PIN Entry Device Security Requirements: *Frequently Asked Questions*

Contents

PCI and PED Security Requirements 1
Laboratory Testing 4
Approval Process 5
PCI PED Testing and EMVco Terminal Type Approval 6
Other 7

PCI and PED Security Requirements

Q Why is the PCI Security Standards Council (PCI SSC) assuming responsibility for the PIN Entry Device (PED) Security Requirements?

A *In the past, PED Security Requirements had been overseen by JCB, MasterCard, and VISA. Now, through PCI SSC, the five major global payment brands (American Express, Discover, JCB, MasterCard and Visa) will manage the PED Security Requirements, allowing even greater opportunity to standardize data and device security requirements, testing methodology, and approval processes for PIN Entry Devices (PED).*

It is a strategic priority for PCI SSC to continue streamlining security standards and the development of secure devices. Each step we take toward common requirements means more consistent security measures and cost effective market deployment. Common requirements benefit all stakeholders in the payments value chain and are intended to improve the overall security for customer-entered data by removing conflicting requirements.

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

A *PCI PED Security Requirements are primarily concerned with device characteristics impacting the security of the PIN Entry 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 PED 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 PED 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 When will the PCI Standards Security Council (SSC) start overseeing the PED Security Requirements program?

A *Migration of the PED Security Requirements and the corresponding evaluation program from JCB, MasterCard, and Visa to PCI SSC is in progress. The effective date of the PCI SSC PED Security Requirements will be July 2007.*

Q Will American Express and Discover accept devices that have been previously approved by Visa, MasterCard and JCB?

A *Yes, American Express and Discover have agreed to grandfather and accept all EPP and POS devices previously approved by Visa, MasterCard, and JCB.*

Q. How does PCI SSC's involvement impact merchants?

A *Having one approval method helps simplify the task of deploying PEDs for acquirers and merchants and avoids duplicate testing, thereby reducing costs.*

Q How does PCI SSC's involvement impact vendors?

A *PCI SSC's management will enable device vendors to develop payment technology more quickly, easily, and cost-effectively. Vendors can reduce the complexity of new product development by undergoing a single security evaluation process and providing faster time-to-market for financial institutions.*

In the past, vendors had to complete proprietary testing at multiple laboratories to meet the security requirements of all the global and local payment schemes. This was time-consuming, expensive and often created confusion. PCI SSC is committed to continuing the efforts toward creation of global security standards that will help reduce the cost and complexity of card payment transactions.

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

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

Q Will PIN Entry Devices that have previously been approved to the old PCI PED requirements maintain their approval status?

A *Yes. They will be on the approval list until the existing, pre-defined expiration dates.*

Q What are the costs to vendors for evaluating devices against PCI PED 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, there will be PCI SSC vendor fees, and these will be announced to Participating Organizations and PED vendors when the PCI PED program is introduced.

Q Will PCI SSC continue to recognize laboratories previously accepted by JCB, MasterCard, and Visa for PED security evaluations?

A *PCI SSC agreements are currently being put in place with the existing PED security labs. A complete list of PED security labs will be available prior to program launch.*

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

A *At present, PCI PED Security Requirements have been released for attended POS PEDs and EPPs in unattended devices. Overall requirements for ATM devices and other unattended PIN acceptance devices are currently under review.*

Q Do you have any statistics on breaches to PEDs 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 PED Security Requirements integrate with the PCI Data Security Standard (DSS)?

A *The PCI PED Security Requirements focus on protection of the cardholder's PIN 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 PED Security Requirements integrate with EMV terminal type approval?

A *The EMV functionality testing and approval process is totally separate and independent from the PED 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 PED test laboratory be accredited for cryptographic device security testing to perform online and offline PED security evaluations against PCI PED Security Requirements.

Q Will PCI SSC assume responsibility for PIN Security Requirements as well as PED Security Requirements?

A *PCI SSC has assumed responsibility only for PED Security Requirements at this time. PIN Security Requirements are still under the management of MasterCard and Visa, although PCI SSC is reviewing these requirements for possible adoption in the future.*

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

A *Both the PIN and PED Security Requirements have the common overall objective of protecting the cardholder's PIN during a financial transaction.*

PED Security Requirements (managed by PCI SSC) are primarily concerned with device characteristics impacting the security of the PIN Entry 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 PED 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 PED 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 (managed by MasterCard and Visa) 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 PIN security requirements (as defined by Visa and MasterCard) to PCI SSC PED Security Requirements?

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

Laboratory Testing

Q What criteria is the PCI PED security evaluation based upon?

A *The PCI PED security evaluation criteria will be listed in the PCI PED 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 PED samples.*

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

A *No.*

Q How do the PCI PED Security Requirements apply to the existing PEDs already installed?

A *It is the responsibility of PCI SSC to establish the PCI PED Security Requirements and evaluate PED and EPP devices against those requirements. However, any mandates regarding installed PEDs 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 impact of having a PED evaluated against online and offline requirements at different times?

A *Under the PCI PED Security Requirements, for any specific model or model family evaluated separately for online and offline PIN entry against the same set of security requirements (major version—e.g., Version 1.x), they will be part of the same approval, with the approval expiration date set as six years from the expiration of the relevant requirements. For example, version 1.x of both the POS and EPP security requirements expire April 2008. All devices evaluated and approved against Version 1.x shall have their approvals expire April 2014. This applies whether or not different hardware and/or firmware versions are used.*

Q What is the availability of the laboratories for starting a new PCI PED 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 PED 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 PED vendors comply with the PCI PED Security Requirements?

A *Yes, the laboratory can:*

a) Provide guidance on designing PEDs 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 PED into compliance with the PCI PED 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 PED 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 PED 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 PED approval be signified?

A *Two methods will be used:*

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

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

Q What will happen to all of the approved devices that are currently listed on JCB, MC and Visa websites?

A *All PCI-approved devices that are currently listed on the payment brand websites will be moved to the PCI SSC website. The "pre-PCI" approved devices will not be moved to the PCI SSC website since most of them will expire by the end of 2007. However, American Express, Discover, JCB, MasterCard, and Visa will still recognize these devices until their expiration dates.*

PCI PED Testing and EMVco Terminal Type Approval

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

A *Yes. PCI PED 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 PED security testing?

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

Q Can the EMV test laboratories perform testing for PED 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 PED security laboratory. Testing cryptographic requirements demands a certain level of technical expertise that EMV laboratories may not possess. PCI SSC requirements mandate that the PED test laboratory be accredited for cryptographic security testing in order to perform online and offline PED evaluations against PCI PED Security Requirements.*

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

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

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

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

Other

Q What is the impact on acquirers and/or merchants if they or their agent deploys POS PEDs or Encryption PIN Pads (EPPs) that have not been approved by PCI SSC?

A *Acquirers and/or merchants deploying POS PEDs or EPPs that have not received PCI PED approval will continue to be liable in the event of a PIN compromise that is attributable to the deployment of those devices, according to the rules and regulations of individual payment brands.*

Q For liability protection, how can acquirers, merchants, and their agents ensure that the POS PEDs and EPPs they purchase comply with the PCI PED 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 PED Testing and Approval Program Guide specifies that the vendor 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: Jeremy King
MasterCard Worldwide
St Andrews House
Kelvin Close
Birchwood
Warrington
Cheshire
UK
WA3 7PB

Q EPPs and POS PEDs 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 *One to one replacement of in-kind devices for repair and replacement are permitted, if the replacement is performed by the device's original purchaser or their agent, even though the approval has lapsed. This does not apply to devices that have had their approval revoked for reasons other than normal approval expiration. For example, in the event of a widespread compromise of the device.*