Read Me First:
For Stakeholder Feedback
Draft SAQ SPoC for PCI DSS v4.0

PCI Security Standards Council

Part One:
Overview of Stakeholder Feedback Process

PCI Security Standards Council®

Thank You in Advance!

First and foremost, the PCI Council would like to thank you for taking the time to review the *Draft Self-Assessment Questionnaire for Software PIN Entry on COTS Solutions (SAQ SPoC) for PCI DSS v4.0*.

Your review and feedback is welcome and is the reason for this stakeholder feedback process.

The following slides will guide your review.

Timeline for Stakeholder Feedback

- The review period will run from Monday 1 August 2022 through Monday 15 August 2022.
- Be sure to submit all feedback to the Portal no later than 8:00pm Eastern Time on Monday 15 August 2022.

Note: *PCI SSC can only accept feedback that is received via the Portal during the review period. Late feedback and feedback submitted via any other channel will not be accepted.*

Accessing the Document

- This stakeholder feedback period for the Draft SAQ SPoC is only available to to the members of the PCI SSC Board of Advisors, Global Executive Assessor Roundtable, Mobile Task Force, and SMB Task Force.
- To access the documents, log-in to the PCI portal: https://programs.pcissc.org with your username and password.
  - If you don't know your password, click "Forgot your password" to create a new password. If you do not have a username, please contact support@pcisecuritystandards.org for assistance.
- Click on "Stakeholder Feedback: SAQ SPoC for PCI DSS v4.0".
- Accept the group Participation Agreement (the NDA) to download the document.
- Click to download the document.

PCI Security Standards Council®

Submitting Feedback

- To enter feedback:
  - Select the Document and Section, enter the page number, and select the feedback Category.
  - Enter your Comments and Suggested Solution for each feedback item. Identify any specific PCI DSS requirement numbers or subsection of the draft SAQ that your feedback refers to (if applicable) in your Comments.
  - Remember to “Save draft comments” after each entry to ensure your work is saved.
- Ensure your work is saved after each entry and before you exit the portal, select “Save Draft Comments.”
  - You can come back later to finish entering feedback; you do not need enter all feedback in the same session.
- When all your feedback is complete, select “Submit Feedback” and then select “Ok” to confirm your submission is complete.
  - Once you select “Ok,” you will be unable to edit your feedback.
  - A confirmation email will be sent after you submit your feedback.
- Alternatively, you can download the feedback spreadsheet, input your feedback, save, and then upload the spreadsheet back to the Portal.

To maximize the value of your feedback:

- In the Comment field, explain the reason for your feedback.
- In the Suggested Solution field, include a recommendation to address your comments.
- Be as detailed as possible with your comments and suggested solutions.
- Feel free to leave either the Comment or Suggested Solution fields blank.
  - It is not necessary to copy the same information into both fields.
- Do not submit the same feedback item more than once.
  - This is unnecessary since PCI SSC reviews every feedback item submitted.
- Consolidate your feedback since you can only provide 50 feedback entries.
- Contact support@pcisecuritystandards.org with any questions.

Part Two: Overview of Request - Stakeholder Feedback Period for Draft SAQ SPoC

PCI Security Standards Council

Overview: Draft SAQ SPoC for PCI DSS v4.0

- The Draft SAQ SPoC for PCI DSS v4.0 is a new SAQ.
  - This SAQ will be in addition to the nine current SAQs.
- SAQ SPoC is similar to SAQ P2PE.
  - SAQ SPoC has 22 applicable PCI DSS requirements
  - SAQ P2PE has 21 applicable PCI DSS requirements.
    - SAQ SPoC includes PCI DSS Requirement 8.3.1, which is the only different requirement between the two SAQs.

Overview: Draft SAQ SPoC for PCI DSS v4.0

- This SAQ is for merchants that process account data:
  - Only via a PCI-listed approved PTS Secure Card Reader-PIN (SCRP) device and accompanying commercial off-the-shelf (COTS) mobile device (e.g., phone or tablet)
  - As part of a validated PCI-listed Software-based PIN Entry on COTS (SPoC) solution
  - Via card-present transactions (contact chip, contactless, and SCRP-based magnetic strip).

Not for unattended card-present, MOTO, or e-commerce channels

Not for SPoC solutions with stand-alone magnetic stripe readers

Not for service providers

Overview: Draft Eligibility Criteria for SAQ SPoC

- For this payment channel:
  - All payment processing is only via a card-present payment channel.
  - All payment processing is via an SCRP as part of a validated PCI-listed SPoC solution.
  - No other systems store, process, or transmit account data.
  - Other electronic account data is not received, transmitted, or stored.
  - No connections to other systems/networks in the environment.
  - Any retained account data is on paper only.
  - All controls in the SPoC Solution Provider's user guide are implemented.

Questions to Consider while Reviewing *Draft SAQ SPOC for PCI DSS v4.0*

- Are the stated eligibility criteria appropriate for merchants using SPoC solutions?
- SAQ SPoC is not applicable to solutions with stand-alone magnetic stripe readers (MSRs) - *included on page iii of SAQ SPoC.*
  - Will this have an impact on merchants' ability to use this SAQ?
- Are the included PCI DSS requirements appropriate for merchants using SPoC solutions?
- For this SAQ, is it clear which TPSPs are in scope for Requirement 12.8?
- Are there PCI DSS requirements that should be added to this SAQ?
- Do you have recommended updates to this SAQ to provide clarity for merchants using SPoC solutions?

For Information: SPoC Reference Materials

- Stakeholders may wish to consider referring to the following documents to provide context about SPoC solutions:
  - Software-Based PIN Entry on COTS Security Requirements.
  - Software-Based PIN Entry on COTS Test Requirements.
  - SPoC MSR Annex.
  - SPoC Unsupported OS Annex.
  - SPoC Technical FAQs.

These documents can be found on the PCI SSC website, in the Document Library, under the SPoC drop-down menu