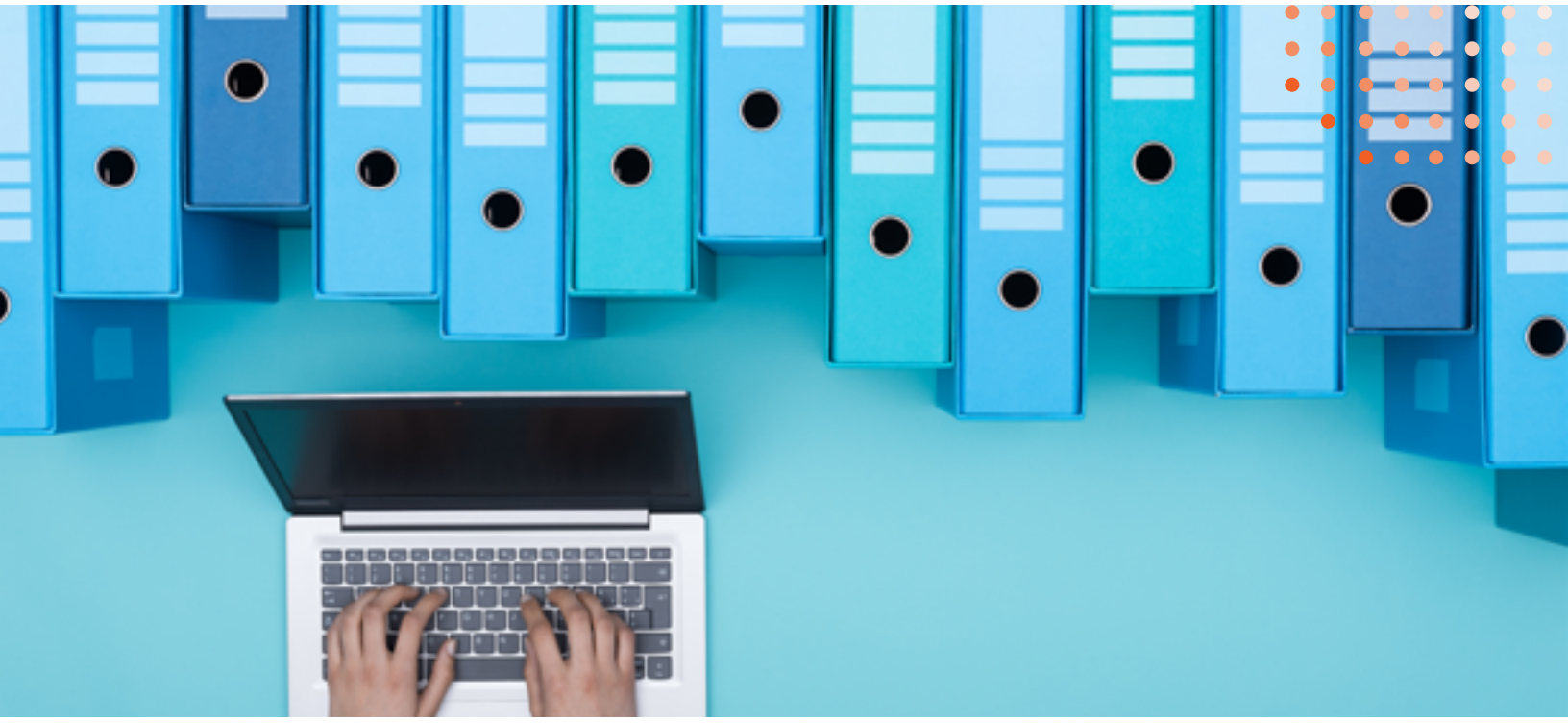
Navigating the PCI Software Security Framework (SSF)

JUNE 2021

PREPARED FOR

SecurityCompass



ALPINE Security Consulting

Executive Summary

As of June 30, 2021, applications can no longer be submitted under the Payment Card Industry (PCI) Payment-Application Data Security Standard (PA-DSS). PCI has created a new standard to replace the PA-DSS: the PCI Software Security Framework (SSF). The PCI SSF is an evolution for PCI that takes secure software development for payment related software to a new level. It is designed to be more flexible and take a more risk-based approach. This new approach brings some challenges and many changes.

While the PCI SSF replaces PA-DSS, we will briefly review how it is structured differently between the optional Secure Software Lifecycle (Secure SLC) standard and the Secure Software Standard (S3).

This paper will review what this means for those required to meet this new standard. If you have been required to meet PA-DSS in the past, the S3 applies to you, but you will need to understand the new approach and how to be prepared for it. If you develop software that has not been required to meet PA-DSS in the past, you also want to understand this approach as the PCI SSF continues to develop and expand the scope of what applications are included.

SSF provides an opportunity to better own the security aspect of your application development process. If done in the right way, this can result in a more efficient development process saving time and money in development and in the assessment process, all while producing a more secure application.

Understanding and following the PCI SSF can help any software developer to produce more secure software if the core principles are followed. This paper will also review how Secure Compass's SD Elements can be leveraged to meet and exceed the different aspects of the PCI SSF while streamlining your development process.

Audience

There are two primary readers who will benefit from the information in this paper:

- Organizations that have developed PA-DSS applications in the past.
- Organizations that develop payment related software that did not require PA-DSS in the past.

Additionally, any organization that has ever used a PA-DSS application or is responsible for an environment that handles cardholder data will need to understand the new standard and how it impacts their PCI-DSS requirements.

PCI SSF Overview

The PCI SSF is indeed a framework rather than just a single standard, and it is used to refer to the entire PCI collection of programs and guidance for the development of secure payment software. There are two distinct programs already mentioned: Secure SLC and S3.

Each of these programs are made up of three parts:

- **Standards:** The defined objectives of the standard. The S3 also contains multiple modules based on either specific functions or platforms.
- **Validation process:** This includes a program guide for each program as well as a reporting template
- **Listings:** Successful validation results in a listing on the PCI SSC website of qualified SLC vendors or qualified Payment Software.

Additionally, there are guidance and support documentation that apply to both programs including the PCI SSF Glossary and the PCI SSF Qualification Requirements for Assessors which is used for the validation process.

The Secure SLC is an "optional program" in that there is no requirement for any developer to get validated and listed as a Secure SLC vendor. Any organization, listed or not, can develop software under S3. However, anyone developing S3 software still needs to address the core Secure SLC objectives. The primary benefit of becoming listed is the ability to perform internal reviews of changes to products listed under S3 instead of needing to engage with a PCI SSF Assessor for those changes. The more applications listed by a single organization under S3, the greater the value this benefit has. Additionally, the removal of the "wildcards" from S3 can provide enough value to becoming a Secure SLC vendor simply to manage the frequency of application changes most software manages on a regular basis. A final, less obvious, benefit is that organizations that are validated as a Secure SLC vendor can potentially use internal resources to provide testing for an S3 validation instead of paying a PCI SSF assessor to do all of this.

S3 itself is the program that mimics the old PA-DSS program as it focuses on one payment software solution at a time. Any software that is in scope for S3 is required to be validated and listed on the PCI SSC website.

For the purposes of this paper, most information applies to PCI SSF, unless Secure SLC or S3 is called out. For additional details and information, you can access all the documents for these programs here.

PCI SSF Challenges and Solutions

CHALLENGES

As of June 2021, there is one Secure SLC Qualified vendor listed, and two Validated Payment applications. The PCI SSF standards were published in January 2019, and the PCI SSF program documentation was initially published in June 2019. After June 30, 2021, no more applications can be submitted for listing under the PCI PA-DSS Program, and all application submissions must use the PCI SSF program.

PCI SSF is not PA-DSS, despite the history and the similarities between them. It is designed to be more flexible, but this flexibility comes with a price in terms of the impact to manage the new standard's objectives. Software vendors who have existing robust security development practices are best suited to meet the PCI SSF objectives. PA-DSS was an application standard built from the PCI DSS, a network focused standard. In contrast, PCI SSF is built from a software development perspective with the goals of supporting modern software development practices, nimble development and update cycles, and modern payment demands including mobile, contactless, real time transactions and data analysis for business objectives.

Here are some key challenges organizations may face with PCI SSF:

- Not approaching PCI SSF in the same way PA-DSS was approached
- Maturing existing software development practices
- Training software developers
- Documenting software development policies
- Satisfying PCI SSF Assessors during the validation process

SOLUTIONS

Overcoming these challenges requires a focused and efficient approach. Here we review each challenge with the goal of identifying what to look for in a solution that best meets your organization's needs.

Not approaching PCI SSF in the same way PA-DSS was approached:

Traditionally PA-DSS assessments had a Payment Application Qualified Security Assessor (PA-QSA) review documentation and policies, test software functionality, and then a requirement to document compliance across all activities. PCI SSF still has those activities but with a different route to get there. Both the Secure SLC and the S3 have statements saying that the "objective-based" approach means that

"software vendors need flexibility to determine the software security controls and features and secure software lifecycle management practices and methods most appropriate to address their specific business and software risks."

In other words, software vendors are empowered to define how they meet the objectives within each standard based on "robust risk-management practice and evidence." It is up to the software vendor to define the rigor and frequency based on their risk-management program.

This is a significant opportunity that requires an effort by software vendors and is dramatically different than the PA-DSS process. This first challenge means that it is critical to take a fresh approach to how to meet the PCI SSF standard, including defining and maintaining a mature risk-management program.

Maturing existing software development practices:

With the increased flexibility of PCI SSF, the need to have standardized and mature development processes becomes critical. Documented procedures for development under PA-DSS can be an excellent place to start. However additional work needs to be done to not just document these practices, but also to demonstrate that these practices are in place for a more rigorous standard.

Training software developers:

A mature software development practice includes adequate security training for developers. The ability to train before and during the development process to keep developers fully up to speed will cover multiple objectives in the Secure SLC.

Documenting software development policies:

PA-DSS development policies will require some additional work to bring them up to speed with S3 objective 12 and several objectives from Secure SLC including 1, 2, 8, 9 and 10. Meeting this for PCI SSF will require an increased ability to track and quickly update changes to these policies.

Satisfying PCI SSF assessors during the validation process:

All the objectives across both standards will require the ability to demonstrate to the PCI SSF assessor that your development and application meet the details specified. The ability to document and track all the objectives relative to your organization's development processes will enable you to move quickly through the assessment process in a way that will save time and money. The complexity that comes with the new opportunity to demonstrate how you meet each objective based on your risk-management program makes this even more critical.

Defining and tracking security controls:

S3 objectives 2, 4, 9, 10 and 11 as well as Secure SLC objectives 3, 4, 5 and 6 all require the ability to define and track various security controls and threats to ensure the application can protect the sensitive data it handles. This represents a significant effort that can only be easily managed with tools that were not typically used for PA-DSS assessments.

How SD Elements Helps

OVERVIEW

SD Elements integrates PCI SSF objectives into the development of payment applications at the beginning of the software development life cycle and verifies compliance throughout the development process. This reduces time to market, minimizes repetitive development cycles, and improves compliance with PCI SSF for payment applications.

BENEFITS FOR PCI SSF

SD Elements has the ability to support an organization with automated processes tailored to meet the majority of the PCI SSF objectives. While reviewing the features and functionality of SD Elements, the following key benefits were observed.

SD Elements:

- Enables an organization to approach the PCI SSF with automation and the ability to tailor development processes and risk-management in a way that meets the PCI SSF objectives.
- Helps an organization to quickly mature existing software development practices.
- Train software developers before coding begins and offers Just-In-Time training during the development process that prevents delays while simultaneously improving security.
- Automates the documentation of software development policies.
- Provides output and internal organization that supports the validation process from a PCI SSF Assessor.
- Provides the ability to quickly define and track multiple security controls and software vulnerabilities within an application.

Software vendors accustomed to the PA-DSS validation process may be in for some difficult surprises with their first PCI SSF validations. The ability for an organization to create and maintain a mature risk management program and then also correlate this to the PCI SSF is a challenging task.

SD Elements offers a way to overcome these many challenges in a way that has the potential to result in assessments for payment software that are efficient and cost effective. Additionally, the software produced will go beyond the compliance objectives and result in payment applications built with security in mind from the ground up.

For software vendors that develop applications that are for non-payment uses, SD Elements can be used for these as well, offering what seemed to be un-obtainable before — the possibility to use compliance processes to benefit an organization's security objectives.

Future Projections

The S3 portion of the PCI SSF program has another feature not seen in the PA-DSS program — Modules. The Core requirements apply to all types of payment software regardless of the software's function or underlying technology.

To start, PCI included Module A, a required and critical module focused on Account Data Protection. This module is focused on specific data protection objectives tailored to Cardholder Data and Sensitive Authentication Data. This includes the original definition from PA-DSS: requirements for payment software that stores, processes, or transmits account data.

With version 1.1 of the S3, Module B was added — Terminal Software requirements focused on the needs of how the software interacts with physical hardware payment terminals — PCI-approved Point-of-Interaction devices.

Looking to the future, the question remains: what additional modules will be added? This question has an impact on what type of scope will be applied to software and the use of software within a payment environment. Per the current PCI FAQ for the SSF:

"In the future, additional modules will be added to the Secure Software Standard to address other software types, use cases, or technologies."

Currently the FAQ also states that the following payment software is not currently eligible for the PCI SSF program if:

- It is developed in house and only used in house.
- It operates on consumer mobile devices that are not dedicated to taking payments.
- It is an operating system, database, or platform.

Some of these do have planned modules for the future (Module B for Hardware terminals is one example that has already added), but each use case has yet to be determined and announced.

The above use cases will have significant impact on software developers should new modules be released. Even though the PCI SSF program does not yet allow for a formal review and listing, this does not mean a software vendor cannot work toward their software meeting the PCI SSF requirements right now. In fact, doing so now is the best time to begin to be prepared for the future, ensure security, and to demonstrate market differentiation.

Conclusion

The new PCI SSF program is a tremendous step forward in securing today's evolving payment software in a comprehensive and flexible way that consumers of payment applications can rely upon. Knowing the challenges involved in meeting the new flexible requirements is the best way to succeed.

SD Elements offers a unique and efficient approach that can make the PCI SSF validation process easier and more cost effective than the PA-DSS validation, while ensuring a more secure product to take to market. Using SD Elements in conjunction with non-payment software development processes is an additional unique benefit that gives organizations the opportunity to leverage a compliance framework that moves far beyond basic compliance. It is a holistic approach to improved software security across your organization.

About Alpine Security Consulting:

Alpine was founded to fulfill a passion for helping businesses and the people that work in them overcome today's cybersecurity challenges and succeed in new ways by leveraging the untapped value that an innovative approach to security can provide. With a background of over 20 years in technology, security, and compliance, Alpine can help virtually any business learn how to leverage innovative technologies to translate their security investments into tangible business value. www.alpineconsults.com

About Security Compass:

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India. For more information, please visit www.securitycompass.com.

About Dan Fritsche, CISSP:

Dan Fritsche, CISSP, is the Founder of Alpine Security Consulting. Dan's specialty is in security innovation, wherein he helps companies turn security from a hurdle into a strategic investment. Dan started his career with a security-focused role at IBM, where he supported functions like penetration testing, vulnerability scanning, application security, and business intelligence across multiple units during his decade-long tenure. After IBM, he worked at Coalfire where he helped companies improve their posture in application security, encryption, tokenization, and many other security specialties. Dan went on to help Global Payments drive the value and involvement of innovative security approaches as early in the application development life cycles as possible. Dan has held several certifications such as PCI QSA, PA-QSA, P2PE QSA/PA-QSA for at least five to 10 years.