Payment Card Industry (PCI)
Software Security Framework

Frequently Asked Questions for Version 1.1 Release

August 2021

Introduction

This document addresses non-technical frequently asked questions (FAQs) related to the Software Security Framework (SSF) version 1.1 release.

The FAQs in this document are organized as follows:

- SSF General
- Secure SLC
- Secure Software

Related Documents

This document should be used in conjunction with current versions of the SSF Standards and program documentation, including but not limited to the following, each available on the PCI SSC web site ("Website"):

- *Payment Card Industry (PCI) Software Security Framework Secure Software Requirements and Assessment Procedures, v1.1* ("Secure Software Standard v1.1")
- *Payment Card Industry (PCI) Software Security Framework Secure Software Program Guide, v1.1* ("Secure Software Program Guide v1.1")
- *Payment Card Industry (PCI) Software Security Framework Secure Software Lifecycle Requirements and Assessment Procedures, v1.1 ("Secure SLC Standard v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Secure Software Lifecycle Program Guide, v1.1 ("Secure SLC Program Guide v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Secure Software Template for Report on Validation, v1.1 ("Secure Software ROV Template v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Secure Software Attestation of Validation, v1.1 ("Secure Software AOV v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Secure Software Lifecycle Template for Report on Compliance, v1.1 ("Secure SLC ROC Template v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Secure Software Lifecycle Attestation of Compliance, v1.1* ("Secure SLC AOC v1.1")
- *Payment Card Industry (PCI) Software Security Framework Qualification Requirements for Assessors, v1.1 ("SSF Qualification Requirements v1.1")*
- *Payment Card Industry (PCI) Software Security Framework Glossary of Terms, Abbreviations, and Acronyms, v1.1 ("SSF Glossary v1.1")*

Frequently Asked Questions

SSF General

Q 1 How has the relationship between the Secure Software Standard/Program and the Secure SLC Standard/Program changed in the Software Security Framework (SSF) v1.1?

A The relationship between the Secure Software Standard/Program and the Secure SLC Standard/Program has not changed in SSF v1.1.

The Secure Software Standard and Secure SLC Standard are two separate, independent standards. While both standards may address similar concepts, each standard approaches those concepts from a different perspective; secure software development processes are addressed in the Secure SLC Standard, and secure functionality and security features for payment software are addressed in the Secure Software Standard. Validation to one standard does not imply or result in validation to the other standard (or to any other PCI Standard).

Secure SLC Qualified Vendors with payment software validated to the Secure Software Standard are provided some additional flexibility under the Secure Software program. Secure SLC Qualified Vendors are empowered to perform and self-attest to their own software "delta" assessments with reduced assessor involvement. More information on payment software delta assessments is available in the Secure Software Program Guide on the Website.

There is no program dependency for Secure SLC Qualified Vendors to have a listed software product.

With the release of SSF v1.1, Secure SLC Program eligibility was expanded to include vendors that produce software that does not meet the definition of payment software but that may be used within the payment environment. This update does not affect the relationship between the Secure SLC and Secure Software standards/programs.

Q 2 When do the SSF Qualification Requirements v1.1 become effective?

A The SSF Qualification Requirements v1.1 were effective upon publication (February 2021).

In this version, the existing requirement for Secure Software Assessors to successfully complete all required Secure Software training has been modified to accommodate the modular nature of the standard. It is important for Assessor Companies and Employees to be aware of these changes as the timelines to complete mandatory module training may impact an assessor's ability to perform Secure Software assessments.

Secure SLC

Q 3 When does version 1.1 of the Secure SLC Standard and supporting documentation become effective?

A New vendor qualifications to Secure SLC v1.0 will be accepted until 31 August 2021. Effective 1 September 2021, all new vendor qualifications must be completed using version

1.1 of the Secure SLC Standard, Program Guide, and associated forms and reporting templates.

New vendor qualification to Secure SLC v1.0 which are “in-queue” (i.e., submitted to the portal and invoice paid prior to 1 September 2021) will have until 1 December 2021 to complete the qualification process.

Q 4 How did vendor eligibility change with the release of Secure SLC Program, version 1.1?

A The Secure SLC Standard is intended for software vendors that develop software for use within the payments industry. The Secure SLC Program Guide v1.1 expands program eligibility beyond payment software vendors to vendors of "Eligible Software" that may be used within the payment environment. This eligibility expansion enables more vendors to leverage Secure SLC qualification and facilitates broader program adoption.

Software vendors who have their software lifecycle management practices validated will be recognized on the PCI SSC List of Secure SLC Qualified Vendors.

Additionally, Secure SLC Qualified Vendors that also have validated and listed Secure Software products 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. Refer to the Secure SLC Program and Secure Software Program Guides for additional information.

Q 5 Which version of the Secure SLC Program Guide should be used by SLC Vendors that were Qualified to version 1.0 of the standard and program?

A SLC Vendors that were Qualified under v1.0 should start using version 1.1 of the Secure SLC Program Guide, which was effective upon publication in February 2021.

Version 1.1 of the Secure SLC Program Guide does not alter the processes to be followed by listed Secure SLC Vendors; however, it does include minor errata edits and clarifications to the process flows and narratives that outline the Secure SLC qualification processes.

Secure Software

Q 6 When does version 1.1 of the Secure Software Standard and supporting documentation become effective?

A New validations to Secure Software Standard v1.0 will be accepted until 31 August 2021. Effective 1 September 2021, all new payment software validations must be completed using version 1.1 of the Secure Software Standard, Program Guide, and associated forms and reporting templates.

New payment software validated to the Secure Software Standard v1.0 which are “in queue” (i.e., submitted to the portal and invoice paid prior to 1 September 2021) will have until 1 December 2021 to complete the validation process.

Q 7 What was updated with the release of Secure Software Standard and Program, v1.1?

A The primary purpose for the updates to the Secure Software Standard and Program was to introduce the Terminal Software Module (TSM), also referred to as Module B, a set of

security requirements designed to specifically address PCI-approved PTS POI devices. However, various other Standards and Program updates were made as well to address errata, add minor clarifications, and align terminology across SSF documentation.

A complete list of the changes is provided in the Secure Software Standard Summary of Changes v1.0 to v1.1, which can be found in the Document Library on the PCI SSC website.

Changes to the Secure Software Program to accommodate the TSM include:

- The examples of payment software eligible for validation have been updated in the Secure Software Program Guide v1.1.
- Updates have been made to the Portal and Website to accommodate TSM submissions and listings, respectively.

Q 8 Which version of the Secure Software Program Guide should be used by Software Vendors with Payment Software validated to version 1.0 of the standard and program?

A Software Vendors with currently listed payment software should start using version 1.1 of the Secure Software Program Guide, which was effective upon publication in April 2021.

Version 1.1 of the Secure Software Program Guide includes details for use of the TSM Module, and also includes some minor errata edits and clarifications.

Q 9 Can non-payment software be validated under the Secure Software Program?

A No, not under the current program. However, vendors of non-payment software may be eligible for qualification under the PCI Secure SLC Program. Refer to the Secure SLC Program Guide v1.1 for further information and the most up-to-date eligibility guidance.

Q 10 Can mobile payment software be validated under the Secure Software Program?

A No, not under the current program. Mobile payment software intended to be installed on a commercial, off-the-shelf device—that is, a device that is not solely dedicated to payment acceptance for transaction processing—is not currently supported under the Software Security Framework.