and associated testing procedures. Compliance dates for PCI POI devices will be set by each of the individual payment brands.*

Q What are the costs to vendors for evaluating devices against PCI POI Security Requirements?

A *Fees for testing services are set independently by the laboratories and do not fall within the scope of the PCI standards. Vendors should contact the testing laboratories directly for pricing information.*

Additionally, vendors are assessed a fee for every new evaluation report received, as well as an annual listing or maintenance fee for each existing PCI approval.

Q Do the PCI POI Security Requirements cover POS, EPP, and ATM devices?

A *At present, PCI POI Security Requirements address the following approval classes: EPP, Non-PED, PED, SCR, and UPT.*

Q Do you have any statistics on breaches to POIs annually?

A *This information is tracked separately by each payment brand, so there is not any comprehensive compilation of this data.*

Q How do the PCI POI Security Requirements integrate with the PCI Data Security Standard (DSS)?

A *The PCI POI Security Requirements focus on protection of the cardholder's PIN and, optionally, on account data under the Secure Reading and Exchange of Data Module, when used in connection with a financial transaction. PCI DSS focuses on the protection of other sensitive data elements such as the Primary Account Number (PAN), the cardholder's name, and the CVC2/CVV2/CID/CAV2, and addresses both the transmission and storage of that data.*

Q How do the PCI POI Security Requirements integrate with EMV terminal type approval?

A *The EMV functionality testing and approval process is totally separate and independent from the POI physical and logical security evaluation process.*

Evaluating cryptographic device security requirements demands a certain level of security-related technical expertise that EMV laboratories may not possess. PCI SSC requirements mandate that the POI test laboratory be accredited for cryptographic device security testing to perform online and offline POI security evaluations against the PCI POI Security Requirements.

Q What is the difference between POI Security Requirements and PIN Security Requirements?

A *Both the PIN and POI Security Requirements have the common overall objective of protecting the cardholder's PIN during a financial transaction, and POI additionally has provisions for protecting account data.*

POI Security Requirements *(managed by PCI SSC) are primarily concerned with device characteristics impacting the security of the POI device used by the cardholder during a financial transaction. The requirements also include device management up to the point of initial key loading, but the evaluation process only addresses device characteristics.*

- ***Device characteristics*** *are those attributes of the POI that define its physical and its logical (functional) characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device—for example, the penetration of the device to determine its key(s) or to plant a PIN-disclosing "bug" within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a clear-text PIN-encryption key.*
- ***Device management*** *considers how the POI is produced, controlled, transported, stored, and used throughout its lifecycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.*

The ***PIN Security Requirements*** *consist of 32 security requirements divided into seven logically related groups, which are referred to as Control Objectives. The PIN requirements are about process management—primarily dealing with the secure management of cryptographic keys throughout their lifecycle (key creation, conveyance, loading, usage, and administration); with the use of secure PIN-processing methodologies; and the management and use of secure equipment for that processing. This results in a complete set of requirements for the secure management, processing, and transmission of Personal Identification Number (PIN) data during online and offline payment card transaction processing at attended and unattended point-of-sale (POS) terminals and for PIN processing at ATMs.*

Q What is the relationship of the PCI SSC PIN Security Requirements to PCI SSC POI Security Requirements?

A *PCI-approved devices must be able to support the implementation of the PCI SSC's PIN security requirements in a manner that is compliant with those requirements.*

Laboratory Testing

Q What criteria are the PCI POI security evaluation based upon?

A *The PCI POI security evaluation criteria will be listed in the* PCI POI Security Requirements *manuals, specifically in the physical and logical security sections. The laboratory will verify the vendor's YES and N/A responses in those sections by having the vendor provide additional evidence of conformance to the requirements, via information from the vendor and required POI samples.*

Q Will any of the payment brands perform their own POI security evaluations?

A *No.*

Q How do the PCI POI Security Requirements apply to the existing POI devices already installed?

A *It is the responsibility of PCI SSC to establish the PCI POI Security Requirements and evaluate POI devices against those requirements. However, any mandates regarding installed POIs have been established by and are the responsibility of the payment brands themselves, and questions regarding those mandates must be addressed to the brand(s) in question.*

Q What is the availability of the laboratories for starting a new PCI POI security evaluation?

A *A new evaluation can generally start within two (2) weeks of receiving all items for testing, but timeslots must be scheduled in advance with the laboratory. Please contact the laboratory directly for the specifics.*

Q How long does it take for a laboratory to perform the PCI POI security evaluation?

A *The evaluation generally takes one to two months of calendar time. It can go more quickly if the laboratory has all the required documentation and hardware, and there are minimal compliance issues to resolve. Please contact the laboratory directly for specific details.*

Q Does the laboratory provide assistance to help POI vendors comply with the PCI POI Security Requirements?

A *Yes, the laboratory can:*

a) Provide guidance on designing POIs to the security requirements.

b) Review a vendor's design, answer questions via e-mail or phone, participate in conference calls to clarify requirements, and perform a preliminary physical security assessment of a vendor's hardware.

c) Provide guidance on bringing a vendor's POI into compliance with the PCI POI Security Requirements if areas of non-compliance are identified during the evaluation.

Vendors are encouraged to contact the laboratory directly in regards to the above services and any fees associated with them.

The laboratory ***cannot:***

a) Design,

b) Develop original documentation for, or

c) Build, code, or implement any part of the product to be tested.

Approval Process

Q If a POI device passes the security evaluation and the report from the laboratory does not show any discrepancies, what else will be looked at before an approval is granted? If it is basically just the test report, couldn't the laboratory issue an approval automatically in order to save time?

A *The PCI POI test laboratory only performs the evaluation and provides an evaluation report; it has no approval authority. Only PCI SSC has approval authority and will base its approval on the evaluation report. If the results are all positive, there should not be any additional requirements for issuance of an approval letter. However, a delay may be possible if PCI SSC needs to contact the laboratory or vendor for additional information. A vendor would need to sign a release agreement with the laboratory for PCI SSC to receive the evaluation report.*

Q How will the PCI POI device approval be signified?

A *Two methods will be used:*

a) PCI SSC will issue a letter to the vendor indicating that the POI has been approved.

b) The approved device will be listed on the PCI SSC website.

PCI POI Testing and EMVCo Terminal Type Approval

Q Will PCI SSC choose different laboratories for POI evaluations than EMVCo chose for EMV terminal type approval testing?

A *Yes. PCI POI physical and logical security evaluations require a different level of expertise (cryptographic module security testing) than that required from laboratories performing EMV testing.*

Q What is the EMV test laboratories' involvement with PCI POI security testing?

A *None. EMV laboratories perform functionality testing, which is totally separate and independent from PCI POI security evaluations.*

Q Can the EMV test laboratories perform testing for POI security compliance as well, in order to prevent delays in the EMV approval process?

A *Yes, but only if that laboratory is a PCI SSC-approved POI security laboratory. Testing cryptographic requirements demands a certain level of technical expertise that EMV laboratories may not possess. PCI SSC requirements mandate that the POI test laboratory be accredited for cryptographic security testing in order to perform online and offline POI evaluations against PCI POI Security Requirements.*

Q How does the POI laboratory testing process relate to EMV approval?

A *The EMV approval process is totally separate from—and independent of—the PCI SSC POI security evaluation process.*

Q Can fixing the POI to pass the PCI POI evaluation affect the POI's EMV approval?

A *Yes. PCI SSC recommends that, if applicable, the POI receive EMV Level 1 approval first. Then the vendor should apply for PCI POI approval. EMV Level 2 testing, if applicable, should occur next.*

Q Does PCI issue compliance mandates in connection with the deployment of POI devices?

A *No, PCI manages the requirements and the device evaluation and approval process. The individual payment brands issue mandates regarding the deployment of POI devices.*

For specific information regarding mandates, contact the payment brand(s) of interest.

Q What is the impact of the device's "renewal" or "expiration" date for a device's approval?

A *The renewal/expiration date for a PCI-approved device is the date by which a vendor must submit the device for re-evaluation against the current security requirements in order for the device to maintain the approval.*

For specific information regarding the impact of approval expiration, contact the payment brand(s) of interest.

Q POI devices are approved for new deployments if they are on the approved list at the time of purchase. If a deployed device that was approved at the time of purchase requires replacement or repair, can that device be replaced with a newly purchased device of the same make/model and hardware/firmware versions when the device's approval has expired?

A *For specific information regarding the replacement of deployed devices whose approval has expired, contact the payment brand(s) of interest.*

Q For approved devices, under payment brand mandates, what is the latest date on which acquirers or their merchant agents can purchase and deploy a PCI-approved POI device?

A *For specific information regarding this date, contact the payment brand(s) of interest.*

Other

Q What is the impact on acquirers and/or merchants if they or their agents deploy POI devices that have not been approved by PCI SSC?

A *For specific information regarding deployment of devices that have not been approved, contact the payment brand(s) of interest.*

Q How can acquirers, merchants, and their agents ensure that the POI devices they purchase comply with the PCI POI Security Requirements?

A *Acquirers, merchants, and their agents should always look to the PCI SSC website and verify that the device matches* ***ALL*** *of the following as listed on the website:*

- *Model name*
- *Hardware version number*
- *Firmware version number*
- *Application version number, if applicable.*

Acquirers, merchants, and their agents should be aware when making purchasing decisions that some vendors may sell the same model in both approved and unapproved versions.

Q The PCI POI Testing and Approval Program Guide specifies that the PCI test laboratory is to provide to MasterCard on behalf of the Council two devices containing the same firmware, any supporting PC based test applications, and any keying material as those evaluated by the test laboratory. Under what conditions are these devices to be provided?

A *This applies to all new evaluations which result in a new approval number. It does not apply to deltas. It also does not apply to a situation where the vendor is merely rebranding another vendor's previously approved product. However, if a vendor is rebranding a product and additionally makes other changes, such as in the firmware, it does apply.*

In conjunction with the transmittal of the evaluation report to the Council, these two devices must be sent to the following location, where they will be placed into secure storage:

Attn: MasterCard Analysis Laboratory (MCAL)
MasterCard Worldwide
5 Booths Park
Chelford Road
Knutsford
Cheshire WA16 8QZ
UK