

New updates: Added Q&A's: Q42.

## Payment Card Industry (PCI) PIN and PED Alignment Efforts

### 1. What does the Payment Card Industry PIN and PED security alignment represent?

PCI alignment for PIN and PED security represents a partnership to standardize data and device security requirements, testing methodology, and approval processes. The current PCI partners for PIN security are Visa and MasterCard. The current PCI partners for PED security are Visa, MasterCard, and JCB.

### 2. How does the alignment impact vendors?

The alignment 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 testing process.

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. Visa is committed to continuing the efforts to create global standards that will help reduce the cost and complexity of card payment transactions.

### 3. Will other companies join this PED alignment initiative?

Yes, other companies may choose to participate in PCI alignment efforts.

### 4. Will JCB and MasterCard accept POS PEDs that have been previously approved by Visa?

Yes, JCB and MasterCard have agreed to grandfather and accept all POS PEDs previously approved by Visa.

### 5. What are the costs to vendors for testing devices against PCI requirements?

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.

### 6. Are there PCI security requirements for POS, EPP, and ATM devices?

At present, PCI requirements have been released for POS and EPP devices. Requirements for ATM devices and other unattended PIN acceptance devices are currently under development. Visa will announce any associated compliance dates for unattended devices after the relevant PCI requirements are released.

## Laboratory Testing

### 7. Which laboratories are recognized by Visa for PED security testing?

Brightsight  
The Netherlands  
+31 15 269 2522  
[www.brightsight.com](http://www.brightsight.com)

DOMUS IT Security Laboratory  
Canada  
+1 613 726-5090  
[www.domusitsl.com](http://www.domusitsl.com)

EWA-Canada Limited  
Canada  
+1.613.230.6067  
[pcilab@ewa-canada.com](mailto:pcilab@ewa-canada.com)

InfoGard Laboratories, Inc.  
United States  
+1 805 783 0810  
[www.infogard.com](http://www.infogard.com)

RFI Global Services Ltd.  
United Kingdom  
+44 (0) 1256 312000  
[www.rfi-smart.com](http://www.rfi-smart.com)

SRC Security Research & Consulting GmbH  
Germany  
+49 228 2806 101  
[www.src-gmbh.de](http://www.src-gmbh.de)

T-Systems ITC Security  
Germany+49 (0)228 9841  
[www.t-systems-itc-security.com](http://www.t-systems-itc-security.com)

Witham Laboratories  
Australia  
+61 3 9846 2751  
[www.withamlabs.com](http://www.withamlabs.com)

## 8. What criteria is the PED evaluation based upon?

The PED evaluation criteria is listed in the 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.

Though required by Visa, the laboratory does not evaluate the PED against the device management requirements specified in the manual.

## 9. Does Visa perform any PED security testing?

No

## 10. How do the PED security requirements apply to the existing POS PEDs already installed?

To retain liability protection, Members (or their Agents) have until 01 July 2010 to ensure that all of their installed attended POS PED models have been approved by Visa. PEDs must be on the current approved list or the expired approval list. There are no requirements to replace existing ATMs or other unattended PIN acceptance devices.

## 11. What is the impact of having a PED evaluated against online and offline requirements at different times than at once?

Under PCI, 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 original approval expiration date applicable. This applies whether or not different hardware and/or firmware versions are used. For a specific model or model family evaluated separately for online and offline PIN entry against different versions of the security requirements (i.e., version 1.x vs. 2.x), the latter evaluation will be treated as a new approval.

## 12. What is the availability of the laboratories for starting a new PED evaluation?

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.

**13. How long does it take for a laboratory to perform the PED evaluation?**

The evaluation generally takes one to two months of calendar time. It can go quicker 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.

**14. Does the laboratory provide assistance to help PED vendors comply with the Visa requirements?**

Yes, the laboratory can:

- a. Provide guidance on designing PEDs to the security requirements
- b. Review a vendor's design, answer questions via email or phone, participate in conference calls to clarify requirements, and perform a preliminary physical security assessment on a vendor's hardware
- c. Provide guidance on bringing a vendor's PED into compliance with Visa's 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 can not a) design, b) develop original documentation for, or c) build, code, or implement any part of the product to be tested.

**15. Will Visa be recognizing additional laboratories for PED testing?**

Yes, PCI participants will consider a laboratory's interest to be recognized for PED security testing. However, a Visa Region or other PCI payment brand participant must first sponsor the laboratory, taking into consideration a justifiable business case and a similar interest by MasterCard and JCB. PCI participants have developed a set of qualifying and technical requirements for any testing laboratory to meet. The accreditations and certifications requirements include:

- a. The test laboratory shall provide evidence of all accreditations claimed. These may include accreditation under the relevant national implementation of ISO/IEC 17025 (Criteria for the competence of testing and calibration laboratories), ISO 9000 (Quality management systems), ISO 15408 (Common Criteria for IT security evaluations) or other similar international, national, or industry standards.
- b. The test laboratory shall also provide evidence of sponsorship or endorsement by a recognized payment scheme engaged in the processing of PIN transactions (either a global payment scheme or a multi-Member national debit scheme/network). The sponsorship or endorsement must include the testing of cryptographic devices to a prescribed set of security requirements.
- c. Additional criteria apply

**Approval Process****16. If a PED passes all tests 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 – to save time?**

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

**17. How will the PED approval be signified?**

Two methods will be used:

- a. Visa will issue a letter to the vendor indicating that the PED has been approved
- b. The approved device will be listed at [www.visa.com/pin](http://www.visa.com/pin).

**18. How can PED approval be maintained when hardware or firmware changes are made?**

There are two likely scenarios:

- a. New Testing is Not Required to Maintain Approval

If the hardware or firmware (including software which impacts security) in the previously approved PED is revised, but is believed to not impact security, then a documentation of the change can be submitted to the laboratory for a review. After which, the laboratory would issue a letter to PCI participants describing the nature of the change and stating that it does not impact the PED security requirements. PCI participants will then review the letter to see whether the change has any impact to the approval status of the PED. Assuming no impact, then the new version number would be considered approved and a new approval letter will be issued to the vendor and the approved PED listing on the Visa site would be updated accordingly with the new version number.

- b. New Testing is Required to Maintain Approval

If changes to the device do impact PED security requirements, then a new evaluation report from the laboratory would need to be submitted to PCI participants for re-approval consideration.

**19. What is the "boundary of approval" for which an approval of an existing PED model can be carried over to a new (or similar) PED model?**

At this time, PCI participants have defined the PED testing boundary as followed:

- a. Vendor describes the design of the new (or similar) PED model in the form of a product revision document
- b. Vendor sends the above documentation to the laboratory for review
- c. Laboratory reviews the documentation (and possibly PED samples)
- d. Laboratory treats the document review process like a product revision of an existing approved PED
- e. Laboratory then sends a letter to the vendor informing it whether a full test evaluation will be required or not

**20. How long will it take Visa to issue an approval letter?**

Once Visa verifies the PED evaluation report from the laboratory, Visa will issue its PED approval letter and list the device on [www.visa.com/pin](http://www.visa.com/pin) within thirty calendar days of receiving the report – time that may be needed to resolve any issues with either the vendor or the laboratory, and personnel availability. However, if there are no discrepancies in the evaluation report, then Visa may issue the approval letter and post the PED approval as quickly as five to ten business days upon receipt of the report. In all cases, approvals are coordinated with the other PCI payment brand participants.

**21. Since Visa PED approvals expire, what is the process to gain an extension?**

Approximately six months before the PED's approval is due to expire, the PIN administrator will notify the vendor to determine whether the vendor intends to renew the PED's approval. The options available for the vendor to consider are:

- a. Letting the PED approval expire and having the PED removed from the list of approved devices.
- b. Contacting a PCI-recognized laboratory and submitting paperwork noting any modifications to the PED since the laboratory last reviewed it. The laboratory will then notify the vendor as to whether the PED needs to undergo a full reevaluation. Upon

receipt from the laboratory of either a successful test report or a letter stating that any changes made to the PED do not impact security, PCI participants will then extend the PED's approval as appropriate.

### **PED Testing and EMVco**

#### **22. Why did Visa choose different laboratories for PED testing and EMV testing?**

PED physical and logical security testing requires a different level of expertise (cryptographic module security testing) than that required from laboratories performing EMV testing.

#### **23. What is the EMV test laboratories' involvement with PED security testing?**

None, EMV performs functionality testing, and is totally separate and independent from PED security testing.

#### **24. Can the EMV test laboratories perform testing for PED security compliance as well, to not delay the EMV approval process?**

Yes, but only if that laboratory is PCI-recognized for PED security testing. Testing cryptographic requirements demands a certain level of security technical expertise that EMV laboratories may not possess. PCI requirements mandate that the PED test laboratory be accredited for cryptographic security testing to perform online and offline PED evaluations against PCI security requirements.

#### **25. Will the PED approval process need to be repeated if a PED fails to gain EMV approval and requires a change in software or hardware?**

If the modified hardware or software changes the PED's physical and logical security for PIN protection, then the PED will likely need to be reevaluated by the laboratory. Visa recommends contacting one of the PCI-PED test laboratories first, to determine whether an evaluation is needed.

#### **26. How does the PED laboratory testing process relate to EMV approval?**

The EMV approval process is totally separate and independent from PED physical and logical security testing process.

#### **27. Is it possible to pass EMV test for Offline PIN functional processing and fail the PED security compliance test?**

Yes, EMV Offline PIN testing addresses functional processing and does not test PED security requirements.

#### **28. Can fixing the PED to pass PED laboratory testing affect the PED's EMV approval?**

Yes, PCI participants recommends that, if applicable, the PED receives EMV's Level 1 approval first. Then the vendor should apply for PCI PED approval. EMV Level 2 testing, if applicable, should occur next.

### **Triple Data Encryption Standard (TDES)**

#### **29. What are Visa's requirements for implementing Triple DES?**

Visa strongly recommends Members develop implementation plans for the migration to TDES. [Effective 1 January 2004, all newly deployed POS PEDs (including replacement devices) must support TDES. Effective 1 January 2003, all newly deployed ATMs (including replacement devices) must support TDES.]

Visa recommends that PINs be encrypted using the TDEA Electronic Codebook Mode of Operation (TECB) mode as described in ISO/IEC 10116 – Information technology – Security techniques – Modes of operation for an n-bit block cipher.

For purposes of these requirements, all references to TECB are using keying option 1 or 2, as defined in ANSI X9.52. For entities directly connected to Visa, only keying option 2 is supported

#### **30. What are the other relevant reference standards for implementing Triple DES?**

ANSI X9.24 – Financial Services: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

ANSI X9.52: Triple Data Encryption Algorithm (TDEA) Modes of Operation, contains the complete specification for Triple DES and its seven modes of operation

ANSI X9.65: Triple Data Encryption Algorithm (TDEA), Implementation Standard, contains information on the various Triple DES modes, including characteristics, implementation issues, and an outline of key management methods for Triple DES keys

ISO 11568-2: Banking -- Key management (retail) -- Part 2: Symmetric ciphers, their key management and life cycle, describes the use of double length DEA keys.

X9 documents can be order via [www.x9.org](http://www.x9.org)

ISO documents can be ordered via [www.iso.ch](http://www.iso.ch)

**31. Can DUKPT be used instead of Fixed Key or Master Key/Session Key?**

Yes, a PIN Entry Device may use the DUKPT protocol. ANSI X9.24 has been updated to include requirements for Triple DES (TDES), including the use of TDES for DUKPT. An example is provided in ANSI X9.24, and it is discussed in ISO 9564 Part 1, Annex C.4.

PIN translation must only occur using one of the allowed key management schemes: DUKPT, Fixed Key, or Master Key/Session Key..

**32. Does Visa offer a standardized test tool for evaluating the robustness of a vendor's implementation of TDES DUKPT?**

Not at present.

**Other**

**33. What are Visa's PIN security requirements for PDAs, mobile phones, and set-top boxes?**

Security requirements for protecting PIN data must remain constant across all payment devices and environments. The requirements for the protection of the PIN should not vary based upon the media used to enter the PIN. Visa will support a consistent "standard of care" for protecting the PIN across the Visa and Acquirer domains using technical solutions and administrative controls to validate any Visa and PCI requirements.

**34. What is the difference between Offline PIN and Online PIN?**

Online PIN means that the cardholder's Issuer (or its designated card processor) verifies the cardholder's PIN. A PIN that is transported to the Issuer for Online verification must be encrypted using TDES. Whereas, with Offline PIN, the cardholder's chip card verifies the cardholder's PIN locally at the card acceptance device, using the onboard cryptography of the card and the PED.

**35. What is PIN compromise?**

PIN compromise is the breaching of secrecy and/or security of a cardholder's personal-identification-number (PIN). An increasingly common problem is "shoulder surfing," where someone would look over a cardholder's shoulder to watch the PIN being entered, then steal the card using distraction techniques or pick pocketing. Fraud that involves card-trapping devices is also on the rise. A device, inserted by a criminal into the device's card slot, could retain the card inside the device, at which point the criminal tricks the victim into re-entering the PIN. After the cardholder gives up trying to get the card out and leaves, the criminal removes the device, with the card, and in the case of an ATM, is potentially able to withdraw cash. The introduction of chip cards combined with PIN will permit cardholders to use a PIN at the point-of-sale instead of a signature, which will make it difficult for criminals to use lost and stolen cards in a face-to-face transaction. Criminals are using more advanced techniques to intercept the PIN or compromise the integrity of secret data. The PED Testing and Approval Program ensures that the device meets a prescribed level of security and will only be approved if it has been properly evaluated by a PCI-recognized laboratory.

**36. What is the impact to an Acquirer if they or their agent deploys POS PEDs or EPPs that have not been evaluated by a Visa recognized laboratory and are not on the current Visa approved list?**

Acquirers deploying POS PEDs or EPPs that have not passed evaluation by a Visa-recognized laboratory and which are not approved by Visa will continue to be liable in the event of a PIN compromise that is attributable to the deployments of those devices, and additionally may be liable for penalties in accordance with the Visa International Operating Regulations, Volume I—General Rules, Section 1.5.

**37. For liability protection, how can Acquirers and their agents ensure that the POS PEDs and EPPs they purchase are compliant to the applicable PIN Entry Device security requirements?**

Acquirers and their agents should always look to the website at [www.visa.com/pin](http://www.visa.com/pin) and validate the device matches ALL of the following as listed on the website: Model Name, Hardware #, Firmware #, and, if applicable, Application #. Acquirers and their agents should be aware when making purchasing decisions that some vendors may sell the same model in both approved and unapproved versions.

**38. What is the impact to the Acquirer of the “renewal” or “expiration” date for a device’s approval? For example, the Pre-PCI approved POS devices all expire 31 December 2007.**

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

The renewal/expiration date for Pre-PCI approved POS devices is fixed at 31 December 2007 and cannot be extended. Pre-PCI approved devices may be submitted for approval against the current PCI requirements to receive a new renewal/expiration date.

Acquirers purchasing devices that are on the approved list retain protection against liability from PIN compromise associated with the deployment of those devices.

Acquirers deploying devices that are not on the current approved list at the time of purchase will continue to be liable in the event of PIN compromise attributable to use of those devices and additionally may be liable for penalties in accordance with the Visa International Operating Regulations, Volume I—General Rules, Section 1.5.A through Section 1.5.D.1.

Security requirements are reassessed every three years based on identified threats. If necessary the requirements are updated. Devices evaluated against earlier versions of security requirements will have their approvals expire on a specific date. This expiration date is also known as the “renewal date”. In order to continue to maintain approval for a new approval cycle, the device must be evaluated against the current version of security requirements.

In the example cited, for devices expiring 31 December 2007, Acquirers retain protection against liability from PIN compromise associated with the deployment of those devices purchased through 31 December 2007. For devices purchased after that date, where the security of that device was not re-assessed and thus was not given a new expiration/renewal date, there will not be any liability protection.

It is important to note that there is currently not a sunset date for devices that were on the approved list at the time of deployment. Deployed devices who have their approval expire 31 December 2007 may continue to be used after that date. The impact of the expiration is strictly associated with new purchases/deployments, and not existing deployments.

**39. Pre-PCI approved POS devices have their approvals for new deployments expire 31 December 2007. Is there a sunset date where these devices must be removed from deployment?**

A sunset date for deployed devices that were approved at the time of deployment, but have had their approvals expire, does not currently exist. Due to the changing threat environment, PCI participants are evaluating the need to establish a sunset date for Pre-PCI devices. However, that date, if established, will take into account the expected normal life cycle of devices subsequent to deployment, balanced against the emergence of threats

## 40. What is the relationship of the PCI PIN Security Requirements to PED testing?

PCI approved PIN Entry Devices must be able to support the implementation of the PIN security requirements in a manner that is compliant to those requirements.

## 41. How do the PCI PIN Security Requirements relate to the PCI PED Security Requirements?

Both the PIN and PIN Entry Device (PED) Security Requirements have the common overall objective of protecting the cardholder's PIN during a financial transaction using a payment card.

The PIN Security Requirements consist of thirty-two 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 life cycle (key creation, conveyance, loading, usage, and administration) and 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 ATMs, and attended and unattended point-of-sale (POS) terminals.

The PED Security Requirements (both POS and EPP) are primarily concerned with device characteristics impacting the security of the PIN Entry Device used by the cardholder during a financial transaction. It also includes device management, but the testing process currently only addresses the device characteristics.

These requirements are divided into the following categories:

Device Characteristics:

- Physical Security Characteristics
- Logical Security Characteristics

Device Management:

- Device Management During Manufacturing
- Device Management Between Manufacturing and Initial Key Loading

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 cleartext PIN encryption key.

Device management considers how the PED is produced, controlled, transported, stored and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

The PED Security Requirements are only concerned with the device management for PEDs up to the point of initial key loading. Subsequent to receipt of the device at the initial key loading facility, the responsibility for the device falls to the acquiring Member and is covered by the operating rules of the Associations and the *PCI PIN Security Requirements*.

## 42. 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?

One to one replacements 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.