Payment Card Industry (PCI)
Software-based PIN Entry on COTS (SPoC)™

Technical FAQs for use with SPoC 1.1

Version 1.8

December 2021

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.
July 2020	1.6	Added Q28-Q30 to clarify reuse of testing results. Added Q36 to clarify the intent of the annual checkpoint.
May 2021	1.7	Added Q26 and 26 to clarify when SPoC Unsupported OS Annex apply and usage of "objective-based" approach. Added Q30 to clarify API or software library integration options can be supported by SPoC solution. Added Q40 to clarify the frequency the required frequency of PCI PIN Assessment. Updated Q28 to clarify the API or software libraries implementations that can supported by SPoC solution. Updated Q15, Q19 and Q39 to align with the publication of SPoC Unsupported OS Annex. Renumbered questions and answers.

Date	Version	Description
December 2021	1.8	Added Q15 to clarify the term "assessed RNG".
		Added Q16 to clarify when the usages of TDES is allowed.
		Updated Q19 to clarify the scope of WBC keys.
		Added Q28 to clarify the expected logical and physical testing of COTS devices.
		Added Q29 to clarify a use-case where back-end attestation and monitoring systems are hosted in multiple environments or hosted by multiple entities.
		Added Q30 to clarify the onsite assessment requirements.
		Added Q46 to describe the process to delay SPoC solution listing.

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   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   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   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 Can an SPoC solution provider compose an 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 1.2

Q 15 [December 2021] What is an assessed or validated RNG, and what is expected from a SPoC lab when evaluating a SPoC solution?

A There are two types of RNGs: Deterministic Random Number Generator (DRNG) and Non-deterministic Random Number Generator (NRNG). Typically, DRNG uses an initial seed value from an NRNG to generate deterministic random values.

The entropy used for an NRNG must meet the requirements in *NIST SP 800-90B* or *§8 of ISO/IEC 18031 Information technology — Security techniques — Random bit generation*.

Many COTS platforms implement their own RNG functions, however not all meet the security requirements as noted in SPoC standard. The implementation of DRNG for security services must meet the following criteria:

- Implements a well-known standard, such as those specified in *NIST SP800-90a or §9 of ISO/IEC 18031 Information technology — Security techniques — Random bit generation*.

- Properly seeded (per SPoC security requirement 1.2.2 and 1.2.5), and
- Implementation is tested for fitness of purpose using industry-recognized test suites, such as NIST SP800-22 or AIS 31.

The SPoC laboratory is required to perform a review of all sensitive services (such as source code review) to confirm that the RNG functions used by the solution are assessed RNGs, and that the RNG functions are used as intended. The SPoC lab must provide a testing methodology and applicable testing evidence to justify their conclusions.

SPoC Security Requirement 1.3

Q 16 **[December 2021] Can TDES be used in an SPoC solution?**

A All security services provided by the solution must use only those algorithms and minimum key lengths as outlined in Appendix C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms. The only exception is customer PINs transmitted from the SCRP to the PCI PIN-compliant back-end processing environment which may be encrypted using TDES.

SPoC Security Requirement 2.2

Q 17 **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 Yes. Although Security Requirement 2.2.2 requires that PIN CVM applications must be developed only for operating systems that are still supported by the OS vendor, PCI Security Standards Council has published an optional *SPoC Unsupported OS Annex* which outlines additional security controls to allow SPoC solution provider to include COTS devices with unsupported operating systems in the COTS system baseline if the requirements in the Annex are met. Otherwise, SPoC solutions must operate only on supported platforms, and 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 18 **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 19 **[December 2021]** **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 protecting keys associated with a PIN encryption?**

A The intent of the requirement is that where white-box cryptography is used to protect sensitive services and sensitive data, each PIN CVM application instance must use unique white-box keys. This includes white-box keys used to protect PIN encryption keys, cryptographic material used to establish secure channels, or secret keys used for authentication of PIN CVM application instance.

SPoC Security Requirement 2.4

Q 20 **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 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 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 by the OS vendor after the initial evaluation, it can continue to be used until an annual checkpoint. As part of annual checkpoint, the SPoC lab need to perform additional testing to confirm security objectives outlined in the SPoC Unsupported OS Annex are met, and that the use of such a platform will not increase PIN exposure or subversion of the payment process.

If evaluation SPoC Unsupported OS Annex is not performed or the implemented security controls and processes are 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 22 **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 23 **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 24 **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 25 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 26 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 27 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.

SPoC Test Requirement C2

Q 28 **[December 2021] What is expected from SPoC labs regarding physical and logical testing of the COTS devices?**

A While there is no expectation to perform physical or logical testing of a COTS device itself, SPoC labs must confirm whether COTS platforms included in the COTS system baseline have known characteristics, such as physical test, debug, or in-circuit emulation features. For example, some Android mobile devices have an NFC logging service, which is intended to be used for debugging purposes. Other COTS devices may produce unique responses based on the COTS platform chipset when used with Android Debug Bridge (ADB), which can be exploited when physically connected to the mobile device.

The SPoC lab is expected to have the expertise and knowledge of such features. Depending on the COTS platforms that the SPoC solution supports, the SPoC lab should use its expertise and knowledge to consider what attack methods should be performed when evaluating the solution, and how their features affect attack costing.

SPoC Test Requirement E1

Q 29 **[December 2021] Can back-end attestation and monitoring systems be hosted in multiple environments by more than one entity?**

A Yes. For each environment that is hosting attestation and monitoring systems, the SPoC solution provider is expected to do either: 1) Provide an Attestation of Compliance (AOC) that has been completed and signed within the previous 12 months demonstrating that the environment complies with the *PCI DSS*, including the additional controls outlined in *PCI DSS* Appendix A3 DESV, or; 2) Demonstrate compliance with the logical and physical security requirements defined in *SPoC Security Requirements*, Appendix A Monitoring and Attestation Environment Basic Protections.

Q 30 **[December 2021] Does assessment of back-end systems require a physical onsite presence of the lab personnel?**

A SPoC solution back-end environments include back-end monitoring and attestation environment, and back-end payment processing environment. The back-end payment processing environment must be compliant with PCI Data Security Standard and PCI PIN Security Requirements, as applicable, and whether remote assessment methods are acceptable is defined by the compliance-accepting entities.

When the back-end attestation and monitoring environment is included in scope of the PCI DSS assessment, it must comply with additional requirements outlined in *PCI DSS Appendix A3 DESV*, and whether physical onsite presence is required continues to be determined by the compliance-accepting entities.

In cases where the back-end attestation and monitoring environment is not subject to PCI DSS, it must be assessed and validated to the security requirements outlined in *SPoC Appendix A*. The requirements in *SPoC Appendix A* are intended to provide comparable security controls to *PCI DSS Appendix A3 DESV*, therefore it is expected that the PCI-recognized lab personnel are physically onsite for each assessment of the environment. While the intent is that assessments of physical environments are performed onsite, the use of remote assessment methods may be a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. PCI SSC has developed and published a framework of remote assessment methods that may be used when an onsite assessment cannot be performed. The PCI SSC Remote Assessment Guidelines and Procedures document can be found in the PCI SSC Document Library.

SPoC Unsupported OS Annex

Q 31   When does the SPoC Unsupported OS Annex apply?

A   The security objectives outlined in the SPoC Unsupported OS Annex are optional, and the security controls are required only for solutions that include unsupported OSes in their COTS system baseline. For example, a solution provider may decide to include an unsupported COTS OS in the COTS system baseline of its initial evaluation, or to retain a previously supported COTS OS that became unsupported during the annual checkpoint.

Q 32   Can an "objective-based" approach be used for security requirements and test requirements in the SPoC Standard?

A   The objective-based approach is intended only for evaluating security controls and processes implemented by an SPoC solution provider, as outlined in the SPoC Unsupported OS Annex, to protect the integrity and confidentiality of a PIN entered on COTS devices running an unsupported operating system.

Program Guide

Q 33   Can APIs (i.e., software libraries allowing third parties to interface with the SPoC solution) be validated and listed as part of an 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.* Whether an implementation of an API or a software library can be supported by the SPoC Program depends largely on whether an SPoC lab can validate the exposed API or a library to SPoC Security Requirements and SPoC Test Requirements.

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 34 **What is expected from an SPoC lab when evaluating an 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 an 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 35 **What API or software library implementation options can be supported by the SPoC solution?**

A Whether an implementation of an API or a software library can be supported by the SPoC Program depends largely on whether an SPoC lab can validate the exposed API or a library to SPoC Security Requirements and SPoC Test Requirements.

There are several ways an SPoC solution provider can allow third-party software developers to interface with an SPoC solution, including exposing back-end API, ability to invoke functionality of a PIN CVM application on the COTS device, and distributing a library or source code. Often, these factors are implementation-specific and platform-specific. For example, on the Android operating system, a PIN CVM application or an additional mobile application working with the SPoC solution could expose an *Intent*[1] that would allow another third-party application to start an *Activity*[2] to handle interaction with the PCI PTS SCRP device and PIN entry on the COTS device. In this example, the SPoC lab validates whether the exposed functionality, operational processes, distribution methods, etc., do not negatively impact the security of the solution or

---

[1] https://developer.android.com/reference/android/content/Intent
[2] https://developer.android.com/reference/android/app/Activity

compliance with the SPoC Standard. In such case, the API or software library is eligible for inclusion in the SPoC solution listing on the PCI SSC website.

A solution can include APIs or libraries that cannot be fully validated by an SPoC Lab. Therefore, some implementation options may not be supported by the SPoC Program. For example, if an API or software library is developed by the SPoC solution provider but signed by a third-party software vendor, or distributed as a library or a source code, the SPoC lab would not be able to perform several test requirements to confirm whether processes such as the signing of the application, secure distribution, etc. are met. Moreover, when certain SPoC functionality is distributed as a software library or source code, the SPoC solution provider has little to no control over how the library is compiled into the third-party payment application, how the functionality is invoked, and how the third-party payment application is distributed to the end-users. In such cases, the API would not be fully validated for listing as part of the SPoC solution on the PCI SSC website.

Q 36 Can an SPoC lab reference an approval from another PCI SSC standard, such as PCI Contactless Payments on COTS (CPoC™), to meet objectives in the SPoC Standard without performing the required testing?

A No. With the exception of references to the PCI DSS AOC for back-end environments, each SPoC evaluation report must demonstrate that the SPoC solution under review was evaluated and meets the security and the test requirements of the *SPoC Standard*.

Q 37 Can testing results be reused from one evaluation to another of the same vendor?

A Yes. Testing from one SPoC evaluation can be reused in another SPoC evaluation from the same solution provider. This situation occurs commonly when two SPoC solutions with similar characteristics are evaluated by the same laboratory in parallel or in close succession. The reused data must be current (less than 12 months old) and must have been completed under the same major version of the *SPoC Standard*. The tester shall:

- Justify how the two solutions are similar. The tester must confirm that the differences in SPoC device hardware, PTS SCRP devices supported by the SPoC solution, SPoC solution software, and configuration do not impact the testing results.

- Clearly indicate that the test is reused data and meets the applicable test requirements.

- Provide evidence of testing, and that the testing is valid for the SPoC solution and the test requirement under review.

Q 38 Can an SPoC lab rely on testing performed by a different SPoC lab without further testing or validation?

A If any element of an SPoC solution was evaluated by an entity other than the SPoC lab performing the evaluation under review, the evaluating SPoC lab must have access to all associated reports and supporting evidence. If those reports are not available for any

reason, the evaluating SPoC lab must determine the additional work required to properly evaluate and attest to the solution's compliance with the SPoC security and test requirements.

If the evaluating SPoC lab is unable to rely on the information, whether available or not, and the SPoC lab is unable to perform the additional work required to achieve such reliance, PCI SSC will not accept the report.

In all cases, PCI SSC may reject the evaluation report if it does not contain adequate information to substantiate the conclusions or compliance with the *SPoC Standard*.

Q 39   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 calendar days 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 an 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 40   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 41   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 an 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, 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 42 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 43 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.

Q 44 What testing and reporting are expected to be performed by SPoC lab as part of an annual checkpoint?

A The annual checkpoint confirms that the SPoC solution continues to meet the security and test requirements of the *SPoC Standard*. The amount of testing that is required will vary. At a minimum, however, the SPoC lab must confirm that:

- Back-end environments remain compliant with PCI DSS or SPoC Appendix A,

- Back-end Processing Environment remains compliant with PCI PIN,

- The SCRP devices supported by the SPoC solution are listed on the PCI SSC Approved Device website (i.e., have not been expired), and

- All operating processes (risk assessment, vulnerability management, change management, and so on) are being followed.

The SPoC lab may need to perform additional testing, depending on the extent to which the SPoC solution has changed. For example, if an OS vendor no longer supports an OS that was included in the SPoC solution system baseline, the SPoC lab must verify that the SPoC solution provider has updated its system baseline and is actively working with its merchants to migrate them to a supported version of the OS. If SPoC solution providers want to continue to allow COTS devices with an unsupported OS, the SPoC lab must perform additional testing to confirm that security objectives described in the SPoC Unsupported OS Annex are met.

Moreover, as part of the annual checkpoint, the SPoC lab must consider new risks, vulnerabilities/CVE, and attack techniques (such as new rooting or jailbreaking) and attempt to apply those techniques to ensure that SPoC solution attestation and monitoring systems are able to detect and respond to those attacks.

Each annual checkpoint submission must be made by an SPoC lab and include the submission of an updated *SPoC solution AOV* to PCI SSC after the lab reviews all changes that occurred since the last full evaluation or last annual checkpoint (whichever is more recent). The SPoC lab must also consider any applicable changes that occurred during the previous 12-month period. In addition, the SPoC lab must determine the level of testing needed to ensure that the solution remains compliant with

all applicable SPoC security and test requirements. For more information, see the *SPoC Program Guide v1.2*, section 5.1 "Annual Checkpoints."

Q 45 How often must an SPoC Solution's Back-end Processing Environment undergo a PCI PIN Assessment?

A The SPoC Solution's Back-end Processing Environment must be assessed and validated by a PCI-qualified PIN Assessor (QPA) annually (i.e., at least every 12 months). Evidence of the PIN Assessment is verified by the SPoC lab during the annual checkup.

Q 46 [December 2021] Can a SPoC Solution Listing be delayed at a vendor's request?

A Yes, solution providers may choose to delay listing a newly approved SPoC solution for up to a maximum of six calendar months. Written notification to PCI SSC must be submitted by the SPoC solution provider, through the SPoC laboratory performing the evaluation, along with the completed SPoC Evaluation Report. In addition, the SPoC lab must make a notation in the applicable field of the Lab Report Portal when submitting the evaluation report, indicating the period of time the listing should be withheld.

Delaying listing does not extend the solution's validation period; annual checkpoint and solution reevaluation dates will be based on the date of the countersigned AOV, not the date on which the solution is listed. A solution is not considered to be a validated SPoC solution until it is listed on the PCI SSC website.