

How should payment terminals be considered during a PCI DSS assessment?

PCI SSC FAQ | Article 1301 | August 2023

The PCI PIN Transaction Security (PTS) standards define physical and logical security requirements for different types of payment devices, including PIN-entry devices (PEDs) and other point of interaction (POI) devices. The PTS POI standard protects the PIN, which is the original objective of the PTS standard. Devices approved to PTS with SRED (Secure Reading and Exchange of Data) have additionally been assessed to provide the option to encrypt account data. PCI PTS devices with SRED, when used as part of a PCI-listed Point-to-Point Encryption (P2PE) solution, can facilitate PCI DSS scope reduction for merchants. However, for many PCI PTS devices the use of SRED is optional and this may be controlled by the payment application resident in the payment terminal. These payment applications can be expected to vary based on the merchant, terminal model, acquirer, and region/location. Therefore, unless included as part of a validated PCI P2PE Solution, or assessed against the PCI Secure Software requirements, an assessor should not assume that any payment terminal is encrypting cardholder data without further validation.

While use of PTS-approved payment devices can facilitate PCI DSS compliance, such devices do not by themselves guarantee PCI DSS compliance or reduce the scope of a merchant's cardholder data environment. The boundaries of the cardholder data environment are not affected by the presence or absence of a PTS-approved terminal, and any payment terminal interactions with the merchant's environment are in scope for a merchant's PCI DSS implementation. Payment terminals, regardless of whether they are validated to the PCI PTS POI standard, must be reviewed during a PCI DSS assessment to confirm that payment account data is protected during storage, processing, and transmission; either through encryption within the terminal, or by PCI DSS controls maintained across the interfacing merchant systems.

Often, the payment terminals will be managed by a third party (for example, the merchant's acquiring bank), and not by the assessed entity. Also, a terminal management system (TMS) may be used to manage the terminals and to update software and configurations on those payment terminals. The entity or assessor should determine if a TMS is in use, and if so, which entity is responsible for the TMS and whether the TMS is a connected-to system that needs to be included in scope for the merchant's PCI DSS assessment. The assessed entity should work with the third-party as part of its regular business-as-usual processes to maintain compliance of the payment terminals, and to prepare the appropriate evidence to demonstrate compliance with the applicable PCI DSS requirements to its assessor.

Assessors conducting these assessments are expected to possess sufficient knowledge and experience to conduct technically complex assessments associated with payment devices in the CDE to confirm the applicable PCI DSS requirements are met, or to work with an individual who possesses the required knowledge (for example, an entity employee, employee of a third-party managing the payment

terminals, or another employee of the QSAC).

For all instances where payment terminals are used in the cardholder data environment (CDE), the assessor is expected to include those payment terminals in the PCI DSS assessment. Where there are large numbers of payment terminals in the population being tested, the assessor may choose to select samples, as long as they are representative samples of the population that include all payment terminal types, locations, acquirers, and payment applications used.

The following activities can be performed to determine if cardholder data is being output in the clear from the payment terminal:

- Capture network traffic from the payment terminal during test transactions,

- Capture traffic from the payment terminal to any attached systems (for example, cash registers or point-of-sale systems).

In addition, the assessor should perform the following:

- Confirm that the payment terminals are included in the merchant's inventory of POI devices and that they are configured in accordance with vendor instructions, including that vendor default passwords are changed (Requirement 2).

- Confirm that any cardholder data stored by the merchant is rendered unreadable (Requirement 3).

- Confirm that transmitted account data is either rendered unreadable in the payment terminal or in merchant interfacing systems, prior to transmission (Requirement 4).

- Determine which applications are installed on the payment terminal.

- Confirm that the device and installed applications are still supported by the vendor(s), and that vendor-supplied security patches/updates have been applied (Requirement 6).

- Confirm that multi-factor authentication is in place for any access in to the CDE, including for remote access to the payment terminals and the TMS, as applicable (Requirement 8).

- Confirm that any payment devices used in card-present transactions and that capture payment card data via direct physical interaction with a payment card are protected from tampering and substitution (Requirement 9).

Where the payment terminals are managed by a third-party (for example, via a TMS), the assessor should also confirm with the third-party which of the above bullets they are responsible for, and which are the responsibility of the merchant.

Assessors should be familiar with PCI standards related to security of payment terminals, security of payment applications residing in the payment terminals, and payment solutions that include secure payment devices, cryptographic processes, and solution provider management processes, and have a good understanding of how compliance with these standards can facilitate compliance with applicable PCI DSS requirements. These PCI standards include PIN Transaction Security (PTS) Point-of-Interaction (POI), Secure Software, and Point-to-Point Encryption (P2PE). The lists of devices and solutions for these standards can be found at:

- Approved PIN Transaction Security (PTS) Devices
(https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpin_transaction_devices)

- Validated Payment Software
(https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpayment_software)

- Point-to-Point Encryption (P2PE) Solutions
(https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions)

It should be noted that while PCI DSS does not require the use of PTS-approved devices, some payment brands have requirements for the use of PTS-approved devices. Entities should contact their acquirer or the payment brands directly for information about any such requirements. Contact details for the payment brands can be found in FAQ #1142 How do I contact the payment card brands?.

Source: <https://www.pcisecuritystandards.org/faqs/1301/>