Payment Card Industry (PCI)

Software Security Framework

Frequently Asked Questions

January 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

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 (SLC) Standard*

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

A *All program-related materials for the PCI Software Security Framework (including the Program Guide, Assessor Qualification Requirements, reporting templates, etc.) are scheduled for publication in mid-2019.*

2. Secure Software Standard

Q3 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. Requirement 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 requirement modules will be added to the Secure Software Standard to address other software types, use cases, or technologies.

Q4 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 applications developed in-house for the sole use of the company that developed the application, nor is it intended for software applications developed and sold to a single customer for the sole use of that customer. Even though in-house or custom payment software is not intended for validation, organizations designing and developing such software are encouraged to follow the principles and objectives in the Secure Software Standard.

Q5 What is the process for evaluating software to the Secure Software Standard?

A *Software vendors initiate the process by selecting a PCI-qualified assessor company from the PCI SSC's list of qualified assessors 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 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.*

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 software validation 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 software to the PCI SSC's List of Validated Payment Software on the PCI SSC website.

Q6 Who will be qualified to perform assessments to the Secure Software Standard?

A *PCI-qualified Secure Software Assessor Companies and their employees. PCI Secure Software Assessor (SSA) 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 SSA Companies that have satisfied and continue to satisfy all requirements of the SSA program.*

Q7 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.*

3. Secure Software Lifecycle Standard

Q8 What is the Secure Software Lifecycle (SSLC) Standard?

A *The Secure Software Lifecycle 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 Software Lifecycle 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.*

Q9 To whom does the SSLC Standard apply?

A *The SSLC Standard is intended for software vendors that develop software for the payments industry. Vendors who have their software lifecycle management practices validated will be recognized on the PCI SSC's List of SSLC-Qualified Payment Software Vendors. Additionally, SSLC-qualified vendors will be empowered to perform and self-attest to their own software "delta" assessments (as part of validation of their software products to the Secure Software Standard) with reduced assessor involvement or oversight. More information on software delta assessments will be provided when the Program materials are published.*

Q10 What is the relationship between the Secure Software Standard and the Secure Software Lifecycle Standard?

A *The Secure Software Standard and Secure Software Lifecycle 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 processes in the SSLC 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 SSLC-qualified vendors as part of the validation of their payment software to the Secure Software Standard. SSLC-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 will be provided when the Program materials are published.*

Q11 What is the process for SSLC Qualification?

A *Similar to Secure Software validation, SSLC qualification is initiated by the software vendor by selecting a PCI-qualified assessor company from the PCI SSC's list of qualified assessors 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 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 SSLC assessment.*

The SSLC assessment involves evaluating the vendor's secure software lifecycle management practices to determine whether the vendor complies with all applicable requirements within the Secure Software Lifecycle Standard. If the assessor determines that the vendor has met all applicable SSLC 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 SSLC assessment 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 all 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 vendor to the PCI SSC's List of SSLC-Qualified Payment Software Vendors on the PCI SSC website.

Q12 Who is qualified to perform SSLC assessments?

A *PCI-qualified Secure Software Lifecycle Assessor Companies and their employees. PCI Secure Software Lifecycle Assessor (SSLCA) Companies are independent security organizations that have been qualified by PCI SSC to validate software vendor adherence to the Secure Software Lifecycle Standard. Secure Software Lifecycle Assessors are employees of SSLCA Companies that have satisfied and continue to satisfy all requirements of the SSLCA program.*

Q13 Does PCI SSC provide a list of payment software vendors who are validated to the PCI SSLC Standard?

A *Yes. Upon successful validation to the Secure Software Lifecycle Standard, payment software vendors are added to the List of SSLC-Qualified Payment Software Vendors on the PCI SSC website.*

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

Q14 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 applications. 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.*

Ultimately PA-DSS and its validation program will be incorporated into the PCI Software Security Framework. A gradual transition path will be implemented to ensure continued support for PA-DSS applications until transition is complete. See Section 5, "PA-DSS Transition" for more information on the transition from PA-DSS to the PCI Software Security Framework.

Q15 What is the relationship between the PCI Software Security Framework and PCI DSS?

A *Validation to the Secure Software Standard and the Secure Software Lifecycle 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 captures, 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.

Q16 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

Q17 What is the timeline for transitioning from PA-DSS to the PCI Software Security Framework?

A *A three-year transition period will commence upon the launch of the Software Security Framework Validation Program in mid-2019. 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 (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. At that point, further updates to PA-DSS validated payment applications after PA-DSS expiry will need to be assessed under the Software Security Framework.*

Q18 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 vendors time to adjust to the differences between the two programs. Therefore, payment application vendors are encouraged to continue to submit changes to currently validated applications via the PA-DSS program. Additionally, 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-2020 and be valid through late 2022. Assessments against the PCI Software Security Framework are anticipated to begin in Q3 2019 and will have a three-year validity period, putting the expiry date of those validations at roughly the same expiry date as PA-DSS validations.*