General PED Frequently Asked Questions *Updated May 2010*

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, JCB, Discover and American Express. For further information, see www.pcisecuritystandards.org.

2. What are Visa's requirements for PIN Entry Device Testing and deployment?

PIN Entry Device Testing Requirements:

- Effective 1 January 2004, all newly deployed attended POS PIN acceptance device models (including replacement devices) must have passed testing by a PCI-recognized laboratory and be approved by Visa for new deployments.
- Effective 1 October 2005, all newly deployed EPPs, including replacements or those in newly deployed ATMs, must have passed testing by a PCI-recognized laboratory and be approved by Visa for new deployments.
- Effective 1 October 2007, all newly deployed unattended POS PIN acceptance devices must contain an EPP that has passed testing by a PCI recognized laboratory and is approved by Visa for new deployments, and if used for offline PIN acceptance, a laboratory validated and Visa approved secure smart card reader.
- Effective 1 July 2010, all attended POS PIN acceptance device models must have passed testing by a PCI-recognized laboratory and have been approved by Visa.
- Effective 31 December 2014, all pre-Payment Card Industry Point of Sale (PCI POS) PIN acceptance devices (devices designed and tested earlier than PCI POS PIN Entry Device (PED) Version 1.x specifications) used in an attended environment are to be replaced by devices that are PCI-approved for deployment at the time of deployment.

3. What are Visa's requirements for implementing Triple DES?

PIN Entry Device TDES Capability Requirements:

- Effective 01 January 2003, all newly deployed ATMs (including replacement devices) must support TDES.
- Effective 01 January 2004, all newly deployed POS PIN acceptance devices (including replacement devices) must support TDES.

Effective 1 July 2010, Cardholder PINs must be TDES encrypted from all Points-of-Transaction to the Issuer. However, each Visa Region's TDES dates will supersede the global TDES date whenever the Visa Region date precedes the global date.

Note: "Must support" means the device has all the necessary hardware and software required for TDES installed and only requires the loading of a TDES key.

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 NIST SP800-67. For entities directly connected to Visa, only keying option 2 is supported.

For specific regional TDES implementation dates contact your Visa regional risk management contacts.

General PED Frequently Asked Questions *Updated May 2010*

4. What are the other relevant reference standards for implementing TDES?

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

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.

ISO/IEC 18033-3: Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers.

ISO TR19038: Guidelines on Triple DES Modes of Operation.

NIST SP800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

X9 documents can be ordered via www.x9.org. ISO documents can be ordered via www.iso.ch. NIST documents are available at csrc.nist.gov/publications/nistpubs/

5. How do the PED security requirements apply to the existing attended POS PEDs already installed?

To retain liability protection, Members (or their Agents) have until 1 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 at www.pcisecuritystandards.org/pin or the expired approval list at www.visa.com/pin.

NOTE: Visa Europe (VE) has announced new PED usage requirements. Within VE, no further pre-PCI PEDs (i.e. those devices designed and tested earlier than PCI PED version 1.x specifications) are to be newly deployed in an attended (face-to-face) environment after **31 December 2009.** Additionally, all pre-PCI PEDs (devices designed and tested earlier than PCI PED version 1.x specifications) used in an attended (face-to-face) environment must be replaced with PCI approved devices (at the time of deployment) by **31 December 2012.** Clients should refer to their VE regional risk office for more information**.**

For Visa Inc, all pre-PCI PEDs used in an attended (face-to-face) environment must be replaced with PCI approved devices (at the time of deployment) by **31 December 2014.** Clients should refer to their Visa regional risk office for more information**.**

6. How do the PED security requirements apply to the existing unattended POS PEDs already installed?

Effective October 1, 2007, all newly deployed *unattended* POS PIN acceptance devices must contain an EPP that has passed testing by a PCI-recognized laboratory and is approved by Visa for new deployments. Additionally, if the device is used for offline PIN acceptance, it must contain a lab-evaluated and Visa-approved secure smart card reader. The intent of this requirement is not retroactive and currently there are not currently any Visa requirements to replace EPPs within existing ATMs or other unattended PIN acceptance devices such as Kiosks and Automated Fuel Dispensers (AFDs).

General PED Frequently Asked Questions *Updated May 2010*

7. How do the PED security requirements apply to the existing U.S. AFDs already installed?

One of the largest populations of unattended POS PEDs are U.S. deployed AFDs. When PED testing requirements were first implemented, AFD vendors were not able to meet Visa's PED evaluation requirements for older AFDs deployed in the U.S. region. The AFD vendors built some PEDs that were successfully evaluated; however, these AFDs were primarily for new markets outside of the U.S. Recognizing that U.S. petroleum merchants had no lab-evaluated PEDs to purchase; Visa granted an extension to the original January 1, 2004 requirement that all newly deployed POS PEDs support TDES and be lab-evaluated and Visa-approved. These two requirements were deferred until **1 January 2009**, only for U.S. PEDs used in conjunction with AFDs. Please note that this extension did not alter any other existing Visa PIN or PED security requirements and acquirers of petroleum merchants remain fully liable and responsible for ensuring that merchants meet all other existing PCI PIN Security Requirements. **Effective 1 January 2009**, all newly deployed U.S. AFDs must contain an EPP that has passed testing by a PCI-recognized laboratory and is approved by Visa for new deployments. The intent of this requirement is not retroactive and currently there are no Visa requirements to replace EPPs within existing (currently deployed) AFDs.

8. What constitutes a newly deployed unattended POS PED?

Unattended POS PEDs (e.g., Kiosks and AFDs) that have been installed for the first time are considered newly deployed. If an unattended POS device is used for non PIN acceptance only and it is upgraded to accept PINs it is also considered a newly deployed device. If a device is physically moved from one location to another it is considered newly deployed.

9. 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 PCI 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.

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

Acquirers deploying EPPs or POS PEDs that have not passed evaluation by a Visa (PCI) recognized laboratory and which are not approved by Visa (PCI) at the time of purchase 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 1.6.D.9 and Table 1-8.

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

Acquirers and their agents should always look to the website at www.pcisecuritystandards.org/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.

12. What is the impact to the Acquirer of the "renewal" or "expiration" date for a device's approval? For example, the Pre-PCI approved attended POS devices all expire 31 December 2007.

The renewal/expiration date for Pre-PCI or 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 attended 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.

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.

13. 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. Unless additional mitigating steps (including but not limited to those listed below) are taken, 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.

Entities deploying devices should always implement measures to help prevent skimming attacks. Information on measures that can be taken is included in the PCI SSC's skimming prevention best practices guide, which can be found at: https://www.pcisecuritystandards.org/pdfs/skimming_prevention_form.pdf.

Devices that have been compromised, as noted on www.visa.com/cisp, should be replaced with newer, more secure versions of the product, or with different models, whenever an opportunity presents itself.

Entities deploying devices that have been compromised should implement mitigating steps, including, but not limited to:

- Developing and implementing a policy and procedures to train staff to regularly inspect terminals visually to identify anything abnormal, such as missing or altered seals or screws, extraneous wiring, holes in the device or the addition of labels or other covering material that could be used to mask damage from device tampering.
- Physically securing terminals and PIN pads to counters to prevent PED removal with secure locking cable connections.
- Physically securing under lock and key the storage of terminals awaiting deployment and periodically validate the inventory on hand to asset records. Using terminal asset tracking systems/procedures for devices deployed, devices awaiting deployment, devices under repair and devices in transit to location.

- Developing and implementing a policy and procedures to train staff to validate the identity of all payment system repair technicians. Unauthorized or unexpected service personnel should be denied access unless fully validated and authorized. Authorized and validated repair technicians should still be escorted and monitored at all times.
- Periodically weigh PED equipment and compare with vendor specification weight to identify the insertion of tapping mechanisms within devices. This should be done randomly on a continuous basis.
- Deploying a terminal authentication system to enable remote monitoring of the PED's electronic serial number and/or to detect PED connectivity changes.

14. Pre-PCI (Visa) attended POS PEDs expire 31 December 2007. What is the latest date that an acquirer or their merchant agents can purchase a Pre-PCI POS PED and still retain liability protection for the use of those devices?

The expectation is that acquirers or their merchant agents must purchase and take delivery of Pre-PCI attended POS PEDs prior to 2008. These devices can then be deployed as needed.

Under certain conditions, delivery may be taken subsequent to 2007. This is allowed when all of the following conditions are met:

- Full payment or invoicing has occurred prior to 2008.
- The devices purchased are manufactured inventory on hand prior to 2008.
- The devices are specifically identified (e.g., via serial number) and designated for that specific customer.

These conditions must be met when the acquirer or their merchant agent makes the purchase, whether it is from the OEM or a third party reseller.

15. What are the legal conditions and restrictions regarding Pre-PCI PED approvals?

Visa's approval only applies to PEDs that are identical to the PED tested by a Visa (PCI) recognized laboratory. If any aspect of the PED is different from that which was tested by the laboratory – even if the PED conforms to the basic product description contained in the letter, then the PED model should not be considered approved, nor promoted as approved. For example, if a PED contains firmware, software, or physical construction which has the same name or model number as those tested by the lab, but in fact is not identical to those PED samples tested by the laboratory, then the PED should not be considered or promoted as approved.

No vendor or other third party may refer to a PED as "Visa or PCI Approved," nor otherwise state or imply that Visa has, in whole or part, approved any aspect of a vendor or its PEDs, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with Visa, or in an approval letter. All other references to Visa's approval are strictly and actively prohibited by Visa.

When granted, an approval is provided by Visa to ensure certain security and operational characteristics important to Visa's systems as a whole, but the approval does not under any circumstances, include any endorsement or warranty regarding the functionality, quality, or performance of any particular product or service. Visa does not warrant any products or services provided by third parties. Approval does not, under any circumstances, include or imply any product warranties from Visa, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by Visa. All rights and remedies regarding products and services, which have received an approval, shall be provided by the party providing such products or services, and not by Visa. Unless otherwise agreed in writing by Visa, all property and services contemplated in this document which Visa provides to any third parties are provided on an "as-is" basis, "with all faults" with no warranties whatsoever. Visa specifically disclaims any implied warranties of merchantability, fitness for purpose or non-infringement.

16. How will the new PCI Unattended Payment Terminal (UPT) requirements affect Visa's current EPP mandates for unattended POS PEDs?

In 2009 the PCI Security Standards Council published new PED testing requirements for Unattended Payment Terminals (UPTs) and Hardware Security Modules (HSM). For HSM clarification see question 10. Visa does not currently plan to set a compliance mandate for the new UPT requirements. The only requirement Visa has for unattended POS PEDs is specified in Questions 2 - 3 and 6 - 8. Use of a PCI approved EPP, and if the device is used for offline PIN acceptance, it must contain a lab-evaluated and Visa-approved secure smart card reader. These are the only requirements for newly deployed unattended POS PEDs. When Visa does set UPT requirements for newly deployed unattended POS PEDs, it will be for newly deployed devices and will not be retroactive. Although no future date has been set for PCI UPT adoption, clients are encouraged to move to these devices as they offer more overall device security than the current requirements which focus only on the EPP. Visa clients can achieve compliance by following the EPP usage mandates Visa currently has in effect.

17. What is the latest date that an acquirer or their sponsored merchant / agents can purchase a delisted PCI PED and not be subject to fines for violation of the PIN Security program for deploying the device?

The expectation is that acquirers or their merchant agents must purchase and take delivery of delisted PCI PEDs prior to the delisting date. These devices can then be deployed as needed.

Under certain conditions, delivery may be taken subsequent to the delisting date. This is allowed when all of the following conditions are met:

- Full payment or invoicing has occurred prior to the delisting date.
- The devices purchased are manufactured inventory on hand prior to the delisting date.
- The devices are specifically identified (e.g., via serial number) and designated for that specific customer.

These conditions must be met when the acquirer or their merchant agent makes the purchase, whether it is from the OEM or a third party reseller.

18. How will the new PCI Hardware Security Module (HSM) requirements affect Visa's PIN Security and Key Management Compliance Program?

In 2009, the PCI Security Standards Council published new PCI Hardware Security Module (HSM) requirements. Visa does not currently plan to set a compliance mandate for these new requirements. Per the current PCI PIN Security Requirements all cardholder entered PINs must be processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). A Tamper-Resistant Security Module (TRSM) must meet the requirements of a Physically Secure Device as defined in the following ANSI and ISO standards:

Banking—Retail Financial Services Symmetric Key Management	ANSI X9.24
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ANSI TR-31
Personal Identification Number (PIN) Management and Security	ISO 9564
Banking—Key Management (Retail)	ISO 11568
Banking—Secure Cryptographic Devices (Retail)	ISO 13491

Per Visa's *PIN Security Program: Auditor's Guide's* all entities must validate that their current HSMs are compliant by obtaining and examining one or more of the following:

a. NIST certification that the equipment used for PIN translation (hardware or host security modules) complies with a minimum of level 3 of FIPS 140-2-*Security Requirements for Cryptographic Modules*. This may be obtained from the NIST website (csrc.nist.gov). Hardware Security Modules must be compliant with FIPS 140-2 Level 3 or Level 4 (formal certification is not required; however, such certification is evidence of a device's compliance to this requirement).

b. Vendor Certification letters or technical documentation to indicate that the equipment has been designed to meet (ANSI X9.24 and ANSI X9.8/ISO 9564 are the minimum criteria):

– FIPS 140–2—*Security requirements for Cryptographic Modules-Level 3 or 4*.

– ANSI X9.24—*Financial Services Retail Key Management*.

– ANSI X9.8—*Personal Identification Number Management and Security (all parts).*

– ISO 9564—*Banking-Personal Identification Number Management and Security (all parts)*.

– ISO 13491–1—*Banking-Secure Cryptographic Devices (Retail), Part 1 Concepts, Requirements and Evaluation methods*.

As vendors submit HSMs to be evaluated and eventually approved and listed on the PCI Security Standards Council website, Visa will then review that all major vendors have successfully approved some HSMs. Once there are enough devices approved in the market, Visa will announce a future date by which if a HSM is newly deployed it must be a PCI-approved HSM. This is the same process Visa has established since instituting a PED testing program in 2003. When Visa does announce new PCI-approved HSM requirements for newly deployed HSMs, it will be for newly deployed devices and will not be retroactive. Although no future date has been set for PCI HSM adoption, clients are encouraged to move to these PCI-approved devices when available.