Payment Card Industry (PCI)

Software-based PIN Entry on COTS Security Requirements

Technical FAQs for use with Version 1

April 2018

Table of Contents

SPoC Security Requirements: Frequently Asked Questions

These technical FAQs provide answers to questions regarding the application of PCI's (Payment Card Industry) SPoC security requirements and corresponding testing requirements as addressed in the *PCI Software-based PIN Entry on COTS Security Requirements*. These FAQs provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered.

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

General Questions

Q 1 Are non-EMV based contactless transactions allowed under the Software-based PIN Entry on COTS (SPoC) standard?

A *The Standard has been developed for chip-based transactions which support dynamic transaction data. The only method explicitly excluded is contact magnetic stripe because it has static transaction data. Contact magnetic stripe read capabilities are not permitted within SCRPs and contact magnetic stripe transactions are not permitted to be accepted or processed by SPoC solutions.*

Q 2 In the SPOC TRs, where the attack costing thresholds are required, there is no minimum to be met. 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 be working 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 factor in to the development of appropriate attack costing values. Once sufficient data has been obtained a revision to the Test Requirements will be published with the inclusion of these values.*

Q 3 Please explain the difference between a "session" and a "transaction" within the context of the Software-based PIN Entry on COTS (SPoC) standard?

A *A "session" is established when the PIN CVM Application is used to initiate a payment. This session includes establishing secure channels with the SCRP and with the back-end monitoring system. The session is terminated once the payment has completed or if 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 sent to and from the back-end payment processing systems to gain authorization for a customer.

Q 4 A "session" is established when the PIN CVM Application is used to initiate a payment. This session includes establishing secure channels with the SCRP and with the back-end monitoring system. The session is terminated once the payment has completed or if any anomalous behavior is detected in The Solution at any point during the payment process.

A *The intent of the SPoC standard is for merchant COTS devices in attended environments. Attended environments apply when the COTS device is made available to the customer by the merchant during a payment transaction. Merchant COTS devices in unattended environments pose a higher risk of compromise and are not permitted under this standard. Unattended environments mean the COTS device is not in the merchant's physical possession at the time of the payment transaction (i.e. part of a kiosk, part of a vending machine).*

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

Q 5 Is Software-based PIN Entry on COTS (SPoC) synonymous with PIN on Glass?

A *No. The SPoC Standard covers a software-based approach for accepting PIN as the cardholder verification method on a merchant owned COTS device. The phrase "PIN on Glass" is often used generically regarding a variety of use cases, with the commonality simply being entering a PIN value on to a glass-based capture mechanism (i.e., a touch screen) on a variety of device types.*

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

There are numerous PCI PTS approved hardware-based point of interaction (POI) devices for acceptance of PIN using a touch screen (i.e., "PIN on Glass"). These POI devices are purposely built for payment acceptance. Therefore, care must be taken when using the generic phrase "PIN on Glass", as, 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 PIN.

Q 6 Are magnetic stripe-based transactions allowed by the Software-based PIN Entry on COTS Standard?

A *No. Contact magnetic stripe readers (MSRs) are not allowed in a SPoC Solution. Only a Secure Card Reader – PIN, or SCRP, is allowed to be used with a PIN CVM application as part of a solution. The SCRP is a new type of Secure Card Reader (SCR) approval class within the PTS POI Standard that disallows any contact MSR capabilities. Only EMV contact and contactless transactions are allowed in the SPoC Standard. Simply disabling any contact MSR capabilities in the SCRP firmware or via the PIN CVM Application is not allowed – the SCRP shall not incorporate a contact MSR.*

Q 7 Can a merchant use the same PIN CVM Application to accept both EMV contact and contactless transactions and magnetic-stripe based transactions?

A *No. Contact magnetic-stripe read transactions are not allowed with the use of a PIN CVM Application that is part of a SPoC Solution nor is it permitted as part of the SCRP. Other accommodations or solutions a merchant may use to support MSR read transactions are out of scope of the SPoC standard.*

Q 8 Can a merchant use their existing SCR to accept payments in a SPoC Solution?

A *No. Merchants may only use the PTS approved and listed SCRP for use with the SPoC Solution. See FAQ Q7 (above) for more information.*

Q 9 Can a merchant put together their own SPoC solution by choosing a 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 10 What constitutes a SPoC Solution? Does the SPOC standard cover separate components or is it a single solution?

A *Only the Secure Card Reader - PIN (SCRP) will have a separate listing as they are 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 evaluation of a SPoC Solution and listed as part of that SPoC Solution's approval.*

A SPoC Solution consists of a PCI-approved SCRP(s), a PIN CVM Application, a merchant COTS device(s) and back-end monitoring and attestation systems. The SPoC Solution will be listed on the PCI website along with the individual elements. There will not be any individual SPoC component listings (except for the SCRP as detailed above) at this time.

Q 11 What is a COTS device?

A *A commercial-off-the-shelf (COTS) device is a mobile device (i.e. smartphone, tablet or wearable) that is designed for mass-market distribution and is not designed specifically for payment processing.*

SPoC Security Requirement 2.2

Q 1 Is it possible to include in the COTS System Baseline of the initial evaluation of a Solution, a version of an operating system which 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 which are still supported by the operating system vendor. All new solutions need to ensure that they operate only on supported platforms. The initial COTS System Baseline must not include any version of a COTS OS which is not supported by the OS vendor at the time of the initial evaluation.*

Q 2 Security Requirement 2.2.3 states that the PIN CVM Application must only support platforms that provide for a "trusted boot" mechanism that validates the operating systems authenticity. What are the implications of this requirement recognizing that for certain Android versions (e.g. Android 4), some OEMs did not support sufficient hardware capabilities to implement secure boot mechanism and implications associated with scenarios where a clear designation of trust boot support of "yes or no" can be determined?

A *For such scenarios where such Android versions and OEM implementation are supported in the COTS system baseline, the lab must detail these conditions and detail what additional controls are in place to mitigate the risks and demonstrate that such supported COTS system are not representative of a significant portion of the supported customer base.*

Q 3 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 4 **Security Requirement 2.2.5 states that, where white-box cryptography is used, white-box keys must be unique per PIN CVM Application instance and that the reliance and use of common white-box keys must be minimized after the secure provisioning process. Does this requirement as it relates to unique keys per PIN CVM Application apply to all white-box keys or just those used for encrypting PIN?**

A *The intent of the requirement is that where white-box cryptography is used, the PIN CVM Application uses unique keys for PIN encryption. White-box keys shall be updated at time of Application update which must occur at least monthly in accordance with Security Requirement 2.5.6.*

SPoC Security Requirement 3.2

Q 1 **Security Requirement 3.2.13 states that for manual updates to the attestation system, any deployment changes to the production environment must require dual control. Is dual control necessary for attestation system components associated with the PIN CVM Application recognizing such applications are signed by the OS App Store and not under the control of the Solution Provider?**

A *It is acknowledged the signing of a PIN CVM Application made available from the OS App Store(s) is not under the control of a PIN CVM Application provider or overall Solution Provider and dual control cannot be enforced for such PIN CVM Applications by a Solution Provider.*

SPoC Security Requirement 4.3

Q 1 **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, is it the intent of the SPOC standard to disallow transactions on affected COTS devices until the OS on those devices is updated to a supported OS?**

A *No. If a particular OS version has been assessed and is listed as included in the COTS System Baseline, (TR C1) and then that particular instance becomes no longer supported by the OS vendor, then as per Security Requirement 4.3.7 and TR C4, the Solution provider must provide justifications why the acceptance and use of such a platform for accepting PIN entry does not increase the risk of PIN exposure, or subversion of the payment process, beyond use of devices which are supported by security patches as a part of the annual update of the risk-assessment policy and procedure. If such justifications are accepted at time of the review by PCI Council after review of the laboratory evaluation report then the unsupported platform may continue to be used. Such justifications will need to be "re-justified" during each annual Solution evaluation cycle subsequent to any initial Solution approval.*

If such justifications are not provided or are not accepted by the PCI Council, the SPoC standard requires that merchants using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants are migrated to supported platforms. (SR 4.3.7).

Q 2 **If a new updated version of a COTS OS initially listed in the Solution System Baseline is made available by the original OS vendor, is it the intent of the SPOC standard to disallow transactions on affected COTS devices until the OS on those devices is evaluated?**

A *No. If a new updated version of an OS which 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 justifications for the acceptance and use of such a platform as a part of the annual update of the risk-assessment policy and procedure. If such justifications are accepted at time of the review by PCI Council after review of the laboratory evaluation report then the new platform may continue to be used.*

If such justifications are not provided or are not accepted by the PCI Council, the SPoC standard requires that merchants using the PIN CVM Application on affected platforms be notified by the Solution Provider and that the merchants are migrated to supported platforms. (SR 4.3.7).