Payment Network Requirements for PCI PTS POI Devices in Transit

Background

The transit industry often lacks clarity about payment network requirements for Payment Card Industry PIN Transaction Security Point of Interaction (PCI PTS POI) device approvals for terminals. Questions frequently arise, such as why "contactless only" terminals need approval when they do not support PIN encryption. This document aims to clarify these requirements and their rationale for the transit industry.

Frequently Asked Questions

1. What is the PCI Security Standards Council?

"The Payment Card Industry Security Standards Council (PCI SSC) is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. Their role is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders. They achieve this with a strategic framework to guide the decision-making process and ensure that every initiative is aligned with PCI's mission and supports the needs of the global payments industry."[1]

2. What is EMVCo?

EMVCo is a global body that creates and manages the EMV® specifications that enable seamless and secure card-based payments for businesses and consumers worldwide. For in-store, e-commerce or remote transactions, the process needs to be familiar, convenient and reliable. EMV technology helps make this possible with technologies such as Secure Remote Commerce, EMV 3D-Secure, and tokenization. EMVCo collaborates with industry stakeholders to develop these standards and the associated testing processes.

3. What does the PCI PTS POI Standard cover?

The PCI PTS POI Standard "offers security requirements for the characteristics and management of devices used to protect cardholder PINs (personal identification numbers), account data, and other sensitive payment card data at the point of interaction. POI devices are used by merchants, financial institutions, and other payment industry participants at the point-of-interaction to capture payment card data during payment card transactions."[2]

4. What is the difference between EMVCo and PCI SSC?

EMVCo and PCI SSC are both involved in securing payments, but address different aspects. EMVCo sets technical security protocols through specifications for chip-based payment cards and chip readers in payment terminals, ensuring secure and interoperable chip transactions. PCI SSC sets security standards

[1] "PCI Security Standards Council at a Glance," https://listings.pcisecuritystandards.org/documents/At_a_Glance_Role_of_the_PCI_SSC.pdf.
[2] "PIN Transaction Security (PTS) Point of Interaction (POI) Standard," https://www.pcisecuritystandards.org/standards/pts-point-of-interaction-poi/

for account data protection, with the PCI PTS POI standard covering payment terminal devices to protect cardholder data and PINs during payment transactions.

5. What is EMVCo certification?

EMV Level 1 testing assesses the compliance of the acceptance device with the communication protocols defined within the EMV Chip and Contactless Specifications. These cover the transfer of data between the acceptance device and the payment instrument (such as chip cards, smartphones, and smartwatches).

EMV Level 2 testing assesses the compliance of the acceptance device with the software features defined within the EMV Chip and Contactless Chip Specifications. EMVCo has defined the contact kernel approval process for contact chip transactions. For contactless transactions, EMVCo has launched an approval process for the new EMV contactless kernel.

The combination of EMVCo Functional Approvals for EMV acceptance devices is known as Terminal Type Approval. The approval process assesses whether payment products meet EMV specifications and requirements for performance and compatibility.

Level 2 testing for contactless kernels (other than the EMV contactless kernel) and all Level 3 certifications are done with each payment system and are independent of EMVCo.

6. Why do EMVCo-compliant devices require compliance with PCI SSC standards?

EMV specifications and PCI SSC standards work together to provide a layered security approach addressing different aspects of payment security. EMV chip specifications help prevent counterfeit fraud at the point of sale, while devices compliant with the PCI PIN PTS POI Standard are used by a merchant at the point of interaction for capturing payment card data and validating approval of its use for a transaction. The PCI SSC urges merchants to use approved PCI PIN PTS devices in their payment environments.

7. Why does a "contactless only" terminal need to be a PCI PTS POI approved device when it does not allow a credit or debit card to be inserted or prompt for PIN entry?

PCI PTS POI approved devices are designed to reduce data breach risks by meeting defined security standards for handling sensitive cardholder information, such as the primary account number (PAN) and expiration date. Relevant security threats to these devices include skimming, malware, physical tampering, replay attacks, and manipulation of communication interfaces between the terminal and integrated devices. The PCI PTS POI Standard is intended to help mitigate these types of security vulnerabilities. Therefore, compliance with this standard is considered important. Additional information is available in the PCI PTS POI v7 Technical FAQ, available at FAQ_PCI_POI_Technical_FAQ_v7_June_2025.pdf.

8. What are payment network policies for transit access terminals?

The following table summarizes the current published policies and requirements related to PCI PTS POI for contactless acceptance devices used as transit access terminals for each payment network. For any questions regarding these policies, merchants are advised to contact their acquirer for additional information.

Payment Network	PCI PTS POI Requirements
American Express	• PCI PTS POI Approval is required for contactless devices that are reading and handling card/PAN data even if it is a contactless only reader, per PCI PTS POI requirements
UnionPay International (UPI)	• UPI does not have a strict requirement that the transit terminal needs to be PCI PTS POI certified.
Discover Network / Diners Club International / PULSE	• Discover strongly recommends PCI PTS POI approval for contactless devices that read and handle card/PAN data, even if it is a contactless only reader, per PCI PTS POI requirements.
JCB	• JCB strongly recommends that PCI PTS POI approval is obtained for devices that handle card/PAN data.
Mastercard	• Newly deployed transit terminals with PIN entry capability must be PCI PTS POI approved; in addition, the transit operator's data environment must comply with the PCI Data Security Standard (PCI DSS), including not storing account data after authorization, encrypting account data in transit and following the inventory/tamper inspection procedures for POIs. A security best practice for terminals that manage access to transit systems (such as turnstiles/gates) and physically integrate card readers is for the latter to be PCI PTS POI approved as Secure Card Readers (SCRs).
NYCE Payment Network	• NYCE relies on the technology requirements of each of the global payment networks supporting their applications at the terminal and the U.S. Common Debit AID they support.
Visa	• Visa mandates compliance with PCI PTS POI standards for devices accepting Visa cards, including transit terminals.

Resources

- Payment Card Industry Security Standards Council (PCI SSC), https://www.pcisecuritystandards.org/
- PCI SSC Frequently Asked Questions, https://www.pcisecuritystandards.org/faqs/
- EMVCO, https://www.emvco.com

DISCLAIMER

This document is provided solely as a convenience to readers, as a high-level overview of payment network requirements for PCI PIN Transaction Security Point of Interaction (PCI PTS POI) standard certification of POI devices. While we have attempted to ensure that the information in this document is accurate as of the original date of publication, such information is provided "AS-IS", does not constitute legal, business or technical advice, and should be relied on for any purpose. All warranties of any kind, express or implied, regarding the information herein are expressly disclaimed. Readers interested in learning more about payment network requirements for PCI PIN Transaction Security Point of Interaction (PCI PTS POI) standard certification of POI devices should consult their respective security providers, business partner, subject matter experts and professional and legal advisors.