Payment Card Industry (PCI)

# Software-based PIN Entry on COTS (SPoC)

## Program Guide

**Version 1.0**

April 2018

# Document Changes

| Date | Version | Description |
|---|---|---|
| April 2018 | 1.0 | Initial Release of the *PCI Software-based PIN Entry on COTS (SPoC) Program Guide* |

# Table of Contents

# 1 Introduction

This Program Guide provides an overview of the PCI SSC Software-based PIN Entry on Commercial off-the-shelf (COTS) Standard ("SPoC") program operated and managed by the PCI Security Standards Council, LLC and should be read in conjunction with the documents referenced in Section 1.2, "Related Publications," below. This document applies primarily to Vendors developing and seeking validation of their SPoC Solutions and SPoC Labs. Capitalized terms used but not otherwise defined within this document have the meanings defined in or pursuant to Appendix G of this Program Guide.

This Program Guide describes the following:

- Software-based PIN Entry on COTS (SPoC) Solution Overview (Section 1.1)
- Roles and Responsibilities (Section 2)
- Preparation for the Evaluation (Section 3)
- Evaluation and Reporting Process (Section 4)
- Maintaining a Validated SPoC Solution Listing (Section 5)
- Reporting Considerations (Section 6)
- Assessor Quality Management Program (Section 6.3)

## 1.1 Software-based PIN Entry on COTS (SPoC) Solution Overview

Each of the following elements of a Software-based PIN Entry on COTS Solution ("SPoC Solution" or "Solution") requires evaluation and validation for use within the Solution. Additionally, the overall SPoC Solution must be evaluated and successfully validated and submitted to PCI SSC by a SPoC Lab prior to Acceptance and listing by PCI SSC.

- **Secure Card Reader – PIN (SCRP) devices:** Evaluated by a PCI-recognized PTS Laboratory (PTS Lab) per the *PCI PTS POI Modular Security Requirements* (version 5.1 or later) and separately listed on the list of Approved PTS Devices on the Website.
- **PIN Cardholder Verification Method (CVM) Application:** Evaluated by a PCI-recognized SPoC Laboratory (SPoC Lab) per the *SPoC Security Requirements* and *SPoC Testing Requirements* as part of their overall SPoC Solution Evaluation. PIN CVM Applications are listed only as part of the SPoC Solutions in which they have been validated for use under the SPoC Program—i.e., PIN CVM Applications are not separately listed on the Website.
- **Monitoring/Attestation System:** Evaluated by a SPoC Lab per the *SPoC Security Requirements* and *SPoC Testing Requirements* as part of their overall SPoC Solution Evaluation. Monitoring/Attestation Systems are listed only as part of the SPoC Solutions in which they have been validated for use under the SPoC Program—i.e., Monitoring/Attestation Systems are not separately listed on the Website.
- **Back-end Monitoring Environment:** The environment in which the Monitoring/Attestation System resides and operates must be assessed by a SPoC Lab for compliance with Appendix A of the *SPoC Security Requirements*, "Monitoring Environment Basic Protections."

  ***Note:*** *If PAN or SAD is stored, processed or transmitted in the Back-end Monitoring Environment, that environment is considered a cardholder data environment (CDE) and must be assessed and validated by a QSA Company to PCI DSS, including DSS Appendix A3, "Designated Entities Supplemental Validation (DESV)."*

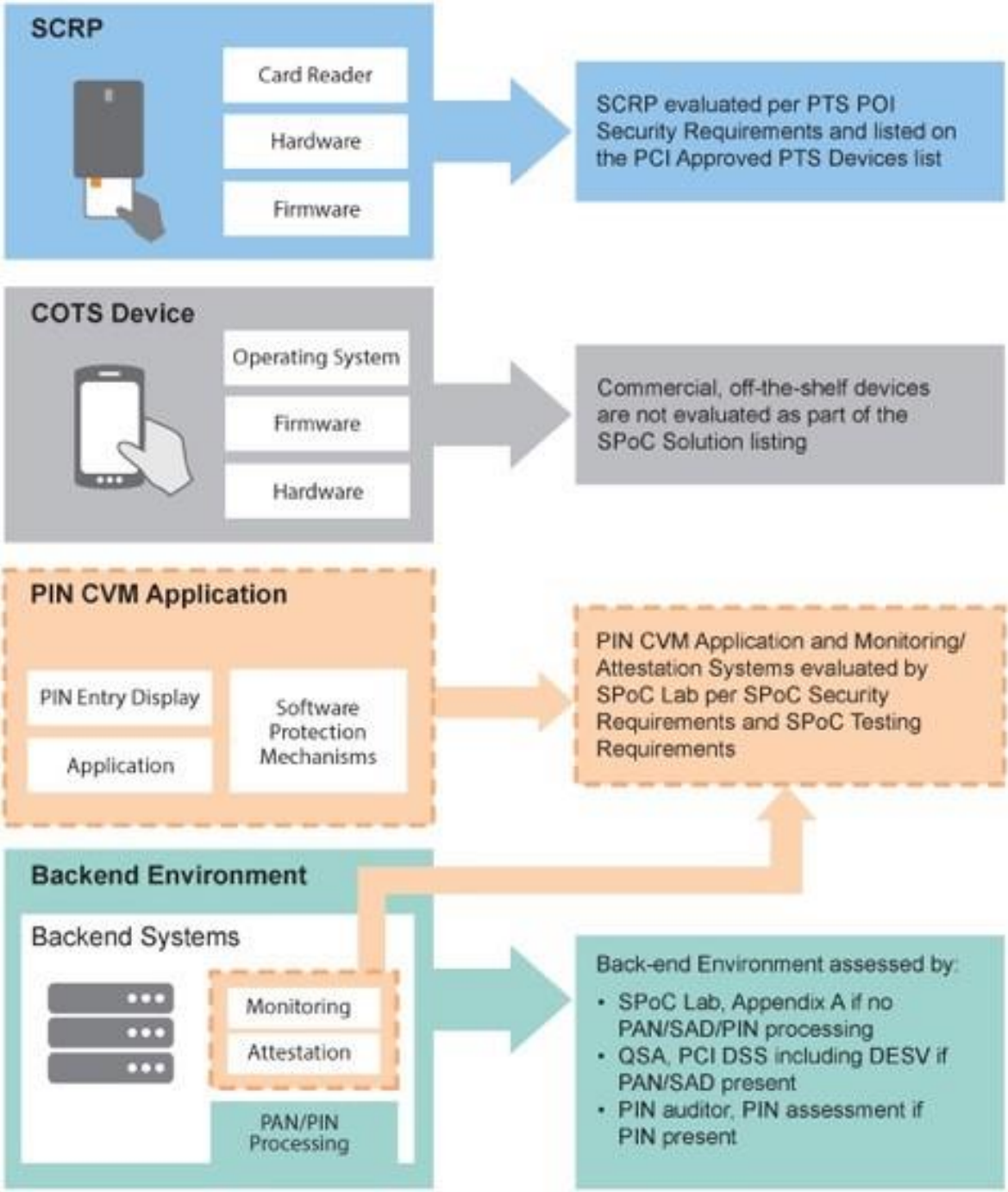
  ***Note:*** *If PIN processing is performed in the Back-end Monitoring Environment, a full PIN audit in accordance with the* PCI PIN Security Requirements *is also required.*

  Back-end Monitoring Environments are not listed on the Website.

The following diagram illustrates each element of the SPoC Solution and the SPoC Program stakeholder that validates each respective element. See the "**Overview"** and "**Software-based PIN Entry on COTS devices"** sections in the *SPoC Security Requirements* for additional details.

# SPoC Solution Elements

Overall solution evaluated by SPoC Lab per
SPoC Security Requirements and SPoC Testing Requirements



## 1.2 Related Publications

The Program Guide should be used in conjunction with the latest versions of (or successor documents to) the following PCI SSC publications, each as available through the Website:

| Document name | Description |
|---|---|
| *Payment Card Industry (PCI) Software-based PIN Entry on COTS Security Requirements* ("SPoC Security Requirements") | The *SPoC Security Requirements* defines the specific technical security requirements for the Solution, PIN CVM Application and supporting Monitoring/Attestation System and Back-end Monitoring Environment |
| *Payment Card Industry (PCI) Software-based PIN Entry on COTS Test Requirements* ("SPoC Test Requirements") | The *SPoC Test Requirements* lists and defines the specific testing and evaluation procedures, required to evaluate the Solution against the *SPoC Security Requirements*. |
| SPoC Solution Attestation of Validation ("AOV") | The AOV is a form for SPoC Labs to attest to the results of a SPoC Solution Evaluation, as documented in the SPoC Solution Attestation of Validation. |
| SPoC Evaluation Report template | The Evaluation Report template is a form for SPoC Labs to document the results of a SPoC Solution Evaluation. |
| *Vendor Release Agreement* ("VRA") | The VRA establishes the terms and conditions under which validated Solutions are Accepted and listed by PCI SSC. |

The most current versions of the following additional documents are used in conjunction with the aforementioned:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* (PCI DSS)
- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms* (Glossary)
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements, version 5.1*
- *Payment Card Industry (PCI) PIN Security Requirements and Test Procedures*

## 1.3 Updates to Documents and Security Requirements

This Program Guide may be modified as necessary to align with updates to the SPoC Program. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required Assessor or Lab training, e-mail bulletins and newsletters, frequently asked questions and other communication methods.

Technical FAQs are updated on a regular basis to add clarification to SPoC Program requirements and may also address new security threats that have arisen. As such, technical FAQs are generally effective immediately upon publication.

PCI SSC reserves the right to change, amend or withdraw security requirements, training and/or other requirements at any time.

# 2 Roles and Responsibilities

This section provides an overview of the roles and responsibilities of the various SPoC Program stakeholder groups. **See Sections 3–5 for details on evaluation, validation and listing of SPoC Solutions**.

## 2.1 SPoC Vendors

A vendor or provider seeking Acceptance of its candidate SPoC Solution, PIN CVM Application, Monitoring/Attestation System or Back-end Monitoring Environment as part of the SPoC Program must provide access to the applicable SPoC Solutions or SPoC Elements and supporting documentation to its SPoC Lab(s) for validation and authorize its SPoC Lab(s) to submit resulting reports and related information to PCI SSC.

***Note:*** SPoC *Vendors are responsible for assuring compliance with all applicable laws, statutes, regulations and rules (including without limitation, privacy laws) applicable to their activities as* SPoC *Vendors and any related services or products.*

### *2.1.1 Solution Providers*

Solution Providers (for example, processors, acquirers or payment gateways) have overall responsibility for the design and implementation of specific Solutions, ensuring that their Solutions satisfy all applicable *SPoC Security Requirements*, managing Solutions for their customers and/or managing corresponding responsibilities.

### *2.1.2 PIN CVM Application Vendors*

A software application vendor that develops PIN CVM Applications must have those applications evaluated for secure operation and must provide the SPoC Lab with access to all corresponding unobfuscated source code and documentation that describes the secure installation and administration of such applications as well as documentation associated with SCRPs that are intended to work with PIN CVM Application.

***Note:*** *The PIN CVM Application must be validated along with its supporting Monitoring/Attestation System as part of the Solution in which it is used.*

The Solution Provider submits a PIN CVM Application for evaluation—along with its supporting Monitoring/Attestation System—to an independent SPoC Lab. Per the *SPoC Security Requirements* and *SPoC Test Requirements*, PIN CVM Application Vendors must provide documentation describing the secure operation and administration of such applications.

### *2.1.3 Monitoring/Attestation System Vendors*

Monitoring/Attestation System vendors develop software applications intended to provide software-based tamper detection and response (i.e., Monitoring/Attestation Systems) for a PIN CVM Application that is evaluated for use in a Solution. Monitoring/Attestation System vendors must have their Monitoring/Attestation System evaluated and validated for compliance per the *SPoC Security Requirements* with each PIN CVM Application that it supports.

The Solution Provider submits a Monitoring/Attestation System for evaluation to an independent SPoC Lab. Per the *SPoC Security Requirements* and *SPoC Test Requirements*, Monitoring/Attestation System vendors must provide documentation describing the secure operation and administration of such applications.

### 2.1.4 Back-end Monitoring Environment Providers

A Back-end Monitoring Environment provider must strictly maintain secure facilities to host Monitoring/Attestation Systems. In order to be used as part of a validated Solution, Back-end Monitoring Environments must be evaluated and validated by a SPoC Lab in accordance with *SPoC Security Requirements* Appendix A, "Monitoring Environment Basic Protections," to ensure requirements are in place to protect systems and data in this environment.

When the Monitoring/Attestation System resides in a Back-end Monitoring Environment provider's CDE, each must additionally be validated by a QSA Company to PCI DSS, including DSS Appendix A3, "Designated Entities Supplemental Validation (DESV)."

If PAN or SAD is not present in the Monitoring/Attestation System's environment and it is not part of the Back-end Monitoring Environment provider's existing CDE, a SPoC Lab must validate that the environment complies with the logical and physical security requirements as defined in *SPoC Security Requirements* Appendix A, "Monitoring Environment Basic Protections."

***Note:*** *If PIN processing is performed in the Back-end Monitoring Environment, a full PIN audit in accordance with the PCI PIN Security Requirements and Test Procedures and PCI PIN Security Derived Test Requirements is also required and evidence submitted to the applicable payment brand(s).*

### 2.1.5 SCRP Device Vendors

A SCRP device Vendor submits a SCRP device to a PTS Lab for evaluation. Per *PCI PTS POI Modular Security Requirements* (version 5.1 or later), SCRP device vendors must develop a supplemental document describing the secure operation and administration of such devices. See *PCI PIN Transaction Security Device Testing and Approval Program Guide* for additional details.

***Note:*** *Only validated Secure Card Reader – PIN (SCRP) devices listed on the PCI SSC's list of PTS Approved PTS Device on the Website are permitted for use in validated Solutions*

### 2.1.6 Third-Party Service Providers

Third-party service providers (such as KIFs) are considered Third-Party Service Providers with respect to the SPoC Element or SPoC Solution for which they provide services, and their services are evaluated/assessed as part of each SPoC Element and/or SPoC Solution. A Third-Party Service Provider must have its third-party services reviewed during each SPoC Solution Evaluation in which its service is used. Note that Third-Party Service Provider services that load key materials must comply with all applicable PCI PIN Security Requirements.

Third-Party Service Providers are not eligible for listing in regard to the SPoC Program.

## 2.2 Entities Involved in SPoC Evaluations

### 2.2.1 PCI-recognized SPoC Laboratories (SPoC Labs)

PCI-recognized SPoC Laboratories (SPoC Labs) are qualified by PCI SSC to perform Evaluations of Solutions for listing on the List of Validated SPoC Solutions. SPoC Labs are also qualified by PCI SSC to separately evaluate PIN CVM Applications and Monitoring/Attestation Systems to be used in Solutions as well as Back-end Monitoring Environment assessments "Basic Protections" (see *SPoC Security Requirements*, Appendix A). For the purposes of the SPoC Program, SPoC Labs are responsible for:

- Performing Evaluations of PIN CVM Applications, Monitoring/Attestation Systems, Back-end Monitoring Environments and overall Solutions in accordance with the *SPoC Security Requirements* and *SPoC Test Requirements*.
- Providing an opinion regarding whether the Solution meets the *SPoC Security Requirements*.
- Documenting each such Evaluation in an Evaluation Report using the applicable reporting template(s).
- Providing adequate documentation within the Evaluation Report to demonstrate the Solution's compliance with the *SPoC Security Requirements*.
- Where applicable, submitting the applicable Evaluation Report and/or any change submission documentation to PCI SSC, along with the applicable SPoC Solution Attestation of Validation (AOV) signed by both the SPoC Lab and Vendor.
- Maintaining an internal quality assurance process for their SPoC Solution Evaluation efforts.

A PCI-recognized PTS Laboratory interested in becoming a SPoC Lab should contact PCI SSC.

### *2.2.2 PTS Labs (PCI-recognized Laboratories)*

PTS Labs are responsible for the evaluation of POI devices against PCI SSC's PIN Transaction Security (PTS) Standards and requirements ("PTS requirements"). Evaluation reports on devices validated as compliant with the PTS requirements are submitted by the PTS Lab to PCI SSC for approval; and if approved, the device is listed on PCI SSC's list of "Approved PTS Devices" on the Website.

PTS Labs are authorized by PCI SSC to perform evaluations of SCRP devices; only PTS Labs are authorized by PCI SSC to evaluate SCRP devices used in SPoC Solutions.

***Note:*** *SCRP device evaluation by a PTS Lab is a separate process from the validation of a SPoC Solution; the SPoC Solution Evaluation validates whether or not a given Solution (which may include multiple SCRP devices) is in compliance with the SPoC Security Requirements.*

In addition to the above, and for the purposes of the SPoC Program, PTS Labs are responsible for:

- Documenting each SCRP device evaluation in a report.
- Providing adequate documentation within the applicable report to demonstrate the compliance with the *PCI PTS POI Modular Security Requirements*.
- Where applicable, submitting applicable change submissions to PCI SSC, along with the applicable documentation signed by both the PTS Lab and SCRP device Vendor.
- Maintaining an internal quality assurance process for their evaluation efforts.

Unless also qualified as a SPoC Lab, a PTS Labs is not authorized by PCI SSC to perform SPoC Solution Evaluations.

## 2.3 Participating Payment Brands

The Participating Payment Brands independently develop and enforce the various aspects of their respective programs related to compliance with PCI SSC Standards, including, but not limited to:

- Defining security and program requirements for merchant and service provider levels
- Managing compliance enforcement programs (requirements, mandates or dates for compliance)
- Establishing penalties and fees

- Establishing requirements and who must validate
- Responding to cardholder data compromises

## 2.4 PCI Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the PCI SSC standards. In relation to the *SPoC Security Requirements*, PCI SSC:

- Maintains a centralized repository for all evaluation reports for Solutions listed on the Website;
- Hosts the List of Validated SPoC Solutions on the Website;
- Qualifies SPoC Labs to evaluate and validate SPoC Solutions and SPoC Elements for compliance with the *SPoC Security Requirements*;
- Maintains and updates the *SPoC Security Requirements*, *SPoC Test Requirements* and related documentation including FAQs; and
- Reviews all Solution Evaluation Reports submitted to PCI SSC and related change submissions for quality assurance and compliance with baseline quality standards.

***Note**: PCI SSC does not evaluate, assess or validate SPoC Elements or SPoC Solutions for SPoC compliance; evaluation and validation are the roles of the SPoC Labs. Listing of a Solution on the List of Validated SPoC Solutions signifies only that the applicable SPoC Lab has determined that it complies with the SPoC Security Requirements, that the SPoC Lab has submitted a corresponding Evaluation Report to PCI SSC and that the report, as submitted to PCI SSC, has satisfied all requirements of the PCI SSC for Evaluation Reports as of the time of PCI SSC's review.*

# 3 Preparation for the Evaluation

The *SPoC Security Requirements* are a cross-functional PCI SSC standard that include specific requirements that have been validated through the PCI SSC PTS Program and, where applicable, the PCI DSS Assessment/QSA Program and/or the PCI PIN program. The *SPoC Security Requirements* and *SPoC Test Requirements* also contain specific requirements for overall Solutions and SPoC Elements (SCRPs, PIN CVM Applications, Monitoring/Attestation Systems and Back-end Monitoring Environments) that are used in the Solution.

***Note:*** *SPoC Vendors, SPoC Labs and Assessors are expected to be acutely familiar with each module within the SPoC Security Requirements and SPoC Test Requirements before commencing an Evaluation.*

## 3.1 Considerations for Elements Used in SPoC Solutions

The following table should be used to help determine requirements and eligibility for various elements used in SPoC Solutions, along with references to the relevant documents and sections:

**Table 3.1**

| Element | Program Guidance |
|---|---|
| SCRP | Secure Card Reader – PIN (SCRP) is a PTS approval class that supports PIN entry on COTS devices in accordance with the *PCI PTS POI Modular Security Requirements* (version 5.1 or higher). PTS device approval helps to ensure that the device has been evaluated and meets industry recognized requirements for payment acceptance devices. SCRPs are listed on the list of Approved PTS Devices on the Website.<br>The Solution must only permit the use of SCRPs listed on the Website.<br>▪ Refer to Module 6, "Secure Card Reader (SCRP)," in the *SPoC Security Requirements*;<br>▪ Refer to the *PCI PTS POI Modular Security Requirements* (version 5.1 or higher) and supporting documentation in the Document Library on the Website.<br>Obtaining and maintaining PTS Program device approval is the responsibility of the secure-card reader vendor. For those devices required to be approved, such approval is a prerequisite for the devices being evaluated as part of a SPoC Solution Evaluation. SPoC Labs will request evidence of PTS Program device approvals being in place and current as part of performing a SPoC Solution Evaluation.<br>Device vendors wishing to obtain device approval under the PTS Program should consult the Website for further information. Obtaining PTS Program approval does not replace or supersede any payment card brand-specific device-approval processes. |

| Element | Program Guidance |
|---|---|
| PIN CVM Application | PIN CVM Applications must undergo validation by a SPoC Lab against:<br>▪ *SPoC Security Requirements*, including Module 2, "PIN Cardholder Verification Method (CVM) Application";<br>▪ *SPoC Security Requirements* Appendix D, "Application Security Requirements"; and<br>▪ *SPoC Test Requirements* Module 2, "PIN CVM Application Requirements."<br>A PIN CVM Application (and its supporting Monitoring/Attestation System) may be used in multiple Solutions, but it is considered a SPoC Element of only the specific Solution(s) for which it has been tested and validated in accordance with SPoC Program requirements.<br>***Note:*** *If the PIN CVM Application and/or the supporting Monitoring/Attestation System requires any additional software to be installed on the SCRP device, that software must also be tested and validated as part of the Solution Evaluation.* |
| Monitoring/Attestation System<br>("Monitoring System") | Monitoring/Attestation Systems must undergo validation by a SPoC Lab against:<br>▪ *SPoC Security Requirements*, including Module 3, "Back-end Systems – Monitoring/Attestation";<br>▪ *SPoC Security Requirements* Module 4, "Solution Integration Requirements"; and<br>▪ *SPoC Test Requirements* Module 3 "Back-end System Monitoring/Attestation Requirements."<br>A Monitoring/Attestation System (and the PIN CVM Application it supports) may be used in multiple Solutions, but it is considered a SPoC Element of only the specific Solution(s) for which it has been tested and validated in accordance with SPoC Program requirements. |
| Back-end Monitoring Environment | The Back-end Monitoring Environment must undergo validation per all requirements in *SPoC Security Requirements*, including Module 5, "Back-end Systems – Processing," and Security Requirements Appendix A, "Monitoring Environment Basic Protections."<br>▪ If PAN or SAD is present anywhere in the Back-end Monitoring Environment, then PCI DSS plus DESV compliance as validated by a QSA is instead required. In such cases, the Vendor's PCI DSS Attestation of Compliance (AOC) would be provided to the SPoC Lab during the SPoC Solution Evaluation as evidence of a compliant Back-end Monitoring Environment.<br>▪ If PIN processing (e.g., decryption or translation) is performed in the Back-end Monitoring Environment, a full PIN audit in accordance with the *PCI PIN Security Requirements and Test Procedures* and *PCI PIN Security Test Requirements* is also required. |

| Element | Program Guidance |
|---|---|
| Back-end Processing Environment<br>*(if separated from the Back-end Monitoring Environment)* | The Back-end Processing Environment, where cardholder data and/or PIN data is decrypted and securely processed, must undergo the following validations, where applicable:<br>▪ PCI DSS validation (ROC and AOC) by a QSA<br>▪ PCI PIN validation by a PCI PIN auditor approved by one of the PCI SSC brands<br>SPoC Labs shall request evidence of such validations, verify they are current and produce evidence during the submission of a SPoC Evaluation Report according to *SPoC Test Requirements* E1 and E2. |

## 3.2 Prior to the Evaluation

***Note:*** *The process for developing and testing Solutions—including guidance for implementing requirements, testing and validating compliance with each requirement—is defined within the SPoC Security Requirements and SPoC Test Requirements.*

Prior to commencing a SPoC Solution Evaluation (Evaluation), all parties involved are encouraged to take the following preparatory actions:

- Review the requirements of both the *SPoC Security Requirements* and *SPoC Test Requirements*, and all related documentation located on the Website.
- Determine/assess the Solution's readiness to comply with the *SPoC Security Requirements*:
  - Perform a gap analysis between security functionality and the *SPoC Security Requirements*;
  - Correct any gaps; and
  - If desired, the SPoC Lab may perform a pre-evaluation or gap analysis of a candidate SPoC Element or candidate SPoC Solution. If the SPoC Lab notes deficiencies that would prevent a compliant result, the SPoC Lab may provide a list of issues to the Vendor to be addressed before the formal Evaluation process begins.
- Solution Providers are responsible for ensuring that the various elements used as parts of their Solutions are each compliant with all applicable *SPoC Security Requirements*, and that they have appropriate agreements in place with the providers and vendors of such elements to ensure proper information disclosures if required under the *Vendor Release Agreement*.

## 3.3 Required Documentation

When submitting a Solution for initial Evaluation and listing, the Vendor must provide the SPoC Lab the documentation described in Appendix D: Documentation Required for SPoC Solution Evaluation.

***Note:*** *All completed Evaluation-related materials such as manuals, install guides, the* Vendor Release Agreement *and all other materials related to the Evaluation must be delivered to the SPoC Lab performing the Evaluation, not to PCI SSC.*

## 3.4 Evaluation and Review Timeframe Considerations

The amount of time necessary for the SPoC Lab to complete its work can vary widely depending on factors such as:

- How close the candidate Solution or Element is to being compliant with SPoC Program requirements at the start of the Evaluation—corrections necessary to achieve compliance will delay validation.
- Prompt payment of the fees due to PCI SSC—PCI SSC will not commence review of the submission until the applicable fee has been paid.
- Quality of the SPoC Lab's submission to PCI SSC:
  - Incomplete submissions or those containing errors—for example, missing, incomplete or unsigned documents—will result in delays in the review process.
  - If PCI SSC reviews any part of the submission more than once, providing comments back to the SPoC Lab to address each time, this will increase the length of time for the review process.

Any Evaluation timeframes provided by a SPoC Lab should be considered estimates, since they may be based on the assumption that the candidate Solution or Element is able to successfully meet all SPoC Program requirements quickly. If problems are found during the review or acceptance processes, discussions between the SPoC Lab, the Vendor and/or PCI SSC may be required. Such discussions may significantly impact review times and cause delays and/or may even cause the review to end prematurely—for example, if the Vendor decides it does not want to make the changes necessary to achieve compliance. Back-end Monitoring Environment Assessments (including PCI DSS Assessments or PIN audits, as applicable) may take additional time to complete and should be factored into the Vendor's overall timeframe planning.

***Note:*** *See Section 6.1, "Evaluation Report Acceptance, Issuance of Approval Overview" for details on PCI SSC review timeframes.*

## 3.5 Technical Support throughout Testing

It is recommended that the Vendor make a technical-resource representative available to assist with any questions that may arise during the Evaluation. During the review, and to expedite the process, a technical contact should be on call to discuss issues and respond to questions from the SPoC Lab.

## 3.6 Vendor Release Agreement (VRA)

For PCI SSC to review any Solution (or candidate Solution) submission for listing on the Website, the Vendor's signed copy of the then-current version of the *Vendor Release Agreement* (as then available on the Website) must be provided by the Vendor to the SPoC Lab, along with access to the Solution and other documents and materials, at the beginning of each SPoC Solution Evaluation process. Among other things, the VRA:

- Covers confidentiality issues;
- Covers the Vendor's agreement to SPoC Program requirements, policies and procedures;
- Gives permission to the Vendor's SPoC Lab to release Evaluation Reports, AOVs and related materials to PCI SSC for review; and
- Requires Vendors to adopt and comply with industry standard Vulnerability Handling Policies.

For PCI SSC review of an Evaluation Report to take place:

- The SPoC Lab must provide to PCI SSC the Vendor's signed copy of the then-current VRA, along with the initial Evaluation Report (and AOV, as applicable) submitted to PCI SSC in connection with that Evaluation.
- So long as an executed copy of the then-current VRA is on file with PCI SSC for the relevant Vendor, the SPoC Lab is not required to re-submit the same VRA with each subsequent Evaluation Report (or AOV, as applicable) for the same Vendor.

## 3.7 The Portal

For any Solution to be listed on the Website, all documents relating to the validation of the corresponding candidate Solution are to be submitted by the applicable SPoC Lab, on behalf of the Vendor, to PCI SSC through the PCI SSC's secure website ("Portal"). Submissions are pre-screened in the Portal by PCI SSC staff to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

The Portal is also used by PCI SSC to track communications relating to a particular submission.

## 3.8 SPoC Program Acceptance Fees

For each Solution to be listed on the Website, the Vendor is also required to pay an Acceptance Fee to PCI SSC. For each new Solution submission, the corresponding Acceptance Fee will be invoiced and must be received by PCI SSC before the submission will be reviewed, Accepted and added to the List of Validated SPoC Solutions. Upon Acceptance, PCI SSC will sign and return a copy of the corresponding AOV to both the Vendor and the SPoC Lab.

***Note:*** *All Evaluation-related fees are payable directly to the Lab (these fees are negotiated between the Lab and its customers).*

*PCI SSC will bill the Vendor for all Acceptance Fees, and the Vendor will pay these fees directly to PCI SSC.*

There are no annual recurring PCI SSC fees associated with the Acceptance of a SPoC Solution or SPoC Element. There are, however, PCI SSC fees associated with Vendor delays in annual revalidation of validated Solutions. Please see the Website for more information.

All SPoC Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

# 4 Evaluation and Reporting Processes

Following is a high-level overview of the SPoC Solution Evaluation process.

1. The SPoC Vendor (or Vendor) contracts with a SPoC Lab to perform an Evaluation of the Solution and negotiates the cost and any associated confidentiality and non-disclosure agreements with the SPoC Lab.

2. The Vendor provides the SPoC Lab with access to all SPoC Elements to be used in the Solution to be evaluated, as well as associated manuals and other required documentation, including but not limited to the SPoC Vendor's signed Vendor Release Agreement. See Section 3.3 for additional required documentation and materials. The SPoC Lab may also require access to the Back-end Monitoring Environment in order to validate the Monitoring/Attestation System functionality.

   When the Monitoring/Attestation System resides in a Back-end Monitoring Environment provider's cardholder data environment (CDE), each of these must adhere to PCI DSS, including DSS Appendix A3: Designated Entities Supplemental Validation (DESV).

   If PAN or SAD is not present in the Monitoring/Attestation System's environment—i.e., it is *not* part of the Back-end Monitoring Environment provider's existing CDE—the environment must comply with the logical and physical security requirements as defined in the *SPoC Security Requirements* Appendix A, "Monitoring Environment Basic Protections."

3. The SPoC Lab performs the SPoC Solution Evaluation, including evaluation of security functions and features, to determine whether the candidate Solution and its associated elements comply with the *SPoC Security Requirements* and are validated in accordance with the *SPoC Test Requirements*.

4. The SPoC Lab completes the Evaluation Report.

5. If the SPoC Lab determines that the Solution is compliant with the applicable *SPoC Security Requirements*, the SPoC Lab submits corresponding Evaluation Report and AOV (for each Solution) along with the Vendor's signed VRA and any other requested documentation to PCI SSC in accordance with applicable PCI templates, guidance and instructions.

6. If required, remedial activities are performed by the Vendor to address security objectives or requirements that are not in place, or security controls that were not sufficiently evidenced. The SPoC Lab will then perform follow-up testing and provide PCI SSC with an updated Evaluation Report.

7. PCI SSC issues an invoice to the Vendor for the applicable Acceptance Fee. After the Vendor has paid the invoice, PCI SSC reviews the Evaluation Report to confirm that it meets the SPoC Program requirements and if confirmed, PCI SSC notifies the SPoC Lab and Vendor that the Solution has successfully completed the process, will counter-sign the AOV and send a copy to the Vendor and the SPoC Lab and will add the Solution to the List of Validated SPoC Solutions on the Website.

   ***Note:*** *A listed SPoC Solution must at a minimum contain one of each successfully validated SCRP, PIN CVM Application and Monitoring/Attestation System and be implemented in a compliant Back-end Monitoring Environment.*

## 4.1 Required Vendor Materials

To support validation that the Solution meets the *SPoC Security Requirements*, the Vendor must provide sufficient evidence to enable a SPoC Lab to validate the requirements. Such evidence may be in the form of formal documentation such as policies and procedures, or informal documentation such as design documents, data-flow diagrams, process descriptions and results of internal analysis or testing (see Section 3.3 for additional details). However, any such evidence must clearly and concisely illustrate that the security controls implemented by the Vendor facilitate conformance with the security objectives and requirements. Such evidence must also illustrate the ongoing effectiveness of those security controls.

Additionally, the Vendor must provide access to (1) all production-level, unobfuscated source code and (2) all production-level, obfuscated code for all internally developed functionality as well as bespoke or custom functionality developed by third parties. Failure to provide adequate access to source code shall be considered a failure to meet applicable security objectives and requirements.

***Note:*** *In some cases, it may not be possible for a Vendor or SPoC Solution/SPoC Element to meet a specific requirement as stated. In such cases, the Vendor must provide clear and unambiguous justification for why the requirement cannot be met. The Vendor must also provide evidence to clearly illustrate that the corresponding security objective is still being met and that other functionality or methods are employed to provide similar 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.*

## 4.2 Supporting Multiple Platforms and Versions

Solutions for different major operating system versions and major versions of the *SPoC Security Requirements* represent different Solutions as far as *SPoC Test Requirements* are concerned. Each update to a Solution to support a new or different major COTS device operating system version, or a new major version of the *SPoC Security Requirements*, must undergo a new, complete ("full") Evaluation of the entire SPoC Solution.

## 4.3 Integrating SPoC Elements

If the SPoC Solution leverages security services from elements defined within the SPoC architecture that reside outside the formal technical boundary of the Solution—for example, at the COTS device or operating system level—those security services will also require validation as part of the Evaluation. SPoC Vendors who utilize these services are responsible for obtaining and providing to the SPoC Lab all evidence and materials necessary to support validation of these elements to the satisfaction of the SPoC Lab. Moreover, as part of the Evaluation, the SPoC Lab must evaluate the interaction between the Solution and the external security services.

The illustrations and descriptions on the following pages explain in further detail processes for the SPoC Program:

| Process | Illustration |
|---|---|
| SPoC Solution Evaluation for PCI SSC Listing | Figure 1 |
| SPoC Solution Submission and PCI SSC Review | Figure 2 |

**Figure 1: SPoC Solution Evaluation for PCI SSC Listing**

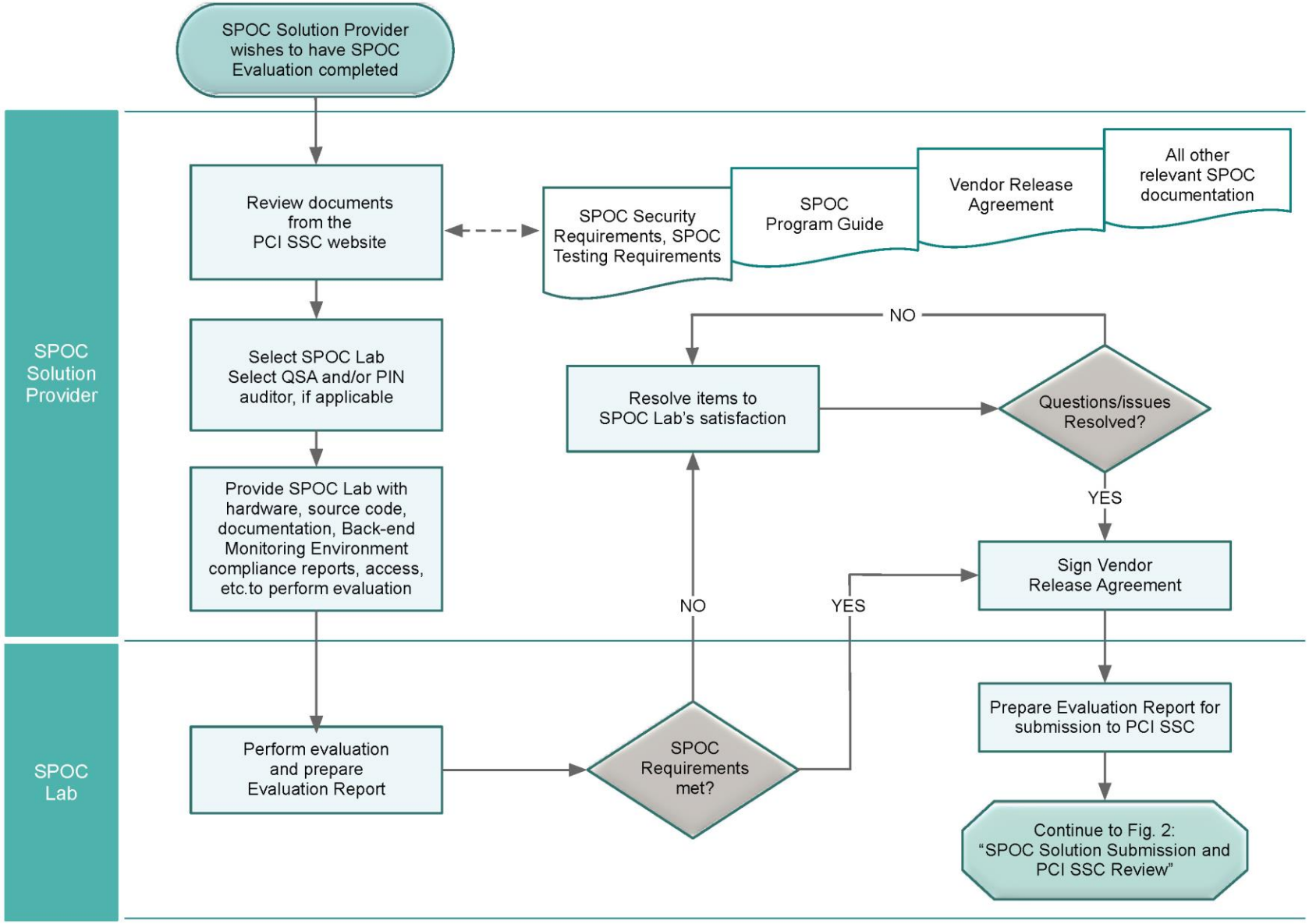
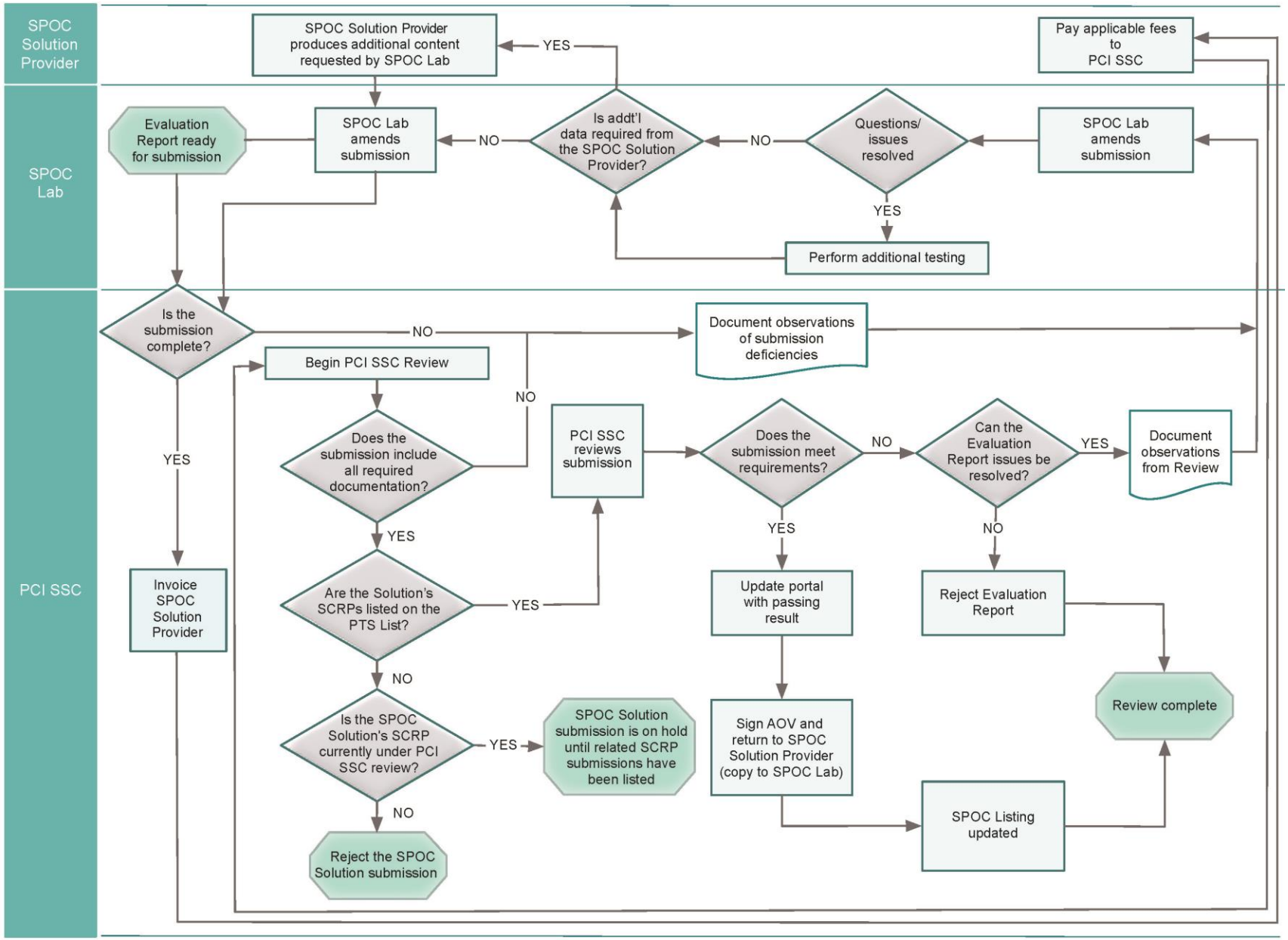


*Figure 2: SPoC Solution Submission and PCI SSC Review*



# 5 Maintaining a Validated Solution Listing

This section describes requirements for reevaluation of validated Solutions. Annual reevaluations are required on or before each one (1) year anniversary of the original date of Acceptance, in three (3) year cycles. Each anniversary is referred to below as a "Reevaluation Date." Solutions require a "checkpoint" reevaluation on or before the first and second Reevaluation Date in each cycle, and a new full Evaluation on or before the third Reevaluation Date in each cycle (the expiry date).

## 5.1 Annual Checkpoints

***Note:*** *Solutions require full Evaluation every three (3) years.*

Vendors are required to perform annual "checkpoints" at 12- and 24-month intervals from the date of Acceptance, including submission to PCI SSC of an updated SPoC Solution Attestation of Validation (AOV) at each checkpoint. Each annual checkpoint submission must be made by a SPoC Lab. SPoC Labs must review all changes that have occurred since the last full Evaluation or last annual checkpoint (whichever is more recent) and consider any Delta Changes that have been validated during the previous 12-month period, if applicable. The SPoC Lab must also perform live testing (i.e., testing full functionality of the live, production-level COTS devices, PIN CVM Application and its Monitoring/Attestation System) to provide assurance that the Solution remains compliant with all applicable SPoC Security Requirements.

PCI SSC will typically provide a courtesy reminder via e-mail to the Vendor's Primary Contact (listed on the AOV) within 90 calendar days of each checkpoint, but it is the sole responsibility of the Vendor to comply with checkpoint requirements and maintain its Listings, regardless of such courtesy reminder(s).

***Note:*** *It is strongly recommended that the Vendor submit its annual checkpoint documentation and attestation to the SPoC Lab that performed the last full SPoC Solution Evaluation, as changing SPoC Labs requires a full SPoC Solution Evaluation.*

As part of this annual checkpoint process, Vendors are required to confirm whether any changes have been made to the Solution, and that:

1) Changes have been applied in a way that is consistent with the *SPoC Security Requirements*;
2) The Solution continues to meet all applicable *SPoC Security Requirements*;
3) The Vendor is capable of—and demonstrably—migrating merchants from unsupported COTS platforms;
4) PCI SSC has been advised of any change that necessitates a change to the Listing on the Website, in accordance with this Program Guide;
5) Changes to the documents described in Appendix D: Documentation Required for SPoC Solution Evaluations are provided to the SPoC Lab for review, annually (i.e., at 12-month and 24-month checkpoints)
6) The operational quality of the Monitoring/Attestation System has been assessed as per Appendix B of the *SPoC Test Requirements*.

The Vendor is required to consider the impact of external threats and whether updates to the Solution are necessary to address changes to the external threat environment. The updated AOV, redlined Evaluation Report and any applicable documentation are submitted by the SPoC Lab to the PCI SSC SPoC Program Manager via the Portal. An updated AOV and redlined Evaluation Report must be submitted to PCI SSC ahead of the annual checkpoint date. PCI SSC has 30 days to review and accept the submittal. If PCI SSC doesn't receive the submittal prior to the annual checkpoint date, the Listing will be subject to early administrative expiry, as follows:

- Fourteen (14) calendar days following the annual checkpoint date, the corresponding Listing will be updated to show the Listing's annual checkpoint date in **Orange** for a period of 90 days past the annual checkpoint date.
- If the updated and complete AOV is received within this 90-day period, PCI SSC will update the corresponding Listing's annual checkpoint date with the new date and remove the **Orange** status.

***Note:*** *To avoid early administrative expiry (described below), Vendors should begin the annual checkpoint process in advance of the anniversary date of the Solution's Acceptance.*

- If the updated and complete AOV is not received within this 90-day period, the corresponding Listing's annual checkpoint date will be updated to show the date in **Red.**
- Once in **Red**, a full Evaluation (including applicable fees) is required to return the Solution Listing status to good standing.

PCI SSC will, upon receipt of the updated AOV and any applicable documentation: (i) review the submission for completeness; (ii) once completeness is established, sign and return a copy of the updated AOV to the Vendor and SPoC Lab; or (iii) update the annual checkpoint date on the Website.

## 5.2 Changes to SPoC Solution Listings

Vendors may update listed Solutions for various reasons—for example, adding additional supported SCRP devices or PIN CVM Applications. Changes do not have any impact on Reevaluation Dates of Solution Listings—i.e., Solution expiry dates or annual checkpoint dates. Changes to SPoC Solutions are categorized as follows:

**Table 5.2.a – Changes to Listed Solutions**

| Change Type | Description |
|---|---|
| **Administrative** | Changes made to a listed Solution that have no impact on the compliance with any of the *SPoC Security Requirements*, but where the List of Validated Solutions is updated to reflect the change.<br><br>Examples of administrative changes include, but are not limited to, corporate identity changes and changes to listing details such as "Description."<br><br>*See Section 5.2.1, "Administrative Changes for SPoC Listings," for details.* |
| **Designated** | Designated Changes are for changes to the Solution's website listing:<br>▪ Add/remove a PCI-approved SCRP<br>▪ Add/move a validated PIN CVM Application<br>*See Section 5.2.2, "Designated Changes for Solutions" for details.* |

**Table 5.2.b – Changes to SPoC Elements within Listed Solutions**

| Change Type | Description |
|---|---|
| **No Impact Change** | Any change that does not impact security functions or compliance with the *SPoC Security Requirements*—for example, maintenance patches or routine key rotation.<br><br>No Impact Changes are not reported in detail but are addressed by the Vendor during the annual checkpoint. |
| **Delta Change** | Delta Changes are limited to non-high-impact changes where the SPoC Lab determines the change has low security risk or low impact on compliance with the *SPoC Security Requirements* and can be assessed separately—e.g., a full Evaluation is *not* required in order to validate the change.<br><br>*See Section 5.2.3, "Delta Changes to PIN CVM Applications and Monitoring/Attestation Systems" for details.* |
| **High-impact Change** | High-impact Changes are changes where the SPoC Lab determines that the extent of the changes have high security risk or significant impact on the overall SPoC Solution, and a full Evaluation is required. High-impact Changes are not reported in a Change Impact template because they require a full Evaluation (see Section 4 for details).<br><br>*See Section 5.2.4, "High-impact Changes to PIN CVM Applications and Monitoring/Attestation Systems" for details.* |

### *5.2.1 Administrative Changes for SPoC Solution Listings*

Administrative Changes are limited to updates where no changes to a listed SPoC Solution have occurred, but the Vendor wishes to request a change to the way the Solution is currently listed on the Website. See Section 5.3, "Change Documentation," for specifics on the below:

***Note:** Administrative Changes are only permissible for already-listed Solutions that have not expired.*

The Vendor prepares a change analysis using the *Change Impact* template (Appendix C1 or Appendix C2, as applicable) and submits it to the SPoC Lab for review. The change analysis must contain the following information at a minimum:

- Name and reference number of the validated Solution Listing
- Description of the change
- Description of why the change is necessary

It is recommended that the Vendor submit change analysis to the same SPoC Lab used for the original SPoC Solution Evaluation, as changing SPoC Labs requires a full Evaluation of the Solution.

If the SPoC Lab agrees that the change as documented by the Vendor is eligible as an Administrative Change:

1) The SPoC Lab notifies the Vendor that it agrees;
2) The Vendor prepares the change documentation, signs the corresponding AOV and sends it to the SPoC Lab;

3) If applicable, the Vendor completes a new VRA;
4) The SPoC Lab completes the corresponding change documentation and signs the corresponding AOV;
5) The SPoC Lab signs its concurrence on the AOV and forwards it, along with the corresponding change documentation (and new VRA if applicable) to PCI SSC;
6) PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and
7) Upon payment of the invoice, PCI SSC will review the submission.

If the SPoC Lab does not agree with the Vendor that the change is eligible as an Administrative Change, the SPoC Lab works with the Vendor to consider the actions necessary to address the SPoC Lab's observations.

Following successful PCI SSC review of the change, PCI SSC will:

1) Amend the corresponding List of Validated SPoC Solutions on the Website accordingly with the new information; and
2) Sign and return a copy of the corresponding AOV to both the Vendor and the SPoC Lab. The Revalidation date of the updated Listing will be the same as that of the parent Listing.

Should there be quality issues associated with any aspect of the submission, PCI SSC will communicate them to the SPoC Lab. PCI SSC reserves the right to reject any change submission if it determines that a change described therein and purported to be an Administrative Change by the SPoC Lab or Vendor is ineligible for treatment as an Administrative Change.

### *5.2.2 Designated Changes for Solutions*

Designated Changes are intended to keep the Website Listing up-to-date. Designated Changes are amendments made only to a listed Solution's current Website listing to:

- Add/remove a validated SCRP device used in a Solution; or
- Add/move a validated PIN CVM Application used in a Solution; or

The Vendor prepares a change analysis using the Change Impact template (Appendix C1) and submits it to the SPoC Lab for review. The change analysis must contain the following information at a minimum:

- Name and reference number of the validated Solution Listing
- Description of the change
- Description of why the change is necessary

It is recommended that the Vendor submit the change analysis to the same SPoC Lab used for the last full Evaluation, as changing SPoC Labs requires a full Evaluation of the respective Solution.

If the SPoC Lab agrees that the change as documented by the Vendor is eligible as a Designated Change:

1) The SPoC Lab must notify the Vendor that it agrees;
2) If applicable, the Vendor completes a new VRA and submits this to the SPoC Lab;
3) The SPoC Lab performs an evaluation of the applicable *SPoC Security Requirements* that are affected by the change;

4) The SPoC Lab completes the corresponding Change Impact template and must produce a red-lined Evaluation Report and document the testing completed per PCI SSC requirements;

5) The Vendor prepares and signs the corresponding AOV (and new VRA if applicable) and sends it to the SPoC Lab;

6) The SPoC Lab signs its concurrence on the AOV and forwards it along with the completed change analysis using the Change Impact template, VRA (as applicable) and the red-lined Evaluation Report to PCI SSC;

7) PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and

8) Upon payment of the invoice, PCI SSC will review the Designated Change submission.

If the SPoC Lab does not agree with the Vendor that the change is eligible as a Designated Change, the SPoC Lab works with the Vendor to consider the actions necessary to address the SPoC Lab's observations.

Following successful PCI SSC review of the change, PCI SSC will:

1) Amend the List of Validated SPoC Solutions on the Website accordingly with the new information; and

2) Sign and return a copy of the corresponding AOV to both the Vendor and the SPoC Lab. The Revalidation date of the updated Listing will be the same as that of the parent Listing.

Should there be quality issues associated with any aspect of the submission, PCI SSC will communicate them to the SPoC Lab. PCI SSC reserves the right to reject any change submission if it determines that a change described therein and purported to be a Designated Change by the SPoC Lab or Vendor is ineligible for treatment as a Designated Change.

### *5.2.3 Delta Changes to PIN CVM and Monitoring/Attestation Systems*

Delta Changes are changes made to a PIN CVM Application and/or supporting Monitoring/Attestation System and are limited to changes where the SPoC Lab determines that a partial evaluation ("Delta Evaluation") can be performed, rather than a full Evaluation of the entire SPoC Solution. For example, changes to the PIN CVM Application that only impact the tamper-protection features may be eligible for Delta Evaluation.

Since the number of possible changes and their impact cannot be determined in advance, the type of evaluation required must be considered on a per-case basis. Vendors are encouraged to contact the SPoC Lab that performed the last full Evaluation of the Solution for guidance. The SPoC Lab engaged by the Vendor for this purpose then determines whether a Delta Evaluation or full Evaluation is required, based on the degree to which the changes impact the security and/or SPoC-related functions of the SPoC Element, the impact to *SPoC Security Requirements* and/or the scope of the changes being made.

See Section 5.3, "Change Documentation," for more specific information on the section below.

The Vendor prepares a change analysis using the Change Impact template (Appendix C2) and submits it to the SPoC Lab for review. The change analysis must contain the following information at a minimum:

- Name and reference number of the validated Solution Listing
- Description of the change
- Description of why the change is necessary

It is recommended that the Vendor submit the change analysis to the same SPoC Lab used for the previous full Evaluation, as changing SPoC Labs requires a full Evaluation of the SPoC Solution. If the SPoC Lab does not agree with the Vendor that the change is eligible as a Delta Change, the SPoC Lab works with the Vendor to consider the actions necessary to address the SPoC Lab's observations.

If the SPoC Lab agrees that the change as documented by the Vendor is eligible as a Delta Change:

1) The SPoC Lab notifies the Vendor that it agrees;
2) The Vendor prepares the change documentation and signs the AOV (and new VRA, if applicable) and sends it to the SPoC Lab;
3) The SPoC Lab completes the corresponding Change Impact document and must produce a red-lined Evaluation Report and document the testing completed per PCI SSC requirements;
4) The SPoC Lab signs its concurrence on the AOV and forwards it along with the completed change documents, VRA (as applicable) and the red-lined Evaluation Report to PCI SSC;
5) PCI SSC invoices the Vendor; upon payment of the invoice, PCI SSC will review the submission.

Following successful PCI SSC review of the change, PCI SSC will:

1) Amend the List of Validated SPoC Solutions on the Website accordingly with the new information; and
2) Sign and return a copy of the corresponding AOV to both the Vendor and the SPoC Lab. The Revalidation date of the updated Listing will be the same as that of the parent Listing.

Should there be quality issues associated with any aspect of the submission, PCI SSC will communicate them to the SPoC Lab. PCI SSC reserves the right to reject any submission if it determines that a change described therein and purported to be a Delta Change by the SPoC Lab or Vendor is ineligible for treatment as a Delta Change.

### *5.2.4 High-impact Changes to PIN CVM Application and Monitoring/Attestation Systems*

High-impact Changes are changes made to a PIN CVM Application and/or supporting Monitoring/Attestation System where the SPoC Lab determines the amount or impact of change cannot be validated by a Delta Evaluation; therefore, a complete ("full") Evaluation of the entire SPoC Solution is necessary. An example is a change that impacts multiple modules of the *SPoC Security Requirements* and cannot be tested or validated separately from the overall Solution. High-impact Changes are not reported in a Change Impact template because they require a full Evaluation (see Section 4 for details).

Since the number of possible changes and their impact cannot be determined in advance, the type of evaluation required must be considered on a per-case basis. Vendors are encouraged to contact the SPoC Lab that performed the last full Evaluation of the Solution for guidance. The SPoC Lab engaged by the Vendor for this purpose then determines whether a full Evaluation is required, based on the degree to which the changes impact the security and/or SPoC-related functions, the impact to *SPoC Security Requirements* and/or the scope of the changes being made.

## 5.3 Change Documentation

| Administrative Change (All SPoC Elements) | Delta Change (Application) | Designated Change (Solution) | Annual Checkpoint (Solution) |
|---|---|---|---|
| ▪ Solution Attestation of Validation (AOV)<br>▪ Change Impact document**<br>▪ Current VRA*<br>▪ Fee | ▪ Solution Attestation of Validation (AOV)<br>▪ Change Impact document **<br>▪ Red-lined Evaluation Report<br>▪ Current VRA*<br>▪ Fee | ▪ Solution Attestation of Validation (AOV)<br>▪ Change Impact document **<br>▪ Red-lined Evaluation Report<br>▪ Current VRA*<br>▪ Fee | ▪ Solution Attestation of Validation (AOV)<br>▪ Red-lined Evaluation Report<br>▪ Current VRA* |

* *If applicable*

** ***Note:*** *The Change Impact documents in Appendices C1 and C2 are mandatory for the SPoC Lab when submitting Administrative, Delta and Designated Changes to PCI SSC on behalf of Solution Providers*.

## 5.4 Renewing Expiring Listings

As a Solution Listing approaches its expiry date, PCI SSC will notify the Vendor of the pending expiration. The two options available for Vendor consideration are either new Evaluation or expiry:

- **New Validation:** If the Vendor wishes the Solution Listing to remain on the List of Validated SPoC Solutions on the Website, the Vendor must engage a SPoC Lab to perform a new full Evaluation against the then-current version of the *SPoC Security Requirements* prior to the expiry date, resulting in a new Acceptance. This new Evaluation must follow the same process as an initial SPoC Solution Evaluation.
- **Expiry:** Listing of Solution for which a new Acceptance has not occurred on or before the applicable expiry date will appear in **Orange** for the first 90 days past expiry, and in **Red** thereafter.

## 5.5 Validation Maintenance Fees

If a listed Solution is revised, the Vendor is required to pay the applicable change fee to PCI SSC.

For any change affecting the Listing of a validated Solution, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be reviewed, Accepted and added to the List of Validated SPoC Solutions. Upon Acceptance, PCI SSC will sign and return a copy of the AOV to both the Vendor and the SPoC Lab.

There is no PCI SSC fee associated with the processing of annual checkpoints.

All SPoC Program fees are posted on the Website. SPoC Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

***Note:*** *The Vendor pays all SPoC Solution Evaluation-related fees directly to the SPoC Lab. These fees are negotiated between the Vendor and the SPoC Lab.*

*PCI SSC will invoice the Vendor for all Validation Maintenance Fees, and the Vendor will pay these fees directly to PCI SSC.*

*A Solution must already be listed and not yet have expired in order to have a change Accepted and listed.*

## 5.6 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability

In the event of a Security Issue (defined in the VRA) relating to a validated SPoC Solution, the VRA requires the applicable Vendor to notify PCI SSC. *Vendors must be aware of and adhere to their obligations under the VRA in the event of a Security Issue.*

# 6 Reporting Considerations

## 6.1 Evaluation Report Acceptance, Issuance of Approval Overview

Upon receipt of the submission for a new SPoC Solution, PCI SSC will identify any technical issues or questions for resolution by the Lab, typically within two weeks of receipt. Subsequent Lab responses and information will be reviewed, and the cycle will repeat until satisfactory responses have been received or the submission is rejected or withdrawn.

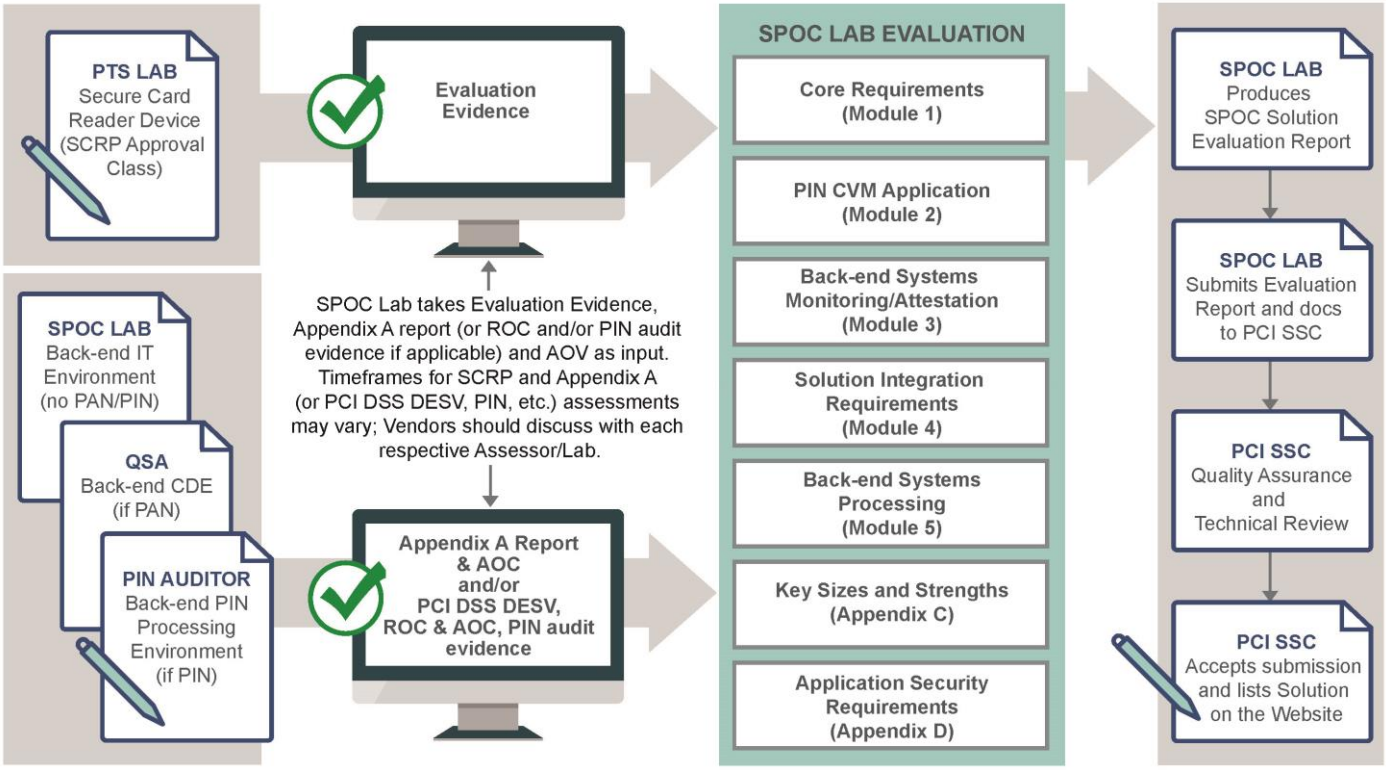
***Note:*** *PCI SSC review timeframes should be considered estimates and may vary based on queue and other factors.*

If and when PCI SSC determines that there are no issues or questions, PCI SSC will add the Solution to the List of Validated SPoC Solutions and issue a corresponding approval letter.

For reports on changes to existing Listed Solutions—i.e., Delta Changes—the same process applies, and PCI SSC will post revised information to the Website and issue a revised approval letter upon its determination that no issues or questions remain. Delta reports are prepared using the major requirements the Solution was assessed against when newly approved.

The diagram below provides a high-level illustration of the various processes, evidence (e.g., reports), participants (Lab, QSA, PIN auditor and PCI SSC) and steps involved in a SPoC Solution submission.

**Figure 3: SPoC Solution Submittal, Lab Evaluation and PCI SSC Review and Acceptance Process**



## 6.2 Delivery of the Evaluation Report and Related Materials

For Solutions to be listed on the Website, all documents required by PCI SSC in connection with the SPoC validation process must be submitted to PCI SSC by the SPoC Lab, through the Portal. PCI SSC will pre-screen Portal submissions to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

There must be consistency between the information in documents submitted for review and the "Details" fields within the Portal. Common errors in submissions include inconsistent product names or contact information and incomplete or inconsistent documentation. Incomplete or inconsistent submissions will result in a delay in the processing of requests for listing and/or may be rejected by PCI SSC.

### *6.2.1 Resubmissions*

For subsequent reviews, if multiple iterations of an Evaluation Report are required before PCI SSC Accepts the report, the SPoC Lab must submit Evaluation Report versions that include tracking of cumulative changes within the document.

## 6.3 Assessor Quality Management Program

Assessors and Labs are required to meet all quality assurance standards set by PCI SSC applicable to the SPoC Program. PCI SSC's Assessor Quality Management (AQM) Program as applicable to the SPoC Program is described below. Additionally, SPoC Labs and QSA Companies remain subject to all quality assurance policies, procedures and requirements of the PTS Program and QSA Program, as applicable.

### *6.3.1 Evaluation Report Submission Review*

PCI SSC reviews each Evaluation Report submission after the invoice for the Acceptance Fee has been paid by the Vendor. PCI SSC performs administrative ("pre-screening") review to ensure that the submission is complete; and if complete, PCI SSC reviews the submission in its entirety.

PCI SSC reviews the submission to determine whether the candidate Solution is eligible for validation pursuant to SPoC Program requirements, including but not limited to the Program Guide. If there is question as to eligibility, PCI SSC will contact the SPoC Lab for additional information. If the candidate Solution is determined to be ineligible for validation under the SPoC Program, the Evaluation Report will be rejected and the SPoC Lab will receive a letter of rejection with optional instructions for appeal.

If the candidate Solution is determined to be eligible for validation under the SPoC Program and the submission is complete, PCI SSC will conduct a complete review of the Evaluation Report submission and supporting documentation provided or subsequently requested by PCI SSC. Any comments or feedback from PCI SSC will be made via the Portal, and the SPoC Lab is expected to address all comments and feedback in a timely manner. PCI SSC's role is to ensure sufficient evidence and detail are present in the SPoC Lab's submission to provide reasonable assurance that the SPoC Solution Evaluation was performed in accordance with SPoC Program requirements and quality standards.

# Appendix A: SPoC Program Acceptance

Acceptance of a given SPoC Solution or SPoC Element by the PCI SSC only applies to the specific SPoC Solution or SPoC Element that has been validated by a SPoC Lab and subsequently Accepted by PCI SSC (each an "Accepted Element"). If any aspect of a SPoC Solution or SPoC Element is different from that which was validated by the SPoC Lab and Accepted by PCI SSC—even if the different SPoC Solution or SPoC Element (each an "Alternate Element") conforms to the basic product description of the Accepted Element—the Alternate Element should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No SPoC Vendor or other third party may refer to a SPoC Solution or SPoC Element as "PCI Approved," or "PCI SSC Approved" or otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a SPoC Vendor or its SPoC Solution or SPoC Element, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a corresponding AOV provided by PCI SSC. All other references to PCI SSC's acceptance of a SPoC Solution or SPoC Element are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC Acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the applicable SPoC Vendor or the functionality, quality or performance of the SPoC Solution or SPoC Element or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC shall be provided by the party providing such products or services, and not by PCI SSC or any Participating Payment Brand.

# Appendix B: Elements for the List of Validated SPoC Solutions

### *Company*

This entry denotes the **Solution Provider** for the validated Solution.

### *Solution Identifier*

**Solution Identifier** refers to a subset of fields in the Listing below the "Company" entry used by PCI SSC to denote relevant information for each validated Solution, consisting of the following fields, explained in detail:

<table>
<tr><th>Field</th><th>Detail</th></tr>
<tr><td>▪ Solution Name</td><td>Solution Name is provided by the Solution Provider and is the name by which the Solution is sold.</td></tr>
<tr><td>▪ Reference Number</td><td>PCI SSC assigns the Reference Number once the validated Solution is posted to the Website; this number is unique per Solution Provider and will remain the same for the life of the Listing.<br><br>An example reference number is 2018-XXXXX.XXX, consisting of the following:
<table>
<tr><th>Field</th><th>Format</th></tr>
<tr><td>Year of listing</td><td>4 digits + hyphen</td></tr>
<tr><td>Solution Provider #</td><td>5 digits + period (assigned alphabetically initially, then as received)</td></tr>
<tr><td>Individual Solution Number #</td><td>3 digits</td></tr>
</table></td></tr>
<tr><td>▪ Solution Details</td><td>Clicking on this link brings up a list of details specific to this Solution consisting of the following:<br><br>– SCRP Devices Supported: This section identifies the PCI-approved SCRP devices validated for use with this Solution and will include relevant PCI PTS reference numbers and the expiry date of the PTS approval for this device. If the expiry date is in the past, this will be denoted by a color change. A website link will be provided to the appropriate entry on the list of Approved PTS Devices on the Website.<br><br>– PIN CVM Application(s) Evaluated: This section identifies the PIN CVM Application(s) validated for use with this Solution.<br><br>Note that while a SPoC Solution or SPoC Element may include third-party services (including services such as KIFs), those are not listed within the Solution. Any use of such a component in another SPoC Solution would require Evaluation as part of each SPoC Solution of which the third-party service is a part.</td></tr>
</table>

### *SPoC Version*

**"SPoC Version"** is used by PCI SSC to denote the standard, and the specific version thereof, used to evaluate and validate compliance of the Solution.

### *Evaluation Lab*

This entry denotes the name of the SPoC Lab that performed the Evaluation and validated that the Solution is compliant with all applicable *SPoC Security Requirements*.

### *Reevaluation Date*

The **Reevaluation Date** is the date by which the Vendor must have the Solution fully re-evaluated against the current *SPoC Security Requirements* in order to maintain the Acceptance. Orange- or red-colored indicators next to this field signify that the Solution is overdue for submittal to PCI SSC

### *Annual Checkpoint Due*

Annual Checkpoint Due indicates the date in which the Solution is due for its annual (12- and 24-month) checkpoints by a SPoC Lab. Orange- or red-colored indicators by this field signify that the Solution is overdue for submittal to PCI SSC.

### *Description Provided by Solution Provider*

This section allows the Vendors to submit a description of the Solution to be used in the List of Validated SPoC Solutions, should the Evaluation Report be Accepted.

# Appendix C1: Change Impact Template for SPoC Solutions

This SPoC Change Impact Template is required for Administrative Change and Designated Change submissions for SPoC Solution Listings. Always refer to the applicable Program Guide for information on any SPoC Solution Listing changes.

The Vendor and/or SPoC Lab must complete each section of this document and all other required documents based on the type of change. The SPoC Lab is required to submit this SPoC Change Impact along with supporting documentation to PCI SSC for review.

### Part 1. SPoC Solution Listing Details, Contact Information and Change Type

| SPoC Solution Listing Details | | | |
|---|---|---|---|
| SPoC Solution Name | | Validated Listing Reference # | |
| Type of Change *(Please check)* | ☐ Administrative *(Complete Part 2)* | ☐ Designated *(Complete Part 3)* | |
| Submission Date | | | |

| Vendor Contact Information | | | |
|---|---|---|---|
| Contact Name | | Title/Role | |
| Contact E-mail | | Contact Phone | |
| **SPoC Lab Contact Information** | | | |
| Contact Name | | Title/Role | |
| Contact E-mail | | Contact Phone | |

## Part 2. Details for Administrative Change (if indicated at Part 1)

| Administrative Change Revision | | | |
|---|---|---|---|
| Current Vendor Company Name | | Revised Vendor Company Name *(if applicable)* | |
| Current SPoC Solution Name | | Revised SPoC Solution Name *(if applicable)* | |
| Additional details, as applicable | | | |

## Part 3. Details for Designated Change (if indicated at Part 1)

| Designated Change Revision | | |
|---|---|---|
| Identify the type of designated changes applicable to this submission and complete the appropriate sections of this SPoC Change Impact Template (check all that apply).<br>*Please refer to the* Program Guide *for details about each type of designated change.* | | |
| Add/Remove SCRP Device *(Complete Part 3a)* | ☐ Add | ☐ Remove |
| Add/Remove PIN CVM Application *(Complete Part 3b)* | ☐ Add | ☐ Remove |
| Add/Remove Monitoring/Attestation System *(Complete Part 3b)* | ☐ Add | ☐ Remove |
| Description of changes to the SPoC Solution | | |
| Description of how Designated Change impacts the SPoC Solution's functionality | | |
| Additional details, as applicable | | |

### Part 3a. Add/Remove SCRP Device Type (if indicated at Part 3)

| SCRP Device Type | | |
|---|---|---|
| Adding for inclusion in listing or removal from listing? | ☐ Addition/Inclusion in listing<br>*(Red-lined Evaluation Report review required, see details below)* | ☐ Removal from listing<br>*(No Red-lined Evaluation Report review required)* |
| SCRP Device type name/identifier | | |
| SCRP Device manufacturer, model and number | | |
| PTS approval number for SCRP Device | | |
| SCRP Device Hardware version # | | |
| SCRP Device Firmware version # | | |

Generate a red-lined Evaluation Report for the added device(s).

**Part 3b. Add/Remove PIN CVM Application or Monitoring/Attestation System (if indicated at Part 3)**

| SPoC Applications | | | | | |
|---|---|---|---|---|---|
| Adding for inclusion in listing or removal from listing? | | | ☐ Addition/Inclusion in listing<br>*(Red-lined Evaluation Report review required, see details below)* | | ☐ Removal from listing<br>*(No Red-lined Evaluation Report review required)* |
| PIN CVM | Monitoring/ Attestation | PIN CVM Application or Monitoring System Name | Version # | Vendor name | Notes (if applicable) |
| ☐ | ☐ | | | | |
| ☐ | ☐ | | | | |
| ☐ | ☐ | | | | |
| ☐ | ☐ | | | | |
| ☐ | ☐ | | | | |

Generate a red-lined Evaluation Report for the added PIN CVM Application or Monitoring/Attestation System (as applicable).

# Appendix C2: Change Impact Template for PIN CVM Applications and Monitoring/Attestation Systems

This SPoC Change Impact Template is required for Administrative Change and Delta Change submissions for PIN CVM Applications and/or Monitoring/Attestation Systems used in a listed SPoC Solution. Always refer to the applicable Program Guide for information on any SPoC Solution listing changes.

The Vendor and/or SPoC Lab must complete each section of this document and all other required documents based on the type of change (see tables in Section 5.2). The SPoC Lab is required to submit this SPoC Change Impact along with supporting documentation to PCI SSC for review.

### Part 1. PIN CVM Application or Monitoring/Attestation System Details, Contact Information and Change type

| SPoC Application Details | | | |
|---|---|---|---|
| Application Name | | ☐ PIN CVM Application | ☐ Monitoring/Attestation System |
| Version # | | Revised Version # *(if applicable)* | |
| Type of Change (check one) | ☐ Administrative *(Complete Part 2)* | ☐ Delta *(Complete Part 3)* | |
| Submission Date | | | |

| PIN CVM Application or Monitoring/Attestation System Vendor Contact Information | | | |
|---|---|---|---|
| Contact Name | | Title/Role | |
| Contact E-mail | | Contact Phone | |
| **SPoC Lab Contact Information** | | | |
| Contact Name | | Title/Role | |
| Contact E-mail | | Contact Phone | |

**Part 2. Details for Administrative Change (if indicated at Part 1)**

| Administrative Change Revision | | | |
|---|---|---|---|
| Current Company Name | | Revised Company Name *(if applicable)* | |
| Current SPoC Application Name | | Revised SPoC Application Name *(if applicable)* | |
| Current SPoC Application Version | | Revised SPoC Application Version *(if applicable)* | |
| Description of how this change is reflected in the Vendor's versioning methodology, if applicable, including how this version number indicates the type of change | | | |
| Additional details, as applicable | | | |

## Part 3. Details for Delta Change (if indicated at Part 1)

For **each** change eligible for Delta Evaluation, provide the following information. Changes that impact compliance with the *SPoC Security Requirements* must be reflected in the red-lined Evaluation Report submitted. Use additional rows or add pages if needed.

| Delta Change – Change Summary | | | |
|---|---|---|---|
| Change # | Detailed description of the change | Description of the purpose of the change | Description of how SPoC security is impacted |
| | | | |
| | | | |
| | | | |
| | | | |
| Additional details, as applicable: | | | |

Generate a red-lined Evaluation Report review for the changes to the PIN CVM Application or Monitoring/Attestation System (as applicable).

# Appendix D: Documentation Required for SPoC Solution Evaluation

The table below sets out documentation which must be provided to the SPoC Lab by the Vendor as part of the Solution Evaluation process. A subset of this documentation may be required by the SPoC Lab for annual checkpoints, as determined by the SPoC Lab.

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Implementation of sensitive services | Protection of Sensitive Services | 1.1.1 | Documentation detailing all sensitive services implemented by the components and solution must exist and be updated as necessary, or at least annually. At a minimum, this must include key loading (for all in-scope areas), signing of applications and SCRP firmware and signing of updates to the monitor services or configuration. |
| Random number generation functions and use | Random Numbers | 1.2.1 | Documentation to identify all random number generation functions and reliance on random data used in The Solution must exist and be maintained. |
| Cryptographic processes and operations | Acceptable Cryptography | 1.3.1 | Documentation must exist to identify cryptographic processes and operations used by The Solution for security services.<br>At a minimum, documentation must include the following:<br>• Cryptographic algorithms used, and where<br>• Identification of all keys, the complete key hierarchy, their purposes and crypto periods<br>• Key-generation or key-agreement processes |
| Key lifecycle management policy and procedures | Key Management | 1.4.1 | Documentation, including procedures, must exist to support all key lifecycle management functions used by The Solution. |
| Key-compromise procedures | | 1.4.8 | Shared public keys/certificates are acceptable, but methods and procedures to revoke compromised public/private key pairs must be documented and implemented. |
| Incident response procedures | | 1.4.12 | Incident response procedures must exist and include activities for reporting and responding to suspicious or confirmed key-related issues, including key compromises. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Application development and design. Includes:<br>• Development procedures<br>• Protection mechanisms<br>• Data-flow diagrams<br>• Block diagrams<br>• Merchant guidance<br>• Buffer management<br>• Vulnerability management and security testing | Development | 2.1.2 | Documentation must exist and be maintained to detail the following:<br>• Protections provided to the application to protect against tampering, side-channel attacks, fault injection and reverse engineering for the various supported platform and protection methods (such as TEE, white-box cryptography).<br>• Details of all areas where functions provided by the application are executed. This should include the main processing environment of the COTS device but may also include other local execution environments (such as a TEE or embedded security processor).<br>• Data-flow diagrams that show how the PIN is entered, processed, encrypted and validated within the application, where the data is transmitted outside of the scope of the application and any assumptions made about these external connections.<br>• Block diagram that indicates where all sensitive data is available in clear text on the merchant-side systems. This includes, but may not be limited to, the SCRP, the COTS operating system, any TEE or physically separate security-processing elements used. This diagram must indicate the flow of sensitive data through the various elements.<br>• Guidance for merchants regarding how to ensure the PIN is entered in a way that it cannot be observed.<br>• Identification of where internal buffers are used and cleared when collecting sensitive data.<br>• Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system.<br>• A policy on how to manage vulnerabilities and perform security testing. |
| Acceptable use policy | Secure Provisioning | 2.2.8 | A security policy must exist for acceptable use of the PIN CVM Application and be provided to all users of the PIN CVM Application, and is part of the PIN CVM Application End User License Agreement (EULA). |
| Tamper-resistance controls | Tamper Checks | 2.3.2 | Documentation must exist and be maintained on how tamper resistance is achieved for each of the supported platforms, including but not limited to:<br>• Code obfuscation<br>• Protections provided by specific platforms<br>• Reliance on TEE, security processor or other security feature of the COTS devices used |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| COTS system baseline parameters and procedures that include:<br>• Methodology used to address vulnerabilities<br>• Roles and responsibilities | COTS System Baseline | 3.1.1 | Documentation must exist and be maintained for the following:<br>• Implemented processes to determine the system baseline for acceptance of COTS devices (for example whitelist, blacklist, or hybrid approach)<br>• How these processes account for known and potential vulnerabilities in systems.<br>• Clear identification of roles and responsibilities for which aspects of the system baseline validation process are performed by the PIN CVM Application itself, and which are performed by other systems or execution environments.<br>• Process that is demonstrably in use for the discovery and remediation of bugs and vulnerabilities in the system. |
| System baseline update procedures | | 3.1.2 | Documentation must exist and processes be demonstrably in use that identify methods used for updating the system baseline as new threats are identified. |
| Attestation policy for SCRP, COTS, PIN CVM application | Attestation Mechanism | 3.2.1 | A documented attestation policy that defines health-check rules for the SCRP, COTS platform and PIN CVM Application attestation mechanisms must exist.<br>• The policy must include detailed response procedures for successful and non-successful results.<br>• The policy must be maintained and strictly controlled, including reviews and updates as necessary, at least annually. |
| Attestation escalation procedures | | 3.2.5 | Escalation procedures must be defined for undocumented and unknown attestation responses. |
| | | 3.2.7 | If the attestation system tamper response involves a manual process—e.g., a potential tamper event— it must be escalated to vendor staff to validate:<br>a. Written procedures for manually processed events must exist and be demonstrably in use.<br>b. These procedures must cover events where staff relied upon for such determinations are unavailable.<br>c. Events must be immediately escalated for manual review and then actioned within 48 hours.<br>d. Automated systems must be in place to disable any further payment processing from systems when an event has not been actioned for 48 hours. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Attestation update policy and procedures | Attestation Mechanism | 3.2.12 | Attestation mechanism changes must adhere to formal change-control procedures. |
| | | 3.2.13 | For manual updates of the attestation system:<br>• There must be documented procedures.<br>• Deployment of changes to the production environment must require dual control. |
| | Type 3 – Monitoring Environment Attestation of PIN CVM Application | 3.5.9 | A documented policy and procedure for assessing these changes to the system baseline must exist and provide details on how:<br>• Decisions are made to remove previously acceptable platforms from the system baseline.<br>• Such changes will affect the parties using these platforms, so the documentation must also include how communication is handled in these cases. |
| Risk-assessment policy methodology and procedures | | 3.5.10 | The Solution Provider must have a documented risk-assessment policy and procedures that provide details on:<br>• The methods used to assess on-going risk of The Solution;<br>• How and when updates to the system baseline are performed; and<br>• How such changes are communicated to affected merchants.<br>The risk-assessment policy and procedures must be reviewed at least annually.<br>It is not considered acceptable for the policy to require a minimum number of PIN CVM Applications to be using a vulnerable platform before it is removed from the system baseline. |
| | | 4.3.7 | The Solution Provider must have a documented risk-assessment policy and procedure, which is reviewed at least annually.<br>This policy must include the methods used to assess ongoing risk of The Solution as well as how and when updates to the system baseline are performed and how such changes are communicated to affected merchants. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Back-end Monitoring Environment Operational Procedures | Operational Management | 3.7.1 | Documented procedures to support the operation of the Back-end Monitoring Environment must exist and be demonstrably in use. |
| Security policies | | 3.7.3 | Reviews must be performed at least quarterly to verify operational procedures are being followed.<br>Reviews must be performed by personnel assigned to the security governance and include the following:<br>• Confirmation that all operation-management processes are being performed<br>• Confirmation that personnel are following security policies and operational procedures—for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc. |
| Secure channel policies and procedures | Secure Channels | 4.2.4 | Documentation must exist and be maintained to identify logical connections between the PIN CVM Application and other components of the system.<br>Documentation must identify how data confidentiality and authenticity is maintained |
| PIN CVM Solution user guide | PIN CVM Solution Requirement | 4.3.1 | A user guide that provides information about the Solution, including identifying control points and security responsibilities for the merchant(s), must exist and be made available to the merchant. |
| Solution incident response procedures | | 4.3.6 | Plans and procedures must be defined to address interruptions to the Solution due to unplanned business disruption, major disaster or failure of services.<br>Testing to ensure viability of such plans and procedures must be performed annually at a minimum. |
| For Appendix A documentation, the Vendor may provide the SPoC Lab with a copy of their report based on *SPoC Security Requirements* Appendix A, "Monitoring Environment Basic Protections," ("Back-end Monitoring Environment Report") and/or the accompanying AOC (if a different SPoC Lab performed the Appendix A assessment) using the template based on *SPoC Security Requirements* Appendix A ("Back-end Monitoring Environment Report template").<br>***Note:*** *If PAN or SAD is present anywhere in the Back-end Monitoring Environment, a full PCI DSS plus DESV Assessment performed by a QSA is required. In such cases, the Vendor would provide the SPoC Lab with the completed, signed PCI DSS AOC during the SPoC Solution Evaluation as evidence of a compliant Back-end Monitoring Environment.*<br>If PIN data is present anywhere in the Back-end Monitoring Environment, the Vendor must also provide the SPoC Lab with evidence that a full PIN assessment in accordance with the *PCI PIN Security Requirements and Test Procedures* and *PCI PIN Security Test Requirements* has been performed within the timeframe as prescribed per the Payment Brands' individual compliance programs. In such cases, the Vendor would provide the SPoC Lab with completed, signed evidence of the PIN assessment during the SPoC Solution Evaluation as evidence of a compliant Back-end Monitoring Environment. | | | |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Personnel background check policy and procedures | Governance and Security Policies | A.1.4 | Documented polices must exist and be demonstrably in use to require background checks on staff involved with the Back-end monitoring environment. |
| Back-end Monitoring Environment Configurations | Secure Networks | Appendix A.2.1 | Network and data-flow diagrams must exist to support the Back-end monitoring environment identifying architecture and security control points. |
| Back-end Monitoring Environment investigation and response procedures | | A2.3 | Alerts must be generated for action by responsible personnel upon detection of suspicious activity or anomalies. Establish and follow procedures for investigation and response. |
| Vulnerability Management policy and procedures | Vulnerability Management | A3.2 | Procedures to identify and rate vulnerabilities based on their criticality must exist and be in use. Procedures must align with industry-accepted practices. |
| Access control procedures | Access Controls | A.4.2 | Documented procedures for granting and managing access must exist and be in use. |
| Incident Response Procedures | Physical Security | A.5.5 | Implement response procedures to be initiated upon the detection of attempts to remove clear-text data from the Back-end monitoring environment via an unauthorized channel, method or process.<br>Response procedures must include:<br>• Procedures for the timely investigation of alerts by responsible personnel<br>• Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss |
| Back-end Monitoring Environment asset management procedures | Physical Security | A.5.3 | Procedures to remove access and return assets such as keys, access cards for terminated personnel or when job duties change must be defined and demonstrably in use. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Back-end Monitoring Environment retention policy and backup and recovery procedures | Physical Security | A.5.6 | System back-up requirements for the Back-end monitoring environment must be defined and address the following:<br>• Back-up copies of information, software and system images must be created and tested regularly.<br>• The frequency and retention of backups must be adequate to support day-to-day production activities and sufficient to facilitate recovery and achieve recovery objectives associated with those systems that require a recovery capability.<br>• Back-up information must be stored securely, with appropriate physical and environmental controls.<br>• Duration and frequency must match documented retention policy. |
| Back-end Monitoring Environment incident response policy and procedures | Incident Response | A.6.1 | Procedures must be defined, documented and communicated to support incident response policies |
| | | A.6.4 | Implement response procedures to be initiated upon the detection of attempts to remove clear-text data from the Back-end monitoring environment via an unauthorized channel, method or process.<br>Response procedures must include:<br>• Procedures for the timely investigation of alerts by responsible personnel<br>• Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss |
| Audit Log management policy and procedures | Audit Logs | A.7.1 | Policies and procedures must exist and be demonstrably in use for generating and managing audit logs for all system components. |
| Software Development policy and procedures including change control practices. | Application Security Requirement | Appendix D.1 | The software development process must be based on a formal process for secure development of applications, which includes:<br>• Development processes based on industry standards and/or best practices<br>• Information security incorporated throughout the software development life cycle<br>• Security reviews performed prior to release of an application or application update<br>At a minimum, the documentation must include quality controls standards and measurements as well as change-control practices to ensure oversight of the development processes. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Software-versioning methodology | Application Security Requirement | Appendix D.9 | The software development process must document and follow a software-versioning methodology, including:<br>• The format of the version scheme, including number of elements, separators, character set, etc. (consisting of alphabetic, numeric and/or alphanumeric characters).<br>• Definition of what each element represents in the version scheme (for example, type of change, major, minor, security or maintenance release, etc.) |
| Secure coding techniques | Application Security Requirement | D.5 | Applications must be developed according to industry best practices for secure coding techniques, including:<br>• Developing with least privilege for the application environment.<br>• Developing with fail-safe defaults (all execution is by default denied unless specified within initial design).<br>• Coding techniques include documentation of how sensitive information (e.g., cryptographic material, certificates, PIN, etc.) is handled in memory.<br>• Developing for all access point considerations, including input variances such as multi-channel input to the application. |
| Change control procedures | Application Security Requirement | D.8 | Software vendor must follow change-control procedures for all application changes. Change-control procedures must follow the same software development processes as new releases, and include the following:<br>• Documentation of impact<br>• Documented approval of change by appropriate authorized parties<br>• Functionality testing to verify that the change does not adversely impact the security of the system<br>• Back-out or product de-installation procedures |
| | Application Security Requirement | D.14 | A process must be implemented to document and authorize the final release of the application and any application updates. Documentation includes:<br>• Signature by an authorized party to formally approve release of the application or application update<br>• Confirmation that secure development processes were followed by the vendor. |

| Required Artifact | Section | SR Req. # | Requirement |
|---|---|---|---|
| Implementation guide | Application Security Requirement | D15 | Develop, maintain and disseminate an implementation guide that must:<br>• Provide relevant information specific to the application<br>• Address all requirements in this document<br>Include a review at least annually and upon changes to the application and is updated as needed to keep the documentation current with all changes affecting the application, as well as to the requirements in this document. |

# Appendix E: Placeholder for Future Use

# Appendix F: Software Versioning Methodology

Changes to production-level code necessitate updates to the respective software application's version numbering. Vendors are required to document and follow a software-versioning methodology as part of their system development lifecycle; the software-versioning methodology may be a separate document or part of the Vendor's Security Policy. Additionally, PIN CVM Application Vendors must communicate the versioning methodology to their customers and integrators/resellers in their implementation guidance documents. Customers and integrators/resellers require this information to understand which version of the application they are using and the types of changes that have been made to each. SPoC Labs are required to verify that the Vendor is adhering to the documented versioning methodology and the requirements of the SPoC Program Guide as part of the SPoC Evaluation. Note that if a separate version-numbering scheme is maintained internally by the Vendor, a method to accurately map the internal version numbers to the publicly listed version number(s) must be documented and maintained by the Vendor.

See *SPoC Security Requirements* Appendix D, "Application Security Requirements," (item 9) for additional information.

## F.1 Version Number Format

The format of the application version number is set by the Vendor and may be comprised of several elements. The versioning methodology must fully describe the format of the application version number including the following:

- The format of the version scheme, including:
  - Number of elements
  - Numbers of digits used for each element
  - Format of separators used between elements
  - Character set used for each element (consisting of alphabetic, numeric and/or alphanumeric characters)
- The hierarchy of the elements
  - Definition of what each element represents in the version scheme
  - Type of change: major, minor, maintenance release, etc.

## F.2 Version Number Usage

All impactful changes[1] to the PIN CVM Application (and/or its Monitoring/Attestation System) must result in a new application version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's published versioning policy. All changes that impact security functionality and/or any *SPoC Security Requirements* must result in a change to the version number listed on the Website.

The Vendor must document how elements of the application version number are used to identify:

- Types of changes made to the application—e.g., major release, minor release, maintenance release, etc.
- Changes that have no impact on the functionality of the application or its dependencies

[1] See Table 5.2.b for an overview of the various change types.

- Changes that have impact on the application functionality but no impact on security or compliance with *SPoC Security Requirements*
- Changes that impact any security functionality or compliance with *SPoC Security Requirements*

Elements of the version number used for non-security-impacting changes must never be used for security-impacting changes.

If the Vendor uses a versioning scheme that involves mapping of internal version numbers to external, published version numbers, all security-impacting changes must result in an update to the external, published version number.

Any version number that is accessible to customers and integrator/resellers must be consistent with the versioning policy described in the applicable implementation guides.

Vendors must ensure traceability between application changes and version numbers such that a customer or integrator/reseller may determine which changes are included in the specific version of the application it is running.

# Appendix G: Terminology

For purposes of this Program Guide, the following terms shall have the meanings set forth below, or if not defined below, in the documents referenced in Section 1.3, Related Publications. All such documents are available on the Website:

***Note:*** *Additional definitions for PCI terminology are provided in the general PCI Glossary on the PCI SSC website at https://www.pcisecuritystandards.org/pci_security/glossary.*

| Term | Definition / Source / Document Reference |
|---|---|
| Accepted/Acceptance | A SPoC Solution is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred) and will be listed on the List of Validated SPoC Solutions on the Website when PCI SSC has:<br>i. Received the corresponding compliant Solution Evaluation Report from the SPoC Lab;<br>ii. Received the corresponding fee and all documentation required with respect to that SPoC Solution as part of the SPoC Program; and<br>iii. Confirmed that:<br>a. The respective compliant Solution Evaluation Report is correct as to form (all applicable documents completed appropriately/sufficiently);<br>b. The SPoC Lab properly determined that the Solution is eligible to be a validated Solution;<br>c. The SPoC Lab adequately reported the compliance of the respective SPoC Solution with SPoC Program requirements; and<br>d. The detail provided in the Solution Evaluation Report meets PCI SSC's reporting requirements.<br>***Note:*** *PCI SSC may suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, complying with remediation requirements) Acceptance and listing of any Solution in accordance with applicable SPoC Program policies and procedures.* |
| Assessment | Assessment of a SPoC Solution's Back-end Monitoring Environment in order to validate compliance with the *SPoC Security Requirements* as part of the SPoC Program. |
| Assessor | A SPoC Lab or a QSA Company or a PIN auditor. |
| AOV | See *SPoC Solution Attestation of Validation.* |

| Term | Definition / Source / Document Reference |
|---|---|
| Back-end Monitoring Environment | The secure facility or environment assessed by a SPoC Lab (or QSA Company or PIN auditor, as applicable) in accordance with *SPoC Security Requirements* Appendix A, "Monitoring Environment Basic Protections," which includes (but is not limited to) network infrastructure, physical and logical security controls, access controls, vulnerability management and governance and security policies—in which a Monitoring/Attestation System is hosted. |
| COTS | Acronym for commercial off-the-shelf device. |
| DESV | Acronym for Designated Entities Supplemental Validation. See the PCI Glossary for additional information. |
| Delta Evaluation | Partial Evaluation of the Solution, performed against applicable *SPoC Security Requirements*, when changes to a Solution are eligible for review under the "Delta Evaluation" change-review process described herein. |
| Evaluation | See *SPoC Solution Evaluation.* |
| Evaluation Report | The SPoC Solution Evaluation Report required to be completed by a SPoC Lab during SPoC Solution Evaluations and submitted to PCI SSC for review and Acceptance, following the SPoC Solution Evaluation Report Template (available on the Website) and instructions therein. For a Solution to be included on the List of Validated SPoC Solutions on the Website, the corresponding Evaluation Report must be submitted to PCI SSC for review and Accepted. |
| List of Validated SPoC Solutions | The list on the Website of Solutions that have been Accepted for SPoC Program purposes. |
| Listing | The listing and related information regarding a Solution on the List of Validated SPoC Solutions. |
| Monitoring/Attestation System | An application—which includes any COTS device-side and back-end monitoring and/or attestation software applications—that has been evaluated and validated by a SPoC Lab to have met all applicable *SPoC Security Requirements*, and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn or terminated.<br>In the *SPoC Security Requirements* and/or *SPoC Test Requirements*, the "Monitoring/Attestation System" is an implementation that may be shared across different execution environments and which provides a level of validation and assurance of the execution environment in which the PIN CVM Application executes, thereby delivering a level of software-based tamper detection and response. |
| Participating Payment Brand | A global payment card brand or scheme that is also a limited liability company member of PCI SSC (or affiliate thereof). |
| PAN | Acronym for Primary Account Number. |
| PCI SSC | Acronym for PCI Security Standards Council, LLC. |

| Term | Definition / Source / Document Reference |
|---|---|
| PIN | Acronym for personal identification number. A numeric personal identification code that authenticates a cardholder. A PIN consists only of decimal digits. |
| PIN auditor | Entity approved by one of the Payment Card Brands to perform assessments of PIN-processing environments. |
| PIN CVM | Acronym for Personal Identification Number Cardholder Verification Method. |
| PIN CVM Application | All parts of the code (regardless of execution environment) that:<br>i. Are installed and executed on the merchant COTS device for the purposes of accepting and processing the cardholder PIN CVM; and<br>ii. Have been evaluated and validated (along with its supporting Monitoring/Attestation System) by a SPoC Lab to be in scope for the SPoC Program and to have met all applicable *SPoC Security Requirements* and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated.<br>Additionally, the client-side monitor and/or a payment application may be incorporated into the PIN CVM Application or may be a separate application. |
| Program Guide | The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) SPoCSoftware-based PIN Entry on COTS Program Guide,* as from time to time amended and made available on the Website. |
| PTS Program | The PCI SSC PIN Transaction Security program. |
| PTS Lab (or PCI-recognized Laboratory) | A security laboratory qualified by PCI SSC under the PCI SSC PCI-recognized Laboratory program. |
| QSA | A QSA Employee or QSA Company as defined in the QSA Qualification Requirements. |
| QSA Company | A company then qualified by PCI SSC as a Qualified Security Assessor Company. |
| QSA Program | Defined in the QSA Qualification Requirements. |
| QSA Qualification Requirements | The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)*, as from time to time amended and made available on the Website. |
| SAD | Acronym for Sensitive Authentication Data. |

| Term | Definition / Source / Document Reference |
|---|---|
| SCRP | Acronym for Secure Card Reader – PIN.<br>A physical, encrypting card reader that has been assessed compliant to the PCI PTS SCRP Approval Class and is listed on the PTS approval website. An SCRP is intended for use with a commercial off-the-shelf (COTS) device such as a mobile phone or tablet.<br>An SCRP can be:<br>▪ A contact chip-card-only reader<br>▪ A contactless-only chip card reader<br>▪ A reader supporting both contact and contactless chip card functionality<br>SCRPs perform PIN translation from PIN blocks received from the payment application on the COTS device to a PIN block for either conveyance to the processing host or for offline to the contact chip card.<br>See the *PCI PTS POI Modular Security Requirements* (version 5.1 or later) and *PCI PIN Transaction Security Device Testing and Approval Program Guide* for additional details. |
| SPoC Lab<br>(or PCI-recognized SPoC Laboratory) | A PCI-recognized Software-based PIN Entry on COTS Laboratory qualified by PCI SSC to perform Evaluations of Solutions, PIN CVM Applications and supporting Monitoring/Attestation Systems for SPoC Program purposes. |
| SPoC Element | A PIN CVM Application, Monitoring/Attestation System, Back-end Monitoring Environment, or SCRP, validated for use in a SPoC Solution. |
| SPoC Program | Refers to PCI SSC's program and requirements for qualification of Assessors, Labs and applicable employees thereof and validation and Acceptance of SPoC Solutions or SPoC Elements, as further described in this document and related PCI SSC documents, policies and procedures. |
| SPoC Security Requirements | The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Software-based PIN Entry on COTS Security Requirements*, any/all testing procedures, appendices, exhibits, schedules and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website. |
| SPoC Solution (or Solution) | The set of elements and processes that support software-based PIN entry on a COTS device, comprising a combination of validated SCRP(s), PIN CVM Application and supporting Monitoring/Attestation System, Back-end Monitoring Environment and related processes, which have been validated separately and as part of an integrated solution by the applicable SPoC Lab(s) and Accepted for listing on the PCI SSC website as part of the SPoC Program. At a minimum, a SPoC Solution must include at least one SCRP, a PIN CVM Application and supporting Monitoring/Attestation System and a Back-end Monitoring Environment. |

| Term | Definition / Source / Document Reference |
|---|---|
| SPoC Solution Attestation of Validation | A Solution "Attestation of Validation" declaring the Solution validation status against the *SPoC Security Requirements*.<br>The AOV, signed by the SPoC Lab and Solution Provider, is used when validating, revalidating or submitting changes to a Solution. |
| SPoC Solution Evaluation | Evaluation of a Solution by a SPoC Lab for purposes of validating compliance against the *SPoC Security Requirements* as part of the SPoC Program, including but not limited to:<br>▪ Evaluation of the PIN CVM Application and supporting Monitoring/Attestation System incorporated therein;<br>▪ Testing and validation of the above with the applicable SCRP device;<br>▪ Back-end Monitoring Environment and all other elements of the Solution; and<br>▪ End-to-end integration evaluation of the overall Solution. |
| SPoC Test Requirements | Requirements that dictate the set of tests that must be performed to confirm compliance with the *SPoC Security Requirements*. |
| SPoC Vendor (or Vendor) | Any of the following: SPoC Solution provider, PIN CVM Application and supporting Monitoring/Attestation System vendor, or Back-end Monitoring Environment provider. |
| Third-Party Service Provider | An entity that acts on behalf of a Solution Provider to provide a service or function that is incorporated into or utilized by the applicable Solution.<br>A Third-Party Service Provider must have its services reviewed during the course of each of its Solution-Provider customers' SPoC Solution Evaluations. |
| Vendor Release Agreement (or VRA) | The then-current and applicable form of release agreement that PCI SSC:<br>a. Requires to be executed by SPoC Solution Providers, Monitoring/Attestation System or Back-end Monitoring Environment Providers and/or PIN CVM Application Vendors (as applicable) in connection with the SPoC Program, and<br>b. Makes available on the Website. |
| Website | The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org. |