Visa Inc.
PIN Entry Device Requirements

The following information is applicable for all Visa Inc. regions.

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

Last Updated: May 1, 2018

Objective

The Visa PIN Entry Device (PED) Requirements is intended to provide organizations information to assist them in their PED purchasing, usage and deployment strategies. This information will help organizations protect themselves against PIN compromises and cardholder PIN data breaches.

Return

Partnership

Visa is committed to protecting the Visa payment system and sensitive data that flows through the network. This includes Visa cardholder PIN data. Visa first introduced a Visa PIN Entry Device (PED) testing program in 2002 to ensure devices that accept and process a cardholder PIN in order to authenticate the cardholder for a payment transaction were secure and trusted devices.

Visa continues to work with all payment system participants including PED manufactures, acquirers, payment processors, third-party agents and merchants to ensure PIN processing is done securely. All payment system participants play a significant role in managing their products and when performing PIN services to ensure the secrecy of the PIN and protect the PIN from unauthorized disclosure.

Visa cardholders interact with PIN accepting point-of-sale devices (POS), kiosks and automated teller machines (ATM) on a daily basis and have come to trust these devices for secure and reliable PIN acceptance and processing. The PIN 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 (PED) found in the payment industry today.

1) **Devices never tested by Visa or Payment Card Industry Security Standards Council (PCI SSC) –** These devices have not been reviewed to understand their ability to protect cardholder PINs. They have not undergone an independently lab evaluation and they have not been approved by Visa or by the PCI SSC as part of a recognized security testing program. The ability of these devices to protect cardholder PINs is unknown and therefore these PED devices should not be trusted and not used.

2) **Pre-PCI** – These PEDs have performed an independent lab evaluation with security testing. These devices were approved by Visa using pre-PCI requirements established in the early 2000's. The Pre-PCI security requirements were developed based on the attack scenarios known at that time. Review the Pre-PCI Device List to see if these devices are in your environment. Organizations using Pre-PCI Devices should make it a priority to replace these devices with PCI PTS Approved Devices at first opportunity.

3) **PCI PIN Transaction Security (PTS) Approved–** These are PEDs that have been evaluated against versions of the PCI PTS Point of Interaction (POI) Security Requirements and have 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 fundamental components in PIN security.

Return

PTS Point of Interaction (POI) Security Requirements

PEDs that meet the PCI PTS Point of Integration (POI) Security Requirements greatly reduces the likelihood and limits the potential impact of PIN compromises by establishing minimum security criteria for the design and manufacture of PEDs. The PTS POI Security Requirements apply to Point of Sale (POS) devices and Encrypting PIN Pads (EPPs) used in ATMs, kiosks and automated fuel dispensers (AFD).

PCI PTS POI Security Requirements are evaluated and re-published on a three-year cycle to address newly identified vulnerabilities, emerging threats and changes in technology.

New devices submitted by hardware manufactures for lab evaluation are tested using the current and highest version of the security requirements. Only devices that meet and successfully fulfill all security requirements are listed on the PCI website, *PTS Approved Device List*, *https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices* . The list provides detailed information about the PED that includes the version number that corresponds to the security requirements that it was tested against.

Each version of the security requirements builds upon the security from the previous versions. Therefore, devices evaluated against the highest requirement versions are best equipped to withstand known and current attacks. Examples of security controls that have been incorporated into the different versions of the PCI PTS POI Security Requirements include:

V1 *- Baseline security requirements with independent lab evaluation. Tamper evident controls required to easily detect unauthorized access to the device.*
V2 *- Improved tamper evident controls by requiring tamper responsive controls that detect intrusion attempts and subsequently destroys the content, including encryption keys.*
V3 *- 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 SRED implementation is strongly encouraged as a best practice)*
V4 - *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.*
V5 – *Must meet detailed physical attack costing potential formulas and firmware scoping. Provides guidance on side-channel based attacks.*

Return

Device Expiration and Sunset Dates Defined

PCI PTS Expiration Date – The expiration date is a key indicator to what Visa rules apply and associated compliance for the purchase, deployment, use and retirement of Pin Entry Devices. (PED)

All organizations have a responsibility to know the security expiration dates associated with their PEDs since this can affect their security compliance to Visa. Everyone is encouraged to plan ahead and prepare to stop purchasing PEDs as they are approaching their expiration date. Organizations should update their PED inventories with newer versions of approved PEDs that have the longest amount security approval.

As PED expiration dates approach, devices may become:

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

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 markets
- Do not use expired devices for new deployments
- Remove expired devices from production environments

Visa PED Sunset Dates – Sunset Dates are the mandatory dates for removing certain classes of PEDs from the Visa payment network. Organizations with PEDs in the payment network after the Sunset Date has passed are considered non-compliant and the organization may be subject to non-compliant assessments.

PED Sunset dates may be specific to individual regions. Contact your regional Risk Representative for additional information.

Return

PED Purchase, Usage and Sunset Dates

Note: Visa may revise PED Requirements based on evolving threats to the payment ecosystem. Contact your regional Risk Representative for additional information.

Lab Evaluation Status	PED Type	PED Expiration Date	Purchase Requirements	Deployment Requirement*	Usage Requirement	Sunset / Retire 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 *Europe Region: Devices must be retired by December 31, 2020*
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 *Europe Region: Devices must be retired by December 31, 2012*
	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 *Europe Region: Devices must be retired by December 31, 2020*
PCI PED or EPP PED V1.X	Attended POS PED	April 30, 2014	Not allowed after device expiration date	Allowed if purchased prior expiration date. *Europe Region: Deployment is not allowed after device expiration date*		Recommend device replacement *Europe Region: Attended/Semi-Attended devices must be retired by December 31, 2017. EPP used in unattended must be retired by December 31, 2020*
	EPP used in Unattended POS / ATM / Kiosk					
PCI PED or EPP PED V2.X	Attended POS PED	April 30, 2017	Not allowed after device expiration date	Allowed if purchased prior expiration date.		Recommend device replacement *Europe Region: EPP used in unattended TBD- Under evaluation*
	EPP used in Unattended POS / ATM / Kiosk					
PCI PTS POI V3.X	Attended POS PED	April 30, 2020	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD: Under evaluation
	EPP used in Unattended POS / ATM / Kiosk					
PCI PTS POI V4.X	Attended POS PED	April 30, 2023	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD: Under evaluation
	EPP used in Unattended POS / ATM / Kiosk					
PCI PTS POI V5.X	Attended POS PED	April 30, 2026	Not allowed after device expiration date	Allowed if purchased prior expiration date.		TBD: Under evaluation
	EPP used in Unattended POS / ATM / Kiosk					

Note: PEDs in the Europe Region formerly covered by the Semi-Attended environment definition are now governed by the requirements for the Attended environment.

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 these devices to protect against potential compromise or data loss.

Please note, many of these PEDs are either past Visa Sunset/Retire dates and must not be deployed, or are approaching Visa Sunset/Retire 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 (PED)?**

   All newly purchased PIN acceptance device models (including POS, EPPs and 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.

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. Realizing that the security threat landscape is constantly changing, PCI security requirements are reviewed (and may be updated) on a 3 year cycle to address new vulnerabilities and attack vectors. A new version number is assigned to each new security requirements update, e.g. PTS v5.

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

   The expiration date for PCI-approved devices is the date upon which the device's PCI security approval expires. Expired devices may not be able to withstand current vulnerabilities and attacks. Visa requirements for purchasing, use and retirement or replacement is dependent on the PED expiration date.

4. **PCI POS and EPP V2.X PEDs expire 30 April 2017. What is the latest date that an acquirer or their merchant agents can purchase a V2.X PCI POS PED and/or EPP?**

   All payment system participants must purchase and take delivery of V2.x PCI attended POS or EPP PEDs prior to April 30, 2017*. These devices can then be deployed as needed after the expiration date.

   Under certain conditions, delivery may be taken subsequent to 30 April 2017. This is allowed when all of the following conditions are met:

   - Full payment or invoicing has occurred prior to 30 April 2017.
   - The devices purchased are manufactured inventory on hand prior to 30 April 2017.
   - 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.

5. **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.

6. What happens when a PED is compromised?

A PIN compromise is the breach of secrecy and/or the security of a cardholder's personal-identification-number (PIN). A PIN compromise can be at a network or device level. When PINs are compromised at the device level, e.g.PED, an organization must follow the instructions outlined in the *What to Do If Compromised guide.* Organizations must inform the PED manufacture and of all details of the attack. In turn, the PED manufacture must inform the PCI SSC of the reported compromise. When the PCI SSC is informed of the attack, they will conduct an investigation and will make the decision as to whether to delist a PED from the PTS Approved Device Listing. Visa manages a list of older vulnerabilities for non-lab evaluated and pre-PCI PEDs. PCI is responsible for communicating the status of PCI PTS devices.

7. 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 are not compliant with Visa PIN requirements and are liable in the event of a PIN compromise that is attributable to the use of those devices. Non-compliance assessments are in accordance with the Visa Core Rules, ID#: 0001288.

8. 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 publicly available, PCI PTS Approved Device List and verify the devices in use matches ***all*** the information listed on the website that includes:

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

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 the PCI PTS listing and obtain a screen print of the approved device details and keep with relevant records to ensure proper evidence is maintained of the device compliance with Visa's PED Requirements.

9. Can Acquirers use a non-PED manufacture for key injection after the device expiration?

Secure key loading is fundamental to the security of the PED device, therefore Visa requires that all key injections to PEDs are performed by organizations that have demonstrated compliance to PCI PIN Security Requirements for Key Injection Facilities (KIF).

Acquirers and merchants must use compliant KIF vendors. To verify a vendor's compliance to stated requirements, visit Visa Global Registry of Service Providers at www.visa.com/onthelist. Search Service Providers and check PCI-PIN in the Validation Type field. Click on the search button. All compliant companies will be listed. Verify the key injection vendor in question is listed with PCI-PIN Services.

10. How does the "expiration" date for a device's approval impact the Acquirer? For example, the PCI Version 3.x POS and EPP devices all expire 30 April 2020?

A device expiration date may affect the ability to purchase or use a PED on Visa's network. Organizations are requested to review the PIN Entry Device (PED) Requirements for specific rules that are dependent on the PED expiration dates. For additional information, contact the Risk Representative in your region.

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 and has not been identified to sunset/retire. 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 PEDs with the highest version number to realize the highest level of security and the longest security life.
- Evaluate your current PED inventories and make plans to limit or stop purchasing devices approaching an expiration date.
- Your organization's policy should be to purchase only 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 does 'Device must be retired' mean?

Devices identified to be retired are to be removed from the Visa network by the sunset date.

15. 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.

Devices that have been compromised should implement mitigating steps until they can be replaced that includes but is not limited to the following:

- 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 visually inspect terminals 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

16. How do organizations demonstrate PED compliance?

- Ensure that the PED hardware, firmware, application and PCI approval numbers; version; product type; and expiration date match exactly to the corresponding information on the PCI Approved PTS Device List.
- Obtain 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 contracts include language that requires purchasing *only* approved PTS devices and forbids the purchase, deployment and use of devices that have expired.
- Purchase orders must include all device information that serves as a confirmation that the PED information exactly matches all PTS device information.

17. What other security measures should entities consider after PEDs have been deployed?

- Review the *PCI PIN Security Requirements* to understand Visa requirements for PIN entry devices.
- Deploy a terminal management 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.

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 can I contact Visa if I have PIN or PED related questions?

For more information about the Visa PIN Security Program, including PED requirements or questions, visit Visa's PIN Security website at www.visa.com/pinsecurity, or e-mail your regional Visa Risk Representative at the email addresses below:

North America:	pinna@visa.com
LAC:	pinlac@visa.com
AP and CEMEA:	pinsec@visa.com
Europe	visaeuropepin@visa.com
Global:	pin@visa.com

Return