Payment Card Industry (PCI)

Software Security Framework

Frequently Asked Questions

June 2019

Introduction

This document addresses frequently asked questions (FAQs) related to the PCI Software Security Framework.

The FAQs in this document are organized as follows:

1. General
2. Secure Software Standard
3. Secure Software Lifecycle Standard
4. Relationship between PCI Software Security Framework and other PCI Standards
5. PA-DSS Transition
6. Assessor Qualification

1. General

Q1 What is the PCI Software Security Framework?

A *The PCI Software Security Framework is a collection of related software security standards, and associated validation and listing programs. There are currently two standards under the PCI Software Security Framework:*

- *Secure Software Standard*
- *Secure Software Lifecycle (Secure SLC) Standard*

Q2 When is the Validation Program for the PCI Secure Software Framework expected to launch?

A *Initial program materials for the PCI Software Security Framework (including Program Guides and Assessor Qualification Requirements) were published in June 2019. Companies wishing to become a Software Security Framework (SSF) Assessor Company will be able to submit applications beginning October 2019 and assessor training will be available shortly afterwards. See Section 6 for further information on Assessor Qualification.*

Q3 What is a Software Security Framework (SSF) Assessor Company?

A *SSF Assessor Companies are qualified by PCI SSC to perform assessments to the Secure Software Standard, the Secure SLC Standard or both. The SSF Assessor Company List on PCI SSC's website indicates whether a company is qualified as a Secure Software Assessor Company and/or as a Secure SLC Assessor Company.*

2. Secure Software Standard

Q4 What is the Secure Software Standard?

A *The Secure Software Standard defines a set of security requirements and associated test procedures to help ensure payment software adequately protects the integrity and confidentiality of payment transactions and data.*

The Secure Software Standard includes a set of "core" requirements that apply to all types of payment software submitted for validation under the PCI Software Security Framework, regardless of the software's functionality or underlying technology. The initial release of the Secure Software Standard also includes an account data protection "module" that applies to software that stores, processes, or transmits account data. Modules are a collection of requirements to address a specific software type, use case, or technology. Where payment software does not possess the specific data or functionality, or does not utilize technologies that trigger a module's applicability criteria, the requirements within that module would not be assessed as part of the software validation. In the future, additional modules will be added to the Secure Software Standard to address other software types, use cases, or technologies.

Q5 To whom does the Secure Software Standard apply?

A *The Secure Software Standard is intended for payment software that is sold, distributed, or licensed to third parties. This includes payment software intended to be installed on customer systems as well as payment software deployed to customers "as a service" over the Internet.*

Validation to the Secure Software Standard is not intended for software developed in-house for the sole use of the company that developed the software, nor is it intended for software developed and sold to a single customer for the sole use of that customer. Refer to the Secure Software Program Guide for additional information.

Q6 What is the process for evaluating software to the Secure Software Standard?

A *Software vendors initiate the process by selecting a company qualified to perform Secure Software assessments from the PCI SSC's list of SSF Assessor Companies on the PCI SSC website, and negotiating any costs and agreements necessary to perform the assessment directly with the assessor company. Then the software vendor and the assessor company determine the scope of the assessment (i.e., what aspects of the payment software should be assessed), including identifying all applicable requirements and materials necessary to effectively perform the assessment. Once scope has been determined and all necessary materials and evidence have been collected, the assessor begins the software evaluation.*

Payment software evaluation includes analyzing all security functions, features, and capabilities provided by the software to determine whether the software complies with all applicable requirements within the Secure Software Standard. If the assessor determines that the software has met all applicable requirements, the assessor then prepares a corresponding Report on Validation (ROV) which details all of the requirements tested, the tests performed and their results, and any other opinions or conclusions the assessor may have. Additionally, the assessor shall also prepare an Attestation of Validation (AOV), which both the assessor and the software vendor shall sign, attesting to the results of the evaluation detailed in the ROV. The assessor then submits both the ROV and signed AOV to PCI SSC for review. PCI SSC reviews the ROV, including test results, vendor evidence, and assessor opinions and conclusions to confirm testing was performed satisfactorily and that all applicable requirements have been met. Upon acceptance of assessor materials and conclusions, PCI SSC adds the payment software to the PCI SSC's List of Validated Payment Software on the PCI SSC website.

Q7 Who is qualified to perform assessments to the Secure Software Standard?

A *Secure Software Assessor Companies and their employees. Secure Software Assessor Companies are independent security organizations that have been qualified by PCI SSC to validate payment software adherence to the Secure Software Standard. Secure Software Assessors are employees of Secure Software Assessor Companies that have satisfied and continue to satisfy the requirements defined in the PCI Software Security Framework Qualification Requirements for Assessors.*

The list of SSF Assessor Companies on PCI SSC's website identifies entities that are qualified as a Secure Software Assessor Company.

Q8 Does PCI SSC provide a list of payment software that is validated to the PCI Secure Software Standard?

A *Yes. Upon successful validation to the Secure Software Standard, payment software is added to the List of Validated Payment Software on the PCI SSC website.*

Q9 What type of payment software can be evaluated under the Secure Software Framework?

A *At the time of program launch, payment software eligible to be evaluated and listed on PCI SSC's website must:*

a) be involved in or directly supporting or facilitating payment transactions, ***and***

b) store, process, or transmit clear-text account data, and can therefore be validated against both the Secure Software Standard and the currently published Module A – Account Data Protection, ***and***

c) *be a commercially available product that is developed by the software vendor for sale to multiple organizations*.

The following software is ***not*** *eligible for validation at the time of initial program launch:*

- *In-house developed payment software that is used only by the company that developed it.*
- *Payment software that operates on any consumer electronic mobile device that is not solely dedicated to payment acceptance for transaction processing.*
- *Software products that are operating systems, databases or platforms; even those that may store, process, or transmit account data.*
- *Payment software intended for use on hardware terminals.*

Future modules are planned to support some of these use cases. Software that is ineligible for validation at initial program launch will not necessarily remain ineligible throughout the life of the program. All exclusions will be re-evaluated each time a new module is added to the Secure Software Standard and as the supporting program evolves.

Q10 As the Secure Software Standard applies to payment software that 'directly supports or facilitates payment transactions' do applications that are not directly involved in authorization or settlement e.g. fraud monitoring applications have to be validated?

A *Payment software involved in supporting payment transaction e.g. fraud monitoring applications may be eligible for validation within the PCI Software Security Framework. More information on eligibility can be found in the Secure Software Standard Program Guide on PCI SSC's website.*

Whether an entity is required to use software validated to the Secure Software Standard is determined by individual payment brand mandates, and not by PCI SSC. For information about payment brand requirements for use of PA-DSS validated applications, please contact the payment brands directly. Payment brand contact details can be found in FAQ How do I contact the payment card brands?

Q11 When must payment software be revalidated?

A *Validations against the Secure Software Standard have a three-year expiration. Further information on revalidations and the process for managing changes to validated payment software can be found in the Secure Software Standard Program Guide on PCI SSC's website.*

3. Secure Software Lifecycle Standard

Q12 What is the Secure Software Lifecycle Standard?

A *The Secure Software Lifecycle (Secure SLC) Standard defines a set of security requirements and associated test procedures for software vendors to validate how they properly manage the security of payment software throughout the software lifecycle. Validation against the Secure SLC Standard illustrates that the software vendor has mature secure software lifecycle management practices in place to ensure its payment software is designed and developed to protect payment transactions and data, minimize vulnerabilities, and defend against attacks.*

Q13 To whom does the Secure SLC Standard apply?

The Secure SLC Standard is intended for software vendors that develop software for the payments industry. Software vendors who have their software lifecycle management practices validated will be recognized on the PCI SSC's List of Secure SLC Qualified Vendors. Additionally, Secure SLC Qualified Vendors will be empowered to perform and self-attest to their own software "delta" assessments (as part of validation of their payment software products to the Secure Software Standard) with reduced assessor involvement or oversight. Refer to the Secure SLC Program Guide for additional information.

Q14 What is the relationship between the Secure Software Standard and the Secure SLC Standard?

A *The Secure Software Standard and Secure SLC Standard are two separate, independent standards. While both standards address some of the same concepts, each standard approaches those concepts from a different perspective (i.e., secure software development processes in the Secure SLC Standard, secure functionality and security features in the Secure Software Standard). Additionally, validation to one standard does not imply or result in validation to the other standard (or to any other PCI standard). With that said, there is additional flexibility provided to Secure SLC Qualified Vendors as part of the validation of their payment software to the Secure Software Standard. Secure SLC Qualified Vendors are empowered to perform and self-attest to their own software "delta" assessments with reduced assessor involvement or oversight. More information on software delta assessments is available in the Secure Software Standard Program Guide.*

Q15 What is the process for Secure SLC Qualification?

A *Similar to Secure Software validation, Secure SLC qualification is initiated by the software vendor by selecting a company qualified to perform Secure SLC Assessments from the PCI SSC's list of SSF Assessor Companies on the PCI SSC website, and negotiating any costs and agreements necessary to perform the assessment directly with the assessor company. Then the software vendor and the assessor company determine the scope of the assessment (i.e., what elements of the software vendor organization, software development processes, or payment software products are to be covered by the assessment), including identifying all applicable requirements and materials necessary to effectively perform the assessment. Once scope has been determined and all necessary materials and evidence have been collected, the assessor begins the Secure SLC Assessment.*

The Secure SLC Assessment involves evaluating the vendor's secure software lifecycle management practices to determine whether the vendor complies with all applicable requirements within the Secure SLC Standard. If the assessor determines that the vendor has met all applicable Secure SLC requirements, the assessor then prepares a corresponding Report on Compliance (ROC) which details all of the requirements tested, the tests performed and their results, and any other opinions or conclusions the assessor may have. Additionally, the assessor shall also prepare an Attestation of Compliance (AOC), which both the assessor and the software vendor shall sign, attesting to the results of the Secure SLC Assessment detailed in the ROC. The assessor then submits both the ROC and signed AOC to PCI SSC for review. PCI SSC reviews the ROC, including all test results, software vendor evidence, and assessor opinions and conclusions to confirm testing was performed satisfactorily and that all applicable requirements have been met. Upon acceptance of assessor materials and conclusions, PCI SSC adds the software vendor to the PCI SSC's List of Secure SLC Qualified Vendors on the PCI SSC website.

Q16 Who is qualified to perform Secure SLC Assessments?

A *Secure SLC Assessor Companies and their Secure SLC Employees. Secure SLC Assessor Companies are independent security organizations that have been qualified by PCI SSC to validate software vendor adherence to the Secure SLC Standard. Secure SLC Assessors are employees of Secure SLC Assessor Companies that have satisfied and continue to satisfy the requirements defined in the PCI Software Security Framework Qualification Requirements for Assessors.*

The list of SSF Assessor Companies on PCI SSC's website identifies entities that are qualified as a Secure SLC Assessor Company

Q17 Does PCI SSC provide a list of payment software vendors who are validated to the Secure SLC Standard?

A *Yes. Upon successful validation to the Secure SLC Standard, software vendors are added to the List of Secure SLC Qualified Vendors on the PCI SSC website.*

4. Relationship between PCI Software Security Framework and other PCI Standards

Q18 What is the relationship between the PCI Software Security Framework and PA-DSS?

A *The PCI Software Security Framework is separate and independent from PA-DSS. While the PCI Software Security Framework includes elements of PA-DSS, the Framework represents a new approach for securely designing and developing both existing and future payment software. PA-DSS was designed specifically for payment applications used in a PCI DSS environment. The PCI Software Security Standards extend beyond this to address overall software security resiliency. The PCI Software Security Framework is designed to support a broader array of payment software types, technologies, and development methodologies in use today and also support future technologies and use cases.*

Q19 What is the relationship between the PCI Software Security Framework and PCI DSS?

A *Validation to the Secure Software Standard and the Secure SLC Standard provides merchants, acquirers, and other payment industry stakeholders assurance that validated payment software is developed securely and with security functions to protect the integrity of the software and the confidentiality of sensitive data it stores, processes, and transmits.*

As with PA-DSS, use of payment software validated under the PCI Software Security Framework may support the security of an entity's cardholder data environment, but it does not make an entity PCI DSS compliant. Entities must ensure all payment software is implemented in a PCI DSS compliant manner and included in their PCI DSS assessments to verify the software is properly configured and meets applicable PCI DSS requirements.

Each entity must understand its compliance obligations and how it is meeting those obligations. While use of validated software can contribute to an entity's overall PCI DSS compliance, it does not replace the need for a full PCI DSS assessment.

Q20 Does validation or qualification under the PCI Software Security Framework result in validation to any other PCI standards?

A *Validation or qualification under the PCI Software Security Framework does not imply or result in validation to any other PCI standard. However, elements of other PCI standards and programs may be incorporated under the PCI Software Security Framework at some point in the future. If and when that will occur will be communicated well in advance of any transition from an existing or future standard or program to the PCI Software Security Framework.*

5. PA-DSS Transition

Q21 How does the PCI Software Security Framework impact PA-DSS validated applications?

A *The PCI Software Security Framework has no immediate impact on PA-DSS validated applications, although PA-DSS will eventually be replaced by the validation programs within the PCI Software Security Framework. Acceptance of new PA-DSS validations will continue until June 30, 2021, and all PA-DSS validated payment applications will remain current and continue to be governed under the PA-DSS program until the expiry date for those applications is reached (October 2022 for payment applications validated to PA-DSS v3.2). Upon expiry, all PA-DSS validated payment applications will be moved to the "Acceptable Only for Pre-Existing Deployments" list.*

Q22 Should vendors continue using PA-DSS or wait until the PCI Software Security Framework is launched before initiating assessments?

A *Transitioning from PA-DSS to the PCI Software Security Framework may take some software vendors time to adjust to the differences between the two programs. Therefore, software vendors are encouraged to continue to submit changes to currently validated applications via the PA-DSS program. Additionally, software vendors who have initiated PA-DSS assessments for new payment applications are encouraged to complete those assessments under the PA-DSS program. New PA-DSS validations will be accepted through mid-2021 and be valid through late 2022. Assessments against the PCI Software Security Framework are anticipated to begin in Q1 2020 and will have a three-year validity period.*

Q23 Can merchants continue to use PA-DSS validated applications after October 2022?

A *PA-DSS validated applications are moved to the "Acceptable Only for Pre-Existing Deployment" when the validation expires. For applications validated to PA-DSS version 3.2 this will occur at the end of October 2022 and the PA-DSS program will close. See FAQ 1195 for further information about applications listed as "Acceptable Only for Pre-Existing Deployment*".

6. Assessor Qualification

Q24 What is the process to become an SSF Assessor Company?

A *The process to become an SSF Assessor Company is documented in the PCI Software Security Framework Qualification Requirements for Assessors, available on the PCI SSC website. Companies will be able to begin the application process in October 2019. In order to be listed as an SSF Assessor Company, the company must have at least one employee successfully complete the Secure Software Assessor or Secure SLC Assessor training and exam. The SSF*

Assessor Company listing will indicate whether a company is qualified to perform Secure Software Assessments, Secure SLC Assessments, or both.

Q25 Is there a pre-requisite requirement to be a QSA or PA-QSA Company before becoming an SSF Assessor Company?

A *No, companies do not need to participate in the QSA or PA-QSA programs before becoming an SSF Company. However, companies which do participate in the QSA or PA-QSA programs may benefit from reduced training requirements for their assessor employees who wish to be, qualified to perform assessments under the PCI Software Security Framework.*

Q26 What are the criteria for becoming a Secure SLC Assessor?

A *QSAs and PA-QSAs who wish to become Secure SLC Assessor are required to complete computer-based training and successfully pass the appropriate exam.*

Other individuals who wish to become Secure SLC Assessors—that is, individuals who do not hold QSA or PA-QSA status–are required to attend instructor-led training and successfully pass the associated exams.

In addition to the training and exam requirements, all individuals and companies must meet the requirements set out in the PCI Software Security Framework Qualification Requirements for Assessors.

Q27 What are the criteria for becoming a Secure Software Assessor?

A *PA-QSAs who wish to become Secure Software Assessors are required to complete computer-based training and successfully pass the appropriate exam.*

Other individuals who wish to become Secure Software Assessors—that is, individuals who do not hold PA-QSA status—are required to attend instructor-led training and successfully pass the associated exams.

In addition to the training and exam requirements, all individuals and companies must meet the requirements set out in the PCI Software Security Framework Qualification Requirements for Assessors.

Q28 How does the PCI Software Security Framework affect PA-QSA qualification and training?

A *PA-QSA qualification and training are unchanged by the PCI Software Security Framework. Companies and individuals wishing to join the PA-QSA program should consult the PA-QSA Qualification Requirements available on the PCI SSC website*.

PCI SSC will be providing further details on the closure of the PA-QSA program in due course.

Q29 How does the PCI Software Security Framework affect P2PE (PA-QSA) qualification and training?

A *P2PE (PA-QSA) qualification and training are unchanged by the PCI Software Security Framework. Companies and individuals wishing to join the P2PE (PA-QSA) program should consult the P2PE Assessor Qualification Requirements available on PCI SSC's website*.

PCI SSC will be providing further details on the closure of the PA-QSA program in due course, including impact to the P2PE(PA-QSA) qualification and program.

Q30 What fees are associated with becoming an SSF Assessor?

A *Fees for becoming qualified as an SSF Assessor are provided on the PCI SSC website.*