Terminal and PIN Entry Security Standards

Frequently Asked Questions

1 September 2020

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third-party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Contents

Terminal and PIN Entry Security Standards Frequently Asked Questions

Terminal and PIN Entry Security Standards

Terminal and PIN Entry Security Standards—Frequently Asked Questions

Document Purpose

The purpose of this document is to answer commonly asked questions about the Mastercard security standards applicable to terminals such as ATM and POS terminals, including PIN entry standards.

Reference Document

The ***Security Rules and Procedures***—*Chapter 2 Cybersecurity Standards and Programs* and *Chapter 4 Terminal and PIN Security Standards*—is available on Mastercard Connect™ for further references.

Terminal and PIN Entry Security Standards

The following list of questions is designed to assist with Mastercard security compliance requirements applicable to terminals and PIN entry.

Q: What are the PIN Security Standards?

The Mastercard PIN Security Standards ensure the protection of personal identification numbers (PINs) during their entire life cycle in the acquirer domain. Mastercard acquiring institutions (or their agents, such as merchants and service providers) must be compliant with such standards when handling PINs entered by cardholders at PIN enabled terminals.

The Mastercard PIN Security Standards refer to several PCI standards specifically aimed at the protection of PIN:

- PCI PIN Security Requirements
  These requirements are mainly targeted at organizations such as processors and acquirers. They address the secure management, processing, and transmission of PIN data during online and offline payment card transaction processing at ATMs and POS terminals.

- PCI Software-based PIN Entry on COTS (SPoC) Security Requirements
  These requirements are mainly targeted at organizations such providers of SPoC Solutions and developers of PIN Cardholder Verification Method (CVM) Applications, Software Development Kits (SDKs) or Application Programming Interface (APIs) for COTS devices (such as mobile phones or tablets) used in SPoC Solutions.

- PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements
  These requirements are mainly targeted at organizations such as manufacturers of encrypting PIN pads for ATMs and Dedicated Hardware POS terminals.

- PCI PTS Hardware Security Module (HSM) Security Requirements
  These requirements are mainly targeted at organizations such as manufacturers of HSMs. Such devices address the confidentiality and/or data integrity of financial transactions processed in the Mastercard acceptance network.

Q: What types of devices are in scope of Mastercard PIN Security Standards?

Devices that are in scope of Mastercard PIN Security Standards include HSMs, PIN pads (EPPs) for ATMs and software/hardware modules that enable PIN entry in two categories of POS terminals:

- Encrypting PEDs in/used by Dedicated Hardware POS terminals
- PIN CVM Applications running in POS terminals based on COTS devices (sometimes referred to as MPOS terminals) that are part of PCI SPoC Solutions.

Q: Where can I find security requirements for ATMs and Dedicated Hardware point-of-sale (POS) terminals?

Security requirements for ATMs and Dedicated Hardware POS terminals can be found in 2.4.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs) in the *Security Rules and Procedures* on Mastercard Connect™. These rules address the secure entry of PINs on ATMs and POS terminals.

Q: Where can I find security requirements for mobile POS (MPOS) terminals that accept PIN entry?

Security requirements for MPOS terminals that accept PIN entry can be found in 2.4.2 Software-based PIN Entry using PIN CVM Applications in the *Security Rules and Procedures*. These rules address the secure entry of PINs on COTS devices.

Q: Where can I find security requirements for hardware security modules (HSMs)?

Security requirements for HSMs for the acquirer domain and for operations such as PIN translation and acquirer keys generation can be found in 2.4 PIN Security Standards of the *Security Rules and Procedures*.

Q: What is meant by the acquirer domain?

The acquirer domain is an abstract reference to all commercial and IT environments that contribute to the acceptance of transactions at the Point of Interaction (POI). With respect to compliance with the Mastercard PIN Security Standards, they include PIN related activities such as PIN translation, encryption, cryptographic management and PIN entry, performed by acquirers and their agents such as merchants, processors, terminal manufacturers and key initialization facilities.

Q: What is meant by the issuer domain?

The issuer domain is an abstract reference to all commercial and IT environments that contribute to the activities of issuers. With respect to PIN security, it includes activities such as PIN generation and PIN validation.

Q: What are Dedicated Hardware POS terminals?

Dedicated Hardware terminals are POS terminals that generally are purpose built and rely on hardware as the first layer of protection (as opposed to POS devices based on a COTS device, such as a mobile phone or a tablet, whose first layer of protection is normally the software of the device).

Q: What are commercial off-the-shelf (COTS) devices?

COTS devices are devices normally used for personal usage such as smartphones or tablets.

Q: When can COTS devices be used as acceptance devices?

COTS devices can be used in the acquirer domain by merchants as POS terminals with the necessary Application and card or payment device reader (either a peripheral reader or an embedded near-field communication [NFC] reader). COTS devices with an embedded NFC reader may be part of PCI Contactless Payments on COTS (CPoC) Solutions.

Q: When can COTS devices be used for PIN enabled acceptance?

COTS devices can be used for PIN enabled acceptance when the PIN is entered either on a peripheral PIN pad or directly on the touch screen. The Application running in the COTS device (PIN CVM Application) and the peripheral card or payment device reader must be part of a PCI SPoC Solution.

From a security perspective, COTS devices generally rely on software as the first layer of protection (as opposed to Dedicated Hardware devices, whose first layer of protection is normally the hardware).

Q: When is the designation PIN entry device (PED) and encrypting PIN pad (EPP) used? What is their relationship with ATM and POS terminals?

PED is the generic designation of the software and hardware modules of a Dedicated Hardware POS terminal that are evaluated by the PCI PTS POI program for the purpose of secure PIN entry. PEDs range from simple PIN pads (to be used as peripheral of POS terminals), original equipment manufacturer (OEM) PEDs (to be integrated into other POS terminals) or complete POS terminals. PEDs may include reader(s) of cards or payment devices.

EPP is the generic designation of the software and hardware modules dedicated to PIN entry to be integrated into ATMs and self-service POS terminals.

Q: What are MPOS terminals?

MPOS terminals are POS terminals based around COTS devices and payment acceptance applications they host. They can be used with peripheral readers and PIN pads, such as used by PC based POS terminals. Alternatively, they can be part of a:

- PCI SPoC Solution, where the PIN is entered in the touch screen of the COTS device and an external reader is used; or
- PCI CPoC Solution, using exclusively the NFC reader of the COTS device (and where PIN entry is not allowed in the POS terminal).

Q: What are the Mastercard security requirements for MPOS terminals?

Mastercard security requirements for MPOS terminals include the following:

- If a MPOS terminal uses a peripheral for PIN entry, the latter device must follow the standards applicable to Dedicated Hardware devices (2.4.1 PIN Entry Devices [PEDs] and Encrypting PIN Pads [EPPs] in the *Security Rules and Procedures*)
- If PINs are entered at the COTS device, the PIN CVM Application and the necessary peripheral card and payment device reader must be part of the PCI SPoC Solution. (2.4.2 Software-based PIN Entry using PIN CVM Applications)
- If the merchant exclusively uses the embedded NFC reader of the COTS device, the Application must be part of a PCI CPoC Solution

PCI approved devices and solutions applicable to MPOS terminals can be found on the PCI Security Standards Council (PCI SSC) website at www.pcisecuritystandards.org/assessors_and_solutions/.

Q: What are the compliance requirements for HSMs in the acquirer domain?

Compliance requirements for HSMs in the acquirer domain state that newly deployed HSMs must be listed either on the PCI SSC website as Approved PCI PTS Devices (with a valid SSC listing number and under the device type "HSM") **OR** in the NIST Cryptographic Module Validation Program (CMVP) list (with a valid listing number and approved to FIPS 140-2 Level 3 or higher).

Q: What are the compliance requirements for HSMs in the issuer domain?

Compliance requirements for HSMs in the issuer domain includes guidelines for operations such as PIN generation and verification and can be found in the *Issuer PIN Security Guidelines* on Mastercard Connect™. These guidelines recommend the use of HSMs listed by the PCI PTS program.

Q: Mastercard requires acquirers to be compliant with the Payment Card Industry (PCI) PIN Security Standards. What does that mean for devices used in the acquirer domain such as HSMs, ATMs and POS terminals?

Devices used in the acquirer domain such as HSMs, ATMs and POS terminals that accept PIN products must meet the requirements of a "Physically Secure Device" as defined in ISO 13491. This is evidenced by their being validated and approved against one of the following:

- One of the versions of the PCI PTS Standard, as members of device type EPP, PED or unattended payment terminal (UPT) - collectively known as POI devices, and Approval Class HSMs; or
- Federal Information Processing Standard (FIPS) 140-2 level 3 or higher (for HSMs only).

Depending on the stage of the life of the device in the Mastercard acceptance network, the acquirer or its agent must proceed as follows for PEDs (for POS terminals), EPPs (for ATMs and other self-service devices):

1. Newly deployed devices:
   - The model must be listed with a valid SSC listing number under device types "OEM/PED", "OEM/UPT" or "OEM/EPP" in the Approved PCI PTS Devices list. Devices with expired PCI

PTS approval (i.e. listed in the PIN Transaction Security Devices with Expired Approvals list), may be deployed in new locations if they were in inventory before the expiration of the approval of the model.

2. Device replacing due to fault condition:
   - If the model of the device to be replaced has its PCI PTS approval expired, the device may be replaced like for like. Mastercard recommends replacement with a model that is listed as approved from the latest PCI PTS version feasible.
3. Device's end of business life:
   - Mastercard recommends replacement with a device whose model is PCI PTS listed as approved from the latest PCI PTS version feasible.
4. Device sunsetting:
   - In exceptional circumstances such as widespread compromise, Mastercard, through an announcement, may require acquirers to stop processing Mastercard branded cards and accepting devices from specific models.

Q: Can PCI PIN Transaction Security (PTS) devices with expired approval be newly deployed in the Mastercard acceptance network?

No. After the PCI PTS expiration, devices may no longer be used in merchant environments. However, if a device model approval expires while the device is in inventory, the device can continue to be used until the end of business life or Mastercard announces a sunset date for the device model.

Mastercard advises acquirers to mitigate attacks by using the most recent models in their deployments and to replace devices before their PCI PTS approval expiration.

Q: What are the Mastercard deployment and sunsetting requirements applicable to the different PCI PTS generations of terminals?

Mastercard deployment and sunsetting requirements applicable to the different PCI PTS generations of terminals are described in the following table:

PIN entry device (PED or EPP); security generation	Latest date for devices to be newly deployed in the Mastercard network (PCI device list expiration)	Any models covered by sunset announcement by Mastercard so far?	Can devices still be currently in operation?
PCI v1	30 April 2014	No	Yes, replacement strongly recommended
PCI v2	30 April 2017	No	Yes, replacement recommended
PCI v3	30 April 2021	No	Yes, replacement recommended before 30 April 2021
PCI v4	30 April 2023	No	Yes, replacement recommended before 30 April 2023
PCI v5	30 April 2026	No	Yes, replacement recommended before 30 April 2026

PCI v6	30 April 2030	No	Yes, replacement recommended before 30 April 2030

Q: Are PCI PTS devices with expired approval eligible to participate in the Mastercard Terminal Integration Process (M-TIP)—chip end to end validation of POS terminal configurations?

Yes. PCI PTS devices with expired approval are eligible to participate in M-TIP if they were in inventory prior to their PCI PTS expiration. Devices with expired approval can be found in the PIN Transaction Security Devices with Expired Approvals list.

Q: When would Mastercard announce a sunset date?

Mastercard may announce a sunset date for a given device model in exceptional circumstances such as widespread compromise of the device model. After the sunset date, devices of a given device model must no longer accept Mastercard branded cards and payment devices.

Q: Has Mastercard announced a sunset date for a model?

No. Mastercard has not yet announced any sunset date of any model of PCI PTS approved devices. This may occur in exceptional cases, for example, the global compromise of a device. Once deployed, devices may accept Mastercard-branded cards or payment devices until their business end-of-life, or whenever Mastercard announces a sunset date.

Q: Do Mastercard PIN security requirements apply differently to devices that operate in attended environments vs. non-attended environments?

No. Mastercard PIN security requirements do not differentiate between attended PIN entry (for example in PEDs in POS terminals or PIN pads) and non-attended PIN entry (for example in EPPs used in ATMs and self-service devices).

Q: Do all payment brands require compliance with PCI PTS standards?

All payment brands refer to the PCI PTS standards, however, brands may have specific brand rules, for example differentiation among regions, categorization of devices, device sunsetting, etc. Mastercard recommends contacting other payment brands directly for information on such requirements.

Q: How do Mastercard PIN Security Standards address the beginning-of-life of POS terminals with PIN Entry in the Mastercard acceptance network?

For Dedicated hardware POS terminals—2.4.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs) in the *Security Rules and Procedures* primarily requires a newly deployed device in the Mastercard acceptance network to have its terminal model listed on the PCI SSC website as an Approved PCI PTS Device.

For COTS devices where PINs are entered in the touch screen—2.4.2 Software-based PIN Entry using PIN CVM Applications in the *Security Rules and Procedures* primarily requires that the Application of the POS terminal (PIN CVM Application) is listed in a PCI SPoC Solution and uses as accessory a reader supported by its specific Approved PCI SPoC Solution.

Q: How do Mastercard PIN Security Standards address the end-of-life POS terminals with PIN entry in the Mastercard acceptance network?

For Dedicated hardware POS terminals—2.4.1 PIN Entry Devices (PEDs) and Encrypting PIN Pads (EPPs) in the *Security Rules and Procedures* primarily allows terminals to continue to accept Mastercard branded cards and payment devices until either the end of their business life or Mastercard announces a sunset date (may happen in exceptional circumstances such as a global compromise).

For COTS devices where PINs are entered—2.4.2 Software-based PIN Entry using PIN CVM Applications in the *Security Rules and Procedures* allows terminals to continue to accept Mastercard branded cards and payment devices until determined by the PCI SPoC Solution itself. As attackers' security skills evolve, the Monitoring/Attestation System of a PCI SPoC Solution may determine that a given PIN CVM Application or COTS device operating platform is no longer suitable to support secure PIN entry and may impose transaction processing restrictions. These restrictions may include halting the full transaction capability of the PIN CVM Application.

Q: Do PIN Security Standards make a compliance differentiation between PEDs and EPPs?

No. PIN Security Standards do not make a compliance differentiation between PEDs and EPPs. Both types of PCI PTS certified devices PEDs (PEDs, to be part of purpose built POS terminals) and EPPs (EPPs, the PIN entry module of self-service devices) are subject to the same life cycle rules in the Mastercard acceptance network (initial deployment conditions, replacement limitations and sunset conditions and dates).

Q: Are the PIN Security Standards applicable to issuers?

No. All issuers and their agents performing PIN processing should refer to the *Issuer PIN Security Guidelines* on Mastercard Connect™ for all aspects of issuer PIN and PIN key management, including PIN selection, transmission, storage, usage guidance, and PIN change. Issuers should follow and enforce these guidelines.

Mastercard Standards for the issuer domain can be found in Chapter 4 Terminal and PIN Security Standards of the *Security Rules and Procedures*.

Q: What are acceptance terminals?

Acceptance terminals are POS terminals, ATM terminals and bank branch terminals. When one of the terminals is newly deployed and supports PIN enabled products, they must respectively include/use a PED or an EPP that is listed on the PCI SSC website as Approved PCI PTS Devices (with a valid SSC listing number and under device types "OEM/PED", OEM/UPT or "OEM/EPP").

Q: Is an HSM an acceptance terminal?

No. In the acquirer domain, HSM are not directly involved in the acceptance of cards and payment devices at the point of interaction. However, HSMs support cryptographic operations in the acquirer domains such as PIN translation, generation of keys for terminals, etc.

Q: Can PEDs and EPPs with expired PCI PTS approval operate in the Mastercard acceptance network?

Yes. PEDs and EPPs with expired PCI PTS approval can operate in the Mastercard acceptance network. Newly deployed PEDs and EPPs (used/part of ATMs and POS terminals) must be listed in the Approved PCI PTS Devices list. Devices in inventory may continue to be used after their PCI PTS approval expired and the models transitioned to the PIN Transaction Security Devices with Expired Approvals list.

Q: What is the relationship between PCI PIN Security Requirements, PCI PIN PTS Point of Interaction (POI) Modular Security Requirements and PCI PTS HSM Security Requirements?

The PCI PIN Standard define security requirements in the scope of the acquirer domain. These requirements address the secure management, processing, and transmission of PIN data processed at ATMs, POS terminals, HSMs and organizations that participate in transactions initiated at the POI by card and payment devices.

The PCI PTS POI Standard and the PCI PTS HSM Standard include security requirements for devices' vendors. Once evaluated and listed by the PCI SSC, these devices may be used in the acquirer domain by acquirers and their agents.

Q: What is the difference between Secure Card Reader (SCR) and Secure Card Reader for PIN (SCRP)?

A SCR is an encrypting card reader that either is intended for use with a non-secure device, such as a mobile phone or other device, or may be defined as an OEM product type to be integrated into a POS terminal. A SCRP may be used in PCI SPoC Solutions. SCRPs perform PIN translation from PIN blocks received from the payment application on a COTS device to a PIN block, either for conveyance to the processing host or for offline verification.

Q: What is a standalone magnetic stripe reader (MSR)?

A standalone MSR is optionally used as a peripheral of a COTS device in a PCI SPoC Solution. MSRs encrypt the data read from the card or payment device and conform to either:

- the PCI PTS POI Modular Security Requirements (validated by the PCI PTS program); or
- the Non-PTS Approved MSR Security Requirements and Derived Test Requirements in the SPoC Magnetic Stripe Readers Annex Security and Test Requirements (validated by the PCI SPoC program).

Q: What is PCI PTS Secure Reading and Exchange of Data (SRED) approval?

The SRED module in PCI PTS ensures that cardholder account data is encrypted immediately upon reading, at the point of acceptance. SRED compliance is required for POS terminals eligible to participate in PCI Point-to-Point Encryption (P2PE) Solutions.

Q: What is the difference between PCI Software-based PIN Entry on COTS (SPoC) Security Requirements and PCI Contactless Payments on COTS (CPoC) Security Requirements?

The difference between PCI SPoC Security Requirements and PCI CPoC Security Requirements is that SPoC is designed specifically for PIN entry using a validated external reader (for example, SCRP) within a COTS environment, whereas CPoC uses the NFC interface directly in the COTS device without the PIN entry.