Payment Card Industry (PCI)

Software-based PIN Entry on COTS (SPoC)™

Technical FAQs for use with SPoC 1.1

Version 1.5

June 2020

Document Changes

Date	Version	Description
April 2018	1.0	Initial release.
May 2018	1.1	Added General Question Q4 and updated General Questions Q5 and Q13.
June 2018	1.2	Added General Question Q14, SPoC Security Requirement 3.6 Q1, and SPoC Security Requirement 5.1 Q1.
May 2019	1.3	Removed General Question Q8. Added General Question Q4, and updated General Question Q1, Q8, Q9 and Q11. Added SPoC Security Requirement 2.4 Q19, SPoC Test Requirement B2 Q25 and SPoC Test Requirement B5.2 Q26. Standardized terminology throughout the document. Minor grammatical updates.
December 2019	1.4	Updated Q1 to align with the definition of COTS in Contactless Payments on COTS™ (CPoC) Standard. Removed Q16 and clarified Q19. Added questions Q26 and Q27 to align with the publication of Contactless Payments on COTS™ Program Guide.
June 2020	1.5	Added General Question Q13. Added Q26 – Q32 to clarify SPoC Program Guide changes. Removed Q1, Q26 and Q27. Updated Q9, Q10, Q12 and Q24 to align with publication of PTS POI v6.0. Moved Q21 and Q22 under Security Requirement 3.1, and updated Q15, Q19 and Q20 to align with the security requirements and changes in the SPoC Program Guide. Renumbered questions and answers.

Table of Contents

SPoC Security Requirements: Frequently Asked Questions

These technical FAQs provide answers to questions about applying Payment Card Industry (PCI) Software-based PIN Entry on COTS™ (SPoC™) security requirements and corresponding testing requirements as addressed in the *PCI Software-based PIN Entry on COTS Security Requirements and PCI Software-based PIN Entry on COTS Magnetic Stripe Readers (MSR) Annex* ("SPoC Annex"). These FAQs clarify the application of *the Security Requirements and Test Requirements*. The FAQs are an integral part of those requirements and must be fully considered.

Updates: New or questions modified for clarity are in red.

General Questions

Q 1 Are there any restrictions to specific form factors for COTS devices and SCRPs that can be approved under the PCI SPoC Program?

A No. The SPoC requirements do not dictate a specific form factor for the COTS device, the SCRP, or the combination thereof for inclusion in an approved and validated SPoC solution.

Q 2 Are contactless transactions allowed under the SPoC Standard?

A Yes. The Standard supports both EMV-based and magnetic stripe mode contactless transactions.

Q 3 In the SPoC Test Requirements (TRs), where the attack-costing thresholds are required, there is no minimum number of thresholds. When will the attack-costing threshold values be added, and how should labs evaluate the relative requirements in the interim?

A The PCI SSC will work directly with the labs that are qualified to perform solution assessments. Each assessment will be used to contribute relative attack-costing information using actual solution validation data that will be factored into the development of appropriate attack-costing values. When sufficient data has been obtained, a revision to the *Test Requirements* that includes these values will be published.

Q 4 What is the difference between a "session" and a "transaction" within the context of the SPoC Standard?

A A "session" is established when the PIN CVM application initiates a payment. This session establishes secure channels with the Secure Card Reader – PIN (SCRP) and the back-end monitoring system. The session terminates when payment is complete or when any anomalous behavior is detected in the solution at any point during the payment process.

A "transaction" consists of the payment-processing messages created and exchanged with the back-end payment processing systems to gain authorization for a customer.

Q 5 Regarding "customer data" and "correlatable data," what is the scope of this data?

A The scope applies to data that either is entered into a PIN CVM application on a COTS device as part of the payment-transaction process or is sent from the back-end monitoring system to the COTS device. The scope is limited to data entered by the cardholder at the time of the transaction for purposes such as receipt transmission.

Q 6 What are the use cases for an SPoC solution?

A SPoC solutions are intended for use in a face-to-face environment where the merchant hands the COTS device to the customer. The customer then enters a PIN and returns the COTS device to the merchant.

SPoC solutions are not intended for environments where the device is part of a kiosk (semi-attended or self-checkout) or automated fuel dispenser. These unattended environments pose a greater risk of compromise and are not permitted under this Standard.

Q 7 What is the intent of use of an SPoC solution in an attended versus an unattended environment?

A The SPoC Standard is intended for merchant COTS devices in attended environments. Attended environments are when the merchant makes the COTS device available to the customer during a payment transaction (for example, when the merchant hands the COTS device to the customer). The customer enters a PIN and returns the COTS device to the merchant.

Merchant COTS devices in unattended environments pose a higher risk of compromise and are not permitted under this Standard. An unattended environment is one in which the merchant does not hand the COTS device to the customer; rather, the COTS device

is part of a kiosk (semi-attended or self-checkout) or a vending machine with no merchant involvement at the time of the transaction.

Q 8 Is SPoC synonymous with PIN on Glass?

A No. The SPoC Standard covers a software-based approach for accepting a PIN as the cardholder-verification method on a merchant-owned COTS device. The phrase "PIN on Glass" is often used to describe a variety of use cases where a PIN is entered on a glass-based capture mechanism (touch screen).

An SPoC solution includes a Secure Card Reader – PIN (SCRP), a PIN CVM application, the merchant's COTS device, and back-end monitoring/attestation systems. These elements work together to ensure the PIN, which has been accepted by a software application on the COTS device, is isolated within the COTS device from other sensitive account data. The back-end monitoring/attestation systems monitor the entire solution continuously for anomalous activity and to ensure that the solution has not deviated from the baseline due to tampering, rooting, or physical attacks. In other words, within an SPoC solution, the merchant-facing COTS device is only one element in the entire solution, whereas a Point of Interaction (POI) device is generally a single device.

There are numerous PCI PIN Transaction Security (PTS)-approved hardware-based POI devices that accept a PIN using a touch screen (PIN-on-Glass). These POI devices are built purposely for payment acceptance. Therefore, care must be taken when using the generic phrase "PIN-on-Glass." For example, a PTS-approved POI device that accepts PIN-on-Glass is very different from an SPoC solution that uses a merchant-facing COTS device to accept a PIN.

Q 9 [June 2020] Are magnetic stripe-based transactions allowed by the SPoC Standard?

A Yes. The Standard supports both EMV-based and magnetic-stripe mode-based contactless transactions. Solutions may optionally support magnetic-stripe readers that meet the security and testing requirements described in Payment Card Industry (PCI) Software-based PIN Entry on COTS Magnetic Stripe Readers Annex.

Q 10 [June 2020] Can merchants use their existing Secure Card Reader (SCR) to accept payments in an SPoC solution?

A Merchants can use PCI-approved SCRPs for chip-based transactions. Solutions may optionally support magnetic-stripe readers that meet the security and testing requirements described in Payment Card Industry (PCI) Software-based PIN Entry on

COTS Magnetic Stripe Readers Annex. The SPoC solution might include existing PCI PTS devices that are listed on the PCI SSC Approved Device website with an SCR Approval Class and support only contact magnetic stripe.

Q 11 Can merchants put together their own SPoC solution by choosing an SCRP, PIN CVM application, and back-end monitoring system?

A No. Only complete SPoC solutions will be approved and listed on the PCI SSC website.

Q 12 [June 2020] What constitutes an SPoC solution? Does the SPoC Standard cover separate elements or is it a single solution?

A The SCRP will have a separate listing because it is evaluated and listed as part of the PTS POI Standard. However, all SCRPs associated with an SPoC solution will be included as part of the SPoC solution evaluation and listed as part of that SPoC solution's acceptance. It is also possible that an MSR evaluated as part of SPoC solution might have a separate listing if it is evaluated and approved as an SCR as part of the PTS POI Standard.

An SPoC solution consists of PCI-approved SCRPs, an optional standalone MSR device that meets the security and testing requirements detailed in Payment Card Industry (PCI) Software-based PIN Entry on COTS Magnetic Stripe Readers Annex, a PIN CVM application, optional libraries or APIs to allow third parties to interface the SPoC solution, merchant COTS devices, and back-end systems. The SPoC solution will be listed on the PCI SSC website.

Q 13 [June 2020] Can a SPoC solution provider compose a SPoC solution from third-party elements?

A The SPoC Standard does not prohibit using a third-party service provider or elements developed by a third-party, as long as the SPoC solution in its entirety and *as a whole* solution is evaluated by the SPoC laboratory. Regardless of whether the SPoC solution, including a PIN CVM application, has been developed in-house or by a third-party, each SPoC solution provider is ultimately responsible for ensuring that all requirements are met and continue to be met throughout the solution's lifecycle.

Q 14 Is an SPoC solution eligible for a Point-to-Point Encryption (P2PE) solution approval?

A No. The SPoC Standard and the P2PE Standard are separate PCI SSC standards that are intended for different use cases.

SPoC Security Requirement 2.2

Q 15 **[June 2020] Is it possible to include an operating system (OS) version in the COTS system baseline of the full solution evaluation that is not supported by the OS vendor at the time of evaluation?**

A No. Security Requirement 2.2.2 requires that PIN CVM applications must be developed only for operating systems that are still supported by the operating system vendor. All SPoC solutions must operate only on supported platforms. The COTS system baseline must not include any version of a COTS OS that is not supported by the OS vendor at the time of the full evaluation.

Q 16 **Does Security Requirement 2.2.3 include OS level or other system applications?**

A No. This requirement is not intended for OS level or other system applications.

Q 17 **Security Requirement 2.2.5 states that where white-box cryptography is used, white-box keys must be unique for each PIN CVM application instance, and that the reliance upon and use of common white-box keys must be minimized after the secure-provisioning process. Does this requirement apply to all white-box keys as it relates to unique keys per PIN CVM application, or just those used for encrypting a PIN?**

A The intent of the requirement is that where white-box cryptography is used, each PIN CVM application instance must use unique keys for PIN encryption. White-box keys shall be updated when the PIN CVM application is updated, which is at least monthly in accordance with Security Requirement 2.5.6.

SPoC Security Requirement 2.4

Q 18 **Security Requirement 2.4.2 states that the PIN CVM application must detect sensor activation and polling of sensor data. Does this requirement apply to all COTS platforms?**

A The intent of the requirement is to protect the PIN entry process from manipulation or subversion. Because several attack vectors use COTS platform sensors and hardware for side-channel attacks, detecting when these sensors are activated or used (i.e., polling sensor data) by untrusted applications can reduce the risk of PIN compromise.

In cases where the COTS platform does not allow the runtime application to detect sensor status or sensor data pooling, the solution provider must verify and document

the COTS platform limitations, and explain how these limitations do not impact the security of the PIN entry process.

SPoC Security Requirement 3.1

Q 19 **[June 2020] If a version of the COTS OS initially listed in the solution system baseline reaches end-of-life such that it is no longer supported by the original OS vendor, does the SPoC Standard disallow transactions on affected COTS devices until the OS on those devices is updated to a supported OS?**

A Yes. Security Requirement 2.2.2 mandates that PIN CVM Applications are developed only for supported COTS platforms, and Security Requirement 3.1.6 mandates that COTS devices using unsupported OS are prohibited from processing transactions.

However, if an OS becomes unsupported after the initial evaluation, it can continue to be used until an annual checkpoint. If, as part of the annual checkpoint, the SPoC solution provider is able to provide evidence that the use of such a platform will not increase the risk of PIN exposure or subversion of the payment process, and the evidence is accepted by the laboratory, the unsupported platform may continue to be used. Such evidence must be evaluated and accepted during each annual checkpoint subsequent to any initial SPoC solution approval until the next full evaluation at which point the unsupported platform must be removed from the system baseline.

If such evidence is not provided or is not accepted by the laboratory, the SPoC Standard requires (Security Requirement 4.3.7) that merchants who are using the PIN CVM application on affected platforms be notified by the SPoC solution provider, and the listed SPoC solution will expire in accordance with the process outlined in the SPoC Program Guide.

Q 20 **[June 2020] If an OS vendor issues an update to a COTS OS that was initially listed in the solution system baseline, does the SPoC Standard disallow transactions on COTS devices using the updated OS until the updated SPoC solution is evaluated?**

A When an OS vendor releases a minor update to the COTS OS included in the SPoC solution system baseline, the solution provider may support the additional COTS OS version as long as it does not increase the risk of PIN exposure or subversion of the payment process, as determined by the SPoC solution provider risk assessment.

In order to support a new major version of COTS OS (e.g., 9.x, 10.x), the SPoC solution provider is required to engage a lab to perform a full or delta change evaluation, *as determined by the SPoC lab,* to ensure the new COTS OS version does not impact the

security of the SPoC solution. The SPoC solution listing will be updated to include the additional major version of the COTS OS.

SPoC Security Requirement 3.2

Q 21 **Security Requirement 3.2.13 states that for manual updates to the attestation system, any deployment changes to the production environment require dual control. Is dual control necessary for attestation system components associated with the PIN CVM application recognizing that such applications are signed by the OS app store and not under the control of the solution provider?**

A While it is acknowledged that the signing of a PIN CVM application made available from the OS app stores is not under the control of a PIN CVM application provider or solution provider, the packaging and release of the application to the OS app store is controlled by a solution provider. The solution provider can implement the required security controls on the processes of publishing the application to the OS app store.

SPoC Security Requirement 3.6

Q 22 **SPoC Security Requirements 3.6.1 and 5.1.2 state that if the back-end monitoring system resides in the Cardholder Data Environment (CDE), *PCI DSS*, Appendix A3 "Designated Entities Supplemental Validation (DESV)" will apply. Does an SPoC solution provider have to be fully compliant with DESV when submitting an SPoC solution for initial validation?**

A If the solution provider cannot meet DESV requirements at the point of an initial SPoC solution validation, the solution provider must provide an action plan to the SPoC lab, demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed for sufficiency.

SPoC Security Requirement 5.1

Q 23 **SPoC Security Requirements 3.6.1 and 5.1.2 state that if the back-end monitoring system resides in the CDE, *PCI DSS,* Appendix A3, "Designated Entities Supplemental Validation (DESV)" will apply. Does an SPoC solution provider have to be fully compliant with DESV when submitting an SPoC solution for initial validation?**

A If the solution provider cannot meet DESV requirements at the point of an initial SPoC solution validation, the solution provider must provide an action plan to the SPoC lab,

demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed for sufficiency.

SPoC Test Requirement B2

Q 24 Test Requirement TB2.5 calls for the disabling of on-device sensors during PIN entry. Does this requirement apply to all COTS platforms?

A The SPoC Standard does not require on-device sensors to be disabled during PIN entry. This requirement applies only if the solution provider implemented programmatic methods, manual processes (for example, prompting the end-user to disable a sensor), or a combination of both to disable on-device sensors.

SPoC Test Requirement B5.2

Q 25 [June 2020] Can an SPoC solution be associated with and communicate with multiple SCRPs or MSRs concurrently?

A Yes. An SPoC solution is permitted to support the use of multiple SCRPs or MSRs that meet the security and testing requirements described in the Payment Card Industry (PCI) Software-based PIN Entry on COTS Magnetic Stripe Readers Annex. The use of multiple SCRPs or MSRs in the SPoC solution is optional. The back-end monitoring system must be able to interact with each SCRP. All SCRPs supported by the SPoC solution must act in accordance with all roles and responsibilities as described in the *SPoC Security Requirements* and *SPoC Test Requirements*, including all interactions with other solution components.

Program Guide

Q 26 [June 2020] Can APIs (i.e., software libraries allowing third parties to interface with the SPoC solution) be validated and listed as part of a SPoC solution?

A Yes. In cases where the SPoC solution provider offers libraries or APIs to allow third parties to interface to the solution, evaluation and validation by a SPoC Lab is required as part of each SPoC solution in which such APIs are provided in order to validate that usage of the API can be done without violating or negatively impacting functionality or compliance with the *SPoC Standard.* Details regarding development, validation and listing of optional third-party APIs are specified throughout the SPoC Program Guide, particularly in Appendix D “SPoC Vendor-provided Libraries or APIs.”

Q 27 [June 2020] What is expected from a SPoC Lab when evaluating a SPoC solution that offers APIs or software libraries to allow third-party developers to interface with the SPoC solution?

A The evaluation and validation of the APIs (together with the SPoC user guidance document described and defined in the SPoC Program Guide) by a SPoC Lab are required as part of each SPoC solution in which such libraries or APIs are provided. It is expected the SPoC Lab validates that third-party usage of the libraries or API cannot negatively impact the functionality, security or compliance with the SPoC Standard.

It is expected that the SPoC Lab evaluates the SPoC user guidance, provided by the SPoC solution provider, which describes how the API is used to interface the SPoC solution.

While reporting on the API's validation, the SPoC Lab should follow the same process used for the reporting of PIN CVM applications. Whereas the SPoC user guidance is produced and distributed under the responsibility of the SPoC solution provider, the SPoC Lab must ensure that it contains the terms and conditions that address the secure usage of the APIs.

Q 28 [June 2020] When does SPoC Standard v1.1 become effective?

A SPoC Standard v1.1 (and SPoC Program Guide v1.2) is effective immediately upon publication and becomes mandatory for all new SPoC solution evaluations. In process evaluations can be completed using SPoC Standard v1.0. PCI SSC must be notified in writing by each SPoC Lab of the specific SPoC solution they have under evaluation. The final laboratory evaluation reports must be received by PCI no later than sixty-day after the SPoC Standard and the associated SPoC Program Guide publication date.

Existing SPoC solutions are not affected and remain validated per the date on the listing on the PCI SSC website. However, SPoC solution provider may choose to engage a SPoC Lab to perform a delta or a full evaluation, as determined by the SPoC lab, to update a listed SPoC solution on the PCI SSC website.

Q 29 [June 2020] How does a minor update to the SPoC Standard affect the expiry date of listed SPoC solutions?

A Minor updates of the SPoC Standard (e.g., from version 1.0 to version 1.1) do not change the expiry dates for listed SPoC solutions; they remain as three years from the initial acceptance/listing date shown on the PCI SSC website.

Q 30 [June 2020] Can a Delta change be submitted to update a listed SPoC solution between minor versions of the SPoC Standard?

A Yes, the change is submitted to a SPoC Lab and it is up to the SPoC Lab to determine whether the extent of the change(s) can be validated via delta evaluation. If the changes are extensive or highly impactful to the SPoC security requirements, then the SPoC Lab may determine that a full evaluation is required. Note that all changes must be accompanied by current SPoC Attestation of Validation (AOV), and in accordance with SPoC Program Guide.

Please note that if a delta change is performed to update a listed SPoC solution between minor versions of SPoC Standard (e.g., from version 1.0 to version 1.1), the re-evaluation/expiry date does not change.

Q 31 [June 2020] Can an Administrative change be submitted to transition a listed SPoC solution from SPoC Standard?

A No, Administrative changes cannot be used to transition between versions of the SPoC Standard - a full or delta change evaluation, *as determined by the SPoC lab,* must be performed.

Q 32 [June 2020] What happened to "Designated Change" in the SPoC Program Guide?

A Designated changes have been incorporated into the delta change process in SPoC Program Guide version 1.2 to help simplify the change and listing process.