Payment Card Industry (PCI)

Software-based PIN Entry on COTS (SPoC™)

Technical FAQs for use with SPoC Standard Version 1

December 2019

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.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

Table of Contents

© 2019 PCI Security Standards Council, LLC. All rights reserved.

SPoC Security Requirements: Frequently Asked Questions

These technical FAQs provide answers to questions regarding the application of 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 **[December 2019] What is a COTS Device?**

A A commercial-off-the-shelf (COTS) Device is a mobile device (smartphone, tablet, or wearable) that is designed for mass-market distribution.

Q 2 **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 3 **Are contactless transactions allowed under the SPoC Standard?**

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

Q 4 **In the SPoC Test Requirements (TRs), where the attack-costing thresholds are required, there is no minimum. 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.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

Q 5 Please explain 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 with 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 6 Regarding "Customer Data" and "Correlatable Data", what is the scope of this data?

A The scope applies to data that is entered into a PIN CVM Application on a COTS Device as part of the payment transaction process, or that 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 7 What are the use cases for a 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 hands the COTS Device back 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 8 What is the intent of use of a 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 COTS Device is made available to the customer by the merchant during a payment transaction. For example, the merchant hands the COTS Device to the customer. The customer enters a PIN and hands the COTS Device back 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 COTS Device is not handed to the customer by the merchant, but rather, the COTS

© 2019 PCI Security Standards Council, LLC. All rights reserved.

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 9 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; that is, a touch screen.

A SPoC Solution includes an SCRP (Secure Card Reader – PIN), 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 continuously monitor the entire Solution for anomalous activity and to ensure The Solution has not deviated from the baseline because of tampering, rooting, or physical attacks. In other words, within a 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 a SPoC Solution that uses a merchant-facing COTS Device to accept a PIN.

Q 10 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. It also optionally supports the contact magnetic stripe reads. Contact magnetic stripe reads must only occur using a separate Magnetic Stripe Reader (MSR) Device that complies with the *SPoC Annex,* and the PIN CVM Application must prevent the entry of the PIN.

Q 11 Can a merchant use their existing Secure Card Reader (SCR) to accept payments in a SPoC Solution?

A Merchants can use PCI-approved SCRPs for chip-based transactions. Contact magnetic stripe reads must only occur using a separate MSR Device that complies with the *SPoC Annex*, which might include existing approved PCI PTS SCRs.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

Q 12 Can a merchant 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 13 What constitutes a 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 a 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 a Secure Card Reader (SCR) as part of the PTS POI Standard.

A SPoC Solution consists of PCI-approved SCRPs, an optional MSR that complies with the *SPoC Annex*, a PIN CVM Application, merchant COTS Devices, and Back-end Monitoring/Attestation Systems. The SPoC Solution will be listed on the PCI SSC Website with the individual elements.

Q 14 Is a 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 Is it possible to include an operating system (OS) version in the COTS System Baseline of the initial 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 new Solutions must operate only on supported platforms. The initial 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 initial 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.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

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 2.2.4 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 3.2

Q 19 **[December 2019] 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.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

SPoC Security Requirement 3.6

Q 20 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), then *PCI DSS*, Appendix A3 "Designated Entities Supplemental Validation (DESV)" will apply. Does a SPoC Solution Provider have to be fully compliant with DESV when submitting a 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 4.3

Q 21 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 No. If an OS version has been assessed and is listed as part of the COTS System Baseline, (TR C1), and then the OS vendor ends support for that OS version, then per Security Requirement 4.3.7 and TR C4, the Solution Provider must provide evidence that the acceptance and use of such a platform that accepts PIN entry will not increase the risk of PIN exposure or subversion of the payment process beyond the use of devices that are supported by security patches as a part of the annual update of the risk-assessment policy and procedure. If such evidence is accepted at the time of the review by the PCI SSC after review of the laboratory evaluation report, then the unsupported platform may continue to be used. Such evidence must be "re-accepted" during each annual Solution evaluation cycle subsequent to any initial Solution approval.

If such evidence is not provided or is not accepted by the PCI SSC, the SPoC Standard requires that merchants who are using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants will be migrated to supported platforms. (SR 4.3.7).

© 2019 PCI Security Standards Council, LLC. All rights reserved.

Q 22 If an OS vender 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 OS is evaluated?

A No. If an updated version of an OS that is already listed in the COTS System Baseline is made available by the original OS vendor, then the Solution Provider may add that version to the COTS System Baseline and must provide evidence that the acceptance and use of such a platform as a part of the annual update of the risk-assessment policy and procedure. If such evidence is accepted at time of the review by PCI SSC after review of the laboratory evaluation report, then the new platform may continue to be used.

If such evidence is not provided or is not accepted by the PCI SSC, the SPoC Standard requires that merchants using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants will be migrated to supported platforms. (SR 4.3.7).

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 Cardholder Data Environment, then *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 disabling on-device sensors 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.

© 2019 PCI Security Standards Council, LLC. All rights reserved.

SPoC Test Requirement B5.2

Q 25 Can a SPoC Solution be associated with and communicate with multiple SCRPs, or MSRs concurrently?

A Yes. A SPoC Solution is permitted to support the use of multiple SCRPs or MSRs (per the *SpoC 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 detailed in the *SPoC Security Requirements* and *SPoC Test Requirements*, including all interactions with other Solution components.

Program Guide

Q 26 [December 2019] What is required by SPoC Solution Providers and SPoC Labs regarding the note in section 4.1 Required Vendor Materials of the SPoC Program Guide?

A In cases where a Vendor or SPoC Solution/SPoC Element cannot meet a specific requirement as stated, the Vendor must clearly explain why the requirement cannot be met as stated. The Vendor must also provide evidence to clearly show how the corresponding security objective is still being met or exceeded, and that the alternative controls or methods are employed to provide equivalent or greater assurance to that provided by the methods described in the requirement. Vendors should work with their SPoC Lab to determine the evidence required to satisfy a specific security objective or associated requirement. The SPoC Lab is responsible for evaluation of the alternative controls or methods, and must include in the evaluation report a description of the testing they performed, justification of how the testing confirms the security objective has been met or exceeded and a statement confirming that the security objective has been met or exceeded.

Q 27 [December 2019] What is required by SPoC Solution Providers regarding the note in the SPoC Program Guide, section 2.1.4 Back-end Monitoring Environment Providers on meeting DESV requirement?

A If PAN or SAD is present in the Monitoring/Attestation System's environment, then that environment must be validated by a QSA as being PCI DSS compliant including DESV. If the SPoC Solution Provider cannot meet DESV requirements at the point of an initial SPoC Solution validation, the Solution Provider must provide the SPoC Lab an action plan demonstrating that work is in progress for requirements to be met by the first annual checkpoint. The action plan will be reviewed by the SPoC Lab for sufficiency

© 2019 PCI Security Standards Council, LLC. All rights reserved.

and submitted to PCI SSC as part of the Solution Evaluation process. Failure to meet DESV requirements by the first annual checkpoint may result in revocation of the SPoC Solution from PCI SSC's listing of validated SPoC Solutions.

© 2019 PCI Security Standards Council, LLC. All rights reserved.