Visa Inc.
PIN Entry Device Requirements

The following information is applicable for Visa Inc. regions. Visa Inc. regions include Asia-Pacific (AP); Central and Eastern Europe, Middle East and Africa (CEMEA); Latin America and Caribbean (LAC); and North America (NA).

Objective

Visa is providing PIN Entry Device (PED) information for organizations to use in their PED purchasing, usage and deployment strategies. This information will help organizations protect themselves against PIN compromises, cardholder PIN data breaches, fraud, and ensures confidentiality and integrity of PIN data.

Return

Partnership

Visa first introduced a PED testing program in 2002 and Visa actively works together with all payment system participants including vendors, acquirers, processors, agents and merchants to ensure secure PIN data processing. All payment system participants play a significant role as the first line of defense to ensure PIN security. Cardholders interact with PIN accepting point-of-sale devices (POS), kiosks and automated teller machines (ATM) on a daily basis and trust these devices for secure and reliable PIN acceptance and processing. The PIN acceptance devices an organization purchases and deploys into the marketplace can greatly influence the security posture for an organization.

Return

PIN Entry Device Types

A first step in any organization's PIN security strategy is to ensure the PIN acceptance hardware used in the payment process is secure.

There are three basic types of PIN Entry Devices found in the payment industry today.

1) **Devices never tested by Visa or Payment Card Industry Security Standards Council (PCI SSC) -** Devices that have never been independently lab evaluated and approved by Visa or by PCI SSC as part of a defined testing program.
2) **Pre-PCI** – Devices that have undergone independent lab evaluation and security testing and approved by Visa under pre-PCI requirements. Review the Pre-PCI Device List to see if these devices are in your environment.
3) **PCI PIN Transaction Security (PTS) Approved–** Devices that have been evaluated against PCI PTS security requirements and obtained PCI PTS security device approval. Review the PCI PTS Approved Device List for more information.

Visa recognizes the Payment Card Industry (PCI) PIN Transaction Security (PTS) Program and PCI PTS approved devices as a fundamental component in PIN security.

Return

PCI PTS Security Requirements

Compliance with the PCI PTS security requirements reduces the likelihood and limits the potential impact of PIN compromise by establishing the minimum criteria for the design and manufacture of secure PEDs. The PCI PTS security requirements apply to Point of Sale (POS) devices and Encrypting PIN Pads (EPPs) used in ATMs and kiosks. Visa requires the use of PTS approved attended POS devices and the use of PTS approved EPPs used in ATMs, kiosks and automated fuel dispensers (AFD).

PCI PTS security requirements are evaluated on a three-year cycle to incorporate newly identified payment device vulnerabilities, emerging threats and changes in technology. If required, PCI PTS security requirements are updated intermittently to address more immediate security risks. New devices submitted by vendors for lab evaluation are tested against the current / highest version of the security requirements. Approved devices are listed on the PCI PTS Approved Device List with the version number of security requirements that it was tested against.

Each version of the requirements builds upon the security from the previous versions and devices tested against the higher requirement versions are better equipped to withstand known and current attacks against PIN accepting devices. Some security controls that have been incorporated into the requirements over the years include:

- **V1 PCI PED or EPP Security Requirements*** - Baseline security requirements with independent lab evaluation. Tamper evident controls required to easily detect unauthorized access to the device.
- **V2 PCI PED or EPP Security Requirements** - Improved tamper evident controls by requiring tamper responsive controls that detect intrusion attempts and subsequently destroys the content, including encryption keys.
- **V3 PCI PTS POI Security Requirements** (includes PED and EPP combined) Introduced secure read and exchange of data (SRED) capabilities that ensures cardholder account data is encrypted at the point of acceptance. (Note: Visa has no mandates for the use of SRED but implementation is a best practice)
- **V4 PCI PTS POI Security Requirements** (includes PED and EPP combined) - Improves testing evaluations and incorporates controls that address communication vulnerabilities that can be remotely exploited to gain access to sensitive data or resources within the device.

**Note there are also V1 HSM and UPT security requirements. Currently these requirements are designated as best practices for their use.*

Click here for a listing of Approved PCI PTS devices.

Return

Device Expiration and Sunset Dates Defined

Note: Visa requires that all device purchases must be made prior to the device PTS expiration date.

Entities must not purchase PCI PTS expired devices.

PCI PTS Expiration Date - When PCI PTS device approval expires. Visa requires that PED devices must not be purchased after the PCI PTS expiration date.

As a best practice Visa recommends that entities plan ahead and begin to stop purchasing PEDs as they are approaching their expiration date. Entities should update their PED inventories with newer higher version number of approved PEDs that will not expire for the longest amount of time possible. Organizations can continue to deploy expired PEDs as long as the entities purchased and took delivery of the PEDs prior to the PED's expiration date. (Note: sponsored entities should work with their sponsoring acquirer to ensure they are following any additional PED usage requirements specific to their acquirer).

As PED expiration dates approach, devices become:

- More vulnerable to attacks
- More likely to be involved in device and/or account data compromise incidents

Visa recommends removal of expired PEDs from the Visa network at the first opportunity and replacement with PCI PTS approved devices tested against the latest security version. To assist acquirers, agents, Encryption and Support Organizations (ESO) and merchants with expiring PED inventories, Visa recommends taking the following steps:

- Actively plan for the replacement of devices prior to the expiration date
- Invest in PEDs with the highest version to reap the benefits from state–of- the-art security
- Do not sell expired devices to secondary market
- Strive not use expired devices for new deployments
- Remove expired devices from production environments

Visa PED Sunset Dates –Visa has announced mandatory sunset dates for removing certain classes of devices from the Visa payment network. Visa PED Sunset dates only apply to Attended POS PEDs that have either never been certified by Visa or PCI SSC or are attended POS Pre-PCI Devices. These devices must be removed from the Visa payment network by the applicable Visa Sunset dates (see table below).

Return

PED Usage, Sunset and Expiration Dates

Lab Evaluation Status	PED Device Type	PCI PTS Device Expiration Date	Visa Purchase Requirements	Visa Deployment Requirement*	Visa Usage Requirement	Visa Sunset Mandates
Devices never lab evaluated by Visa or PCI	Attended POS PED	–	Not allowed	Not allowed		July 31, 2010
	EPP used in Unattended POS / ATM / Kiosk	–	Not allowed	Not allowed	Allowed if device has not been moved prior to Oct 2005	Phase out devices with TDES/EMV conversions
Pre-PCI Approved	Attended POS PED	Dec 31, 2007	Not allowed after device expiration date	Not allowed after sunset mandate	Not allowed after sunset mandate	Dec. 30, 2014
	EPP used in Unattended POS / ATM / Kiosk	Aug 31, 2008		Not allowed after device expiration date	Allowed if device has not been moved prior to Aug 2008	Phase out devices with TDES/EMV conversions
PCI PED or EPP PED V1.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2014	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommend device replacement
PCI PED or EPP PED V2.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2017	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommend device replacement
PCI PTS POI V3.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2020	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommend device replacement
PCI PTS POI V4.X	Attended POS PED EPP used in Unattended POS / ATM / Kiosk	April 30, 2023	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommend device replacement

**Visa deployment requirements are applicable to new and existing deployments.*

Return

Compromised PIN Entry Device List

Visa has identified older PED devices that have been reported as compromised and may be vulnerable to attacks. All organizations are encouraged to periodically review this list to identify if these devices are deployed in your environment and take action to replace the devices to protect from potential compromise or data loss. Please note, many of these older POS PEDs are either past Visa Sunset dates and should no longer be deployed or are approaching Visa sunset dates and should be targeted for replacement

Review the Visa Compromised PIN Entry Device (PED) List to learn more.

If you suspect PED tampering or compromise, visit the *If Compromise* website at www.visa.com/cisp. Specific steps are outlined in *What to Do IF Compromised* guide that will help minimize the impact to your organization. Early reporting of device tampering is important for your organization and the payment industry.

Visa realizes that immediate replacement of vulnerable PEDs may not be feasible and recommends following the PCI SSC Information Supplement: *Skimming Prevention – Best Practices for Merchants* to further secure the acceptance environment.

Return

Frequently Asked Questions (FAQ)

1. **What are Visa's requirements when purchasing PIN Entry Devices?**

   All newly purchased POS and EPPs PIN acceptance device models (including replacement devices) must have passed testing by a PCI-recognized laboratory and be listed on the PCI PTS Approved Device List at the time of purchase.

   All newly purchased ATMs and Kiosks / Automatic Fuel Dispensers (AFDs) must contain Encrypting Pin Pads (EPPs) that have passed testing by a PCI-recognized laboratory and be listed on the PCI PTS Approved Device List at the time of purchase.

2. **Why are there different versions of the PCI PTS Security Requirements?**

   PCI PTS security requirements are based on technology, environments and vulnerabilities known at the time the security requirements are published. Knowing that the security threat landscape is constantly changing, PCI security standards are reviewed and may be updated on a 3 year cycle to address new vulnerabilities and attack vectors. With each update a new version number is assigned to the testing requirements.

3. **What does PCI PTS Expiration date mean?**

   The expiration date for PCI-approved devices is the date upon which the device's PCI approval expires. Expired devices may not be able to withstand current vulnerabilities and attacks. Visa requires that PCI PTS devices must not be purchased after their expiration date.

4. **What are upcoming dates that organizations need to be aware of?**

   ***April 30, 2014*, PTS POS and PTS EPP PED V1.x Devices Expire**
   Organizations must not purchase these devices after this date.

   ***December 31, 2014*, Visa Sunset Date for Pre-PCI Attended POS PEDs**
   All pre-Payment Card Industry Point of Sale (Pre-PCI) PIN acceptance devices used in an attended environment must be replaced by PCI PTS approved devices. These pre-PCI devices are listed on www.visa.com/pinsecurity .

5. **PCI (POS and EPP V1.X PEDs expire 30 April 2014. What is the latest date that an acquirer or their merchant agents can purchase a V1.X PCI POS PED and/or EPP and still retain liability protection for the use of those devices?**

   The expectation is that all payment system participants must purchase and take delivery of PCI attended POS or EPP PEDs prior to April 30, 2014. These devices can then be deployed as needed.

   Under certain conditions, delivery may be taken subsequent to 30 April 2014. This is allowed when all of the following conditions are met:

- Full payment or invoicing has occurred prior to 30 April 2014.
- The devices purchased are manufactured inventory on hand prior to 30 April 2014.
- 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.

6. How do PED security requirements apply to existing unattended Kiosks and ATMs currently installed?

All newly deployed *unattended* POS PIN acceptance devices must contain an EPP that has passed testing by a PCI-recognized laboratory and is PTS approved. The intent of this requirement is not retroactive and currently there are no Visa requirements to replace EPPs within existing ATMs or other unattended PIN acceptance devices such as Kiosks and Automated Fuel Dispensers (AFDs). Visa rules require that if an ATM / Kiosk or AFD is moved or redeployed, it must contain a PTS approved EPP. Note, the PCI SSC has testing requirements for PTS approved Unattended Payment Terminals (UPTs) and it is a best practice to deploy Kiosks or AFDs that are UPT approved.

7. What happens when a PIN Entry Device is compromised?

A PIN compromise is the breaching of secrecy and/or security of a cardholder's personal-identification-number (PIN). A PIN Compromise can be at a network or device level. When PEDs are compromised at the device level, per V*isa's What to Do If Compromised guide*, entities must inform the PED Vendor of all details of the attack. By contract between PED vendors the PCI SSC, the Vendor must in turn inform the PCI SSC. When the PCI SSC is informed of the attack they will make the decision as to whether to delist a PED from the PTS approved device listing. Visa historically managed a list of older vulnerable non-lab evaluated and pre-PCI PEDs, however, more recently the PCI SSC delisted a V1.X device.

8. What is the impact to an Acquirer if they or their agent deploys PEDs that have not been evaluated by a PCI recognized laboratory or are not listed as a PCI PTS approved device?

Acquirers and their agents deploying PEDs that have not passed evaluation by a PCI recognized laboratory and which are not approved by PCI, or listed as expired 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. Additionally, they may be liable for penalties in accordance with the Visa International Operating Regulations, ID#: 0001288.

9. For liability protection, how can Acquirers and their agents ensure that PEDs they purchase are compliant with the applicable PIN Entry Device security requirements?

Acquirers and their agents should always review the PCI PTS Approved Device List and validate the device matches ***all*** of the following as listed on the website:

- Model Name, Hardware #,
- Firmware #, and, if applicable,
- Application #.
- Loader versions etc.

Relevant articles:

- Encrypting PIN Pads Must Be Industry-Approved, December 6, 2012
- Maximize Point-of-Sale PIN-Entry Device Security, December 6, 2012

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. For audit trail purposes, the purchaser must ensure that the hardware exactly matches to the PCI PTS listing and should make a print screen of the approved device details to ensure proper evidence of compliance with Visa's PED procurement and usage requirements.

10. How does the "expiration" date for a device's approval impact the Acquirer? For example, the PCI Version 1.x POS and EPP devices all expire 30 April 2014?

PCI security requirements are assessed every three years based on identified threats. If necessary, the requirements are updated. The approvals on devices evaluated against earlier versions of security requirements expire on a specific date.

Acquirers, processors, Encryption Support Organizations (ESO) and merchants must not purchase these devices after the specified expiration date.

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, ID#: 0001288

11. 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 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 had approval revoked for reasons other than normal approval

expiration.

12. What should entities consider when purchasing devices?

- Purchase only the highest version available PCI PTS approved devices.
- Evaluate current PED inventories and make plans to limit or stop purchasing devices approaching an expiration date.
- Your organization's policy should be to purchase the latest version of PCI approved PEDs to ensure 1) purchased devices have been evaluated against the most stringent of security requirements and 2) purchased devices will have the longest approved timeline.
- Upgrade PED devices that also support EMV acceptance (contact and contactless) in support of global EMV interoperability.

13. What does 'Recommend to remove from Visa Network' mean?

All payment system participants should be aware that expired devices can pose an increased risk to their organizations. These expired payment devices should be targeted for replacement.

14. What about devices that have been compromised?

Devices that have been compromised, as noted on www.visa.com/pinsecurity website should be physically secured in the short term and replaced with newer, more secure PTS approved versions of the product, or with different models that are PTS approved, whenever an opportunity presents itself.

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

- Implement a device monitoring / authentication system that can monitor the PED's electronic serial number.
- Develop and implement 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 secure terminals and PIN pads to counters to prevent PED removal with secure locking cable connections.
- Physically secure under lock and key the storage of terminals awaiting deployment and periodically validate the inventory on hand to asset records. Use terminal asset tracking systems/procedures for devices deployed, devices awaiting deployment, devices under repair and devices in transit to location.

Also refer to the *PCI SSC Information Supplement: Skimming Prevention –Best Practices for Merchants* document available on the PCI SSC website, https://www.pcisecuritystandards.org/pdfs/skimming_prevention_form.pdf

15. How do entities validate device compliance?

- Ensure that the PED hardware, firmware, application and PCI approval numbers; version; product type; and expiration date match exactly to the corresponding data on the PCI Approved PTS Device List.
- Take a screen shot of PED information from the Approved PTS Device List to include as part of your device acquisition records.
- As a best practice, ensure purchase orders and contacts include language support purchasing *only* approved PTS approved devices that are not expired.
- POs must include all device information that should serve as a confirmation that the pertinent device information exactly matches all PTS device information.

16. What other security measures should entites consider after PEDs have been deployed?

- Review the *PCI PIN Security Requirements* to understand their responsibility to always manage PEDs securely. This may include securing PEDs at the cash register with locking strands or cables to prevent PEDs from being easily removed.
- Deploy a terminal authentication system to enable remote monitoring of the PED's electronic serial number and/or to detect PED connectivity changes.
- Review the PCI SSC skimming prevention best practices guide is available to organizations, https://www.pcisecuritystandards.org/pdfs/skimming_prevention_form.pdf
- Merchants with wireless handheld PEDs should ensure they have inventory controls and that the devices are securely stored when not in use.
- Establish reporting and escalation procedures for devices that have been tampered with or have gone missing.
- Develop and implement 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 to PED devices unless fully validated and authorized. Authorized and validated repair technicians should still be escorted and monitored at all times.

17. Do Visa's PED purchase, usage and deploymentdates apply to Visa Europe?

No. The PED purchase, usage and deployemnt dates specified are applicable for Visa Inc. regions. Visa Inc. regions include Asia-Pacific (AP)/Central and Eastern Europe, Middle East and Africa (CEMEA); Latin America and Caribbean (LAC); and North America (NA). Dates specified in the Roadmap and FAQ do not apply to Visa Europe members or their sponsored agents.

Visa Europe has communicated dates that differ from Visa Inc. Global organization that are subject to comply with both Visa Inc and Visa Europe requirements should comply with the more stringent requirement. www.visaeuropepin@visa.com

18. How do the PCI Unattended Payment Terminal (UPT) requirements affect Visa's current EPP mandates for unattended POS PEDs/Kiosks?

In 2009 the PCI Security Standards Council published new PED testing requirements for Unattended Payment Terminals (UPTs) and Hardware Security Modules (HSM). Visa does not currently plan to set a compliance mandate for the usage of UPT approved devices. Use of a PCI approved EPP is a best practice, Visa may set UPT requirements for newly purchased / deployed unattended POS PEDs in the future and 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 greater overall device security than the current requirements which focus only on the EPP.

19. How will the PCI Hardware Security Module (HSM) requirements affect Visa's PIN Security a 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*.

c. PCI HSM approval

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 may announce a future date by which if a HSM is purchased / newly deployed it must be a PCI-approved HSM. This is the same process Visa has established since instituting a PED testing program in 2002. When Visa does announce new PCI-approved HSM requirements for newly deployed HSMs, it will be for newly purchased/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 more secure PCI-approved devices when available.

Return