atsec Information Security
Tel: +86-10-53056681
Fax: +86-10-53056678
www.atsec.com

PA-DSS 到 PCI SSF 标准的过渡

atsec 张力 ， 2021 年 10 月

关键词：PA-DSS、SSF、Secure Software、Secure SLC

1 背景

支付应用数据安全标准（PA-DSS：Payment Application Data Security Standard）的首个版本最早于2008年4月发布。PA-DSS的目的是帮助软件提供商开发安全的支付应用，确保应用没有存储完整磁条信息、其他敏感认证数据或者PIN等被禁止的数据，并且确保他们的支付应用支持PCI DSS合规。PA-DSS是支付产业非常成熟的标准，相关评估和验证体系也得到产业广泛应用。PA-DSS所维护的最后一个版本为2016年5月发布的PA-DSS v3.2。PA-DSS为支付行业的软件安全奠定了基础，至今已为支付行业服务了10多年，现在需要一种新的方法来支持现代支付软件体系结构和软件开发方法，并保护支付软件免受日益复杂的攻击，针对新的支付技术需要更加灵活的标准扩展能力。

支付卡产业软件安全框架（PCI SSF：Payment Card Industry Software Security Framework）是一套安全标准和相关验证和列表程序的集合，用于促进支付行业的软件安全。PCI SSF由安全软件标准（Security Software Standard）和安全软件生命周期标准（Secure SLC Standard）组成。安全软件标准定义了支付软件必须具备的安全特性和属性，安全SLC标准定义了软件供应商必须具备的安全流程和能力，以确保其软件是安全开发的。

本文将对PA-DSS与PCI SSF标准做出简要对比，以及如何从PA-DSS过渡到PCI SSF标准给出概括性介绍和指导。

2 PA-DSS 到 PCI SSF 的过渡时间表

新的PA-DSS验证申请已于2021年6月30日截止，目前已不再接受关于PA-DSS的验证申请。现有的PA-DSS验证的应用程序将保留在验证的支付应用程序列表中，按照正常的流程，供应商可以在有效期内向PCI标准委员会提交变更申请，直到2022年10月底有效期结束。在此日期之后，所有PA-DSS验证的应用程序列表将被移至“仅可接受预先部署 ”（Acceptable Only for Pre-existing Deployments）列表。

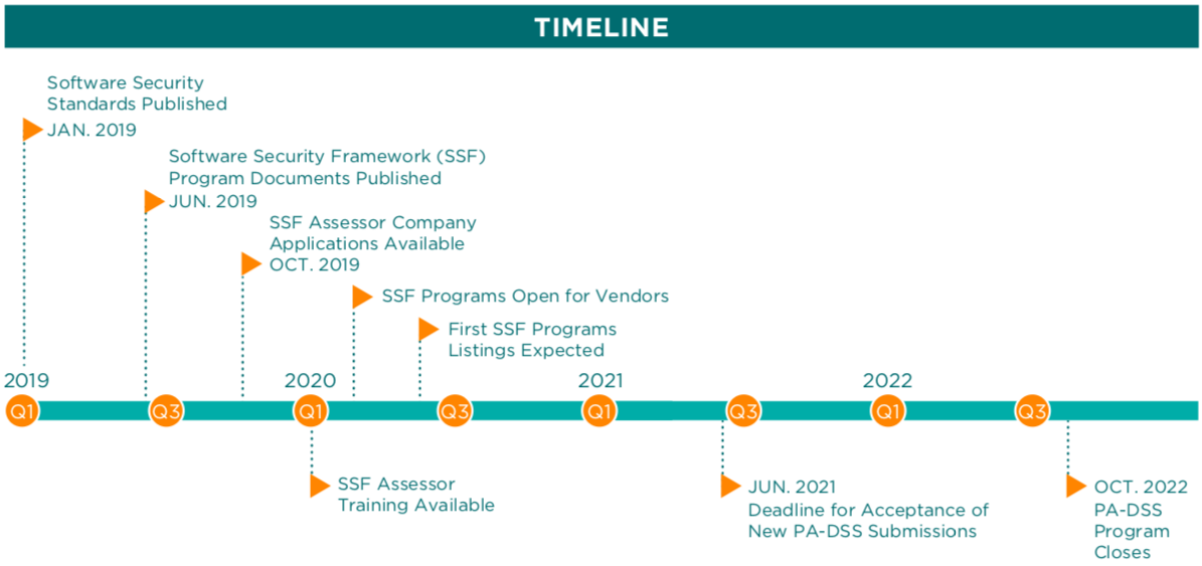

图 1：PA-DSS 到 SSF 过渡时间表（摘自 PCI SSC）

3 PA-DSS 与 PCI SSF 的比较

根据目前产业制定的标准过渡日期要求，2022年10月28日，PA-DSS将正式退出历史舞台。PCI Secure Software标准的评估目标是供应商的软件本身，是针对支付软件功能定义了一套安全需求，最终目的是为了保护支付交易与数据的机密性与完整性；PCI Secure SLC标准评估目标是软件供应商，是针对软件供应商定义了一套安全需求，以验证供应商设计、开发与交付的流程，保障支付软件在整个生命周期的安全。PCI Secure Software标准将取代PA-DSS成为确保支付软件安全的主要标准。

PCI Secure Software标准相比PA-DSS的有以下几个关键优点：

- 可评估的软件多样性增强
- 更敏捷的现代开发技术和发布周期
- 在 PCI 标准家族的不同标准中保持软件安全需求的一致性
- 增加临时软件更新的透明度
- 增加软件供应商实现 PCI 软件安全目标的灵活性和可靠性
- 在软件开发社区中除功能实现外更加强调支付安全的重要性

SSF基于PA-DSS制定和开发，然而SSF为软件供应商和评估人员提供一种比PA-DSS更灵活、更高效完成评估和验证的方法，是可用于更广泛的软件类型的安全验证。

在PA-DSS中，符合验证和列出条件的软件范围仅限于具有支付授权和结算功能的涉及持卡人数据的支付软件。PCI Secure Software标准验证可接受申请的条件已扩大到包括提供额外功能的软件，如欺诈监控或持卡人身份验证等。PCI Secure SLC标准合规的对象是供应商的软件生命周期。由于将软件安全需求和供应商安全需求分离到不同的标准中，对于不符合Secure Software标准验证条件的

软件，比如自研用于内部使用、不对外销售的支付软件，其供应商也能够通过独立的Secure SLC标准验证证明良好的软件安全性。

针对具有合格支付软件产品的软件供应商，支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）建议根据Secure Software标准和Secure SLC标准分别对其支付软件和软件开发生命周期（SLC）实践进行验证。验证这两个标准不仅表明供应商的支付软件在验证时是安全的，而且还表明该软件在其整个生命周期中都将保持安全。为了鼓励软件供应商进行这两个标准的验证，并支持更高效的评估和验证执行策略，PCI SSF提供了一个更为流线型的发布管理过程，具体内容可参考Secure Software与Secure SLC评估程序指南（参见参考文献3与4），以确保SLC合格的软件供应商使用经过验证的支付软件。这个过程使合格的软件供应商能够比以前PA-DSS支持更快地管理和发布其验证的支付软件清单的更新。

3.1 PCI SSF 的安全目标

PCI SSF安全需求被表示为安全目标，在满足标准要求方面提供了更大的灵活性。这种方法被称为“基于目标的”，并认识到通常有许多不同的方法来满足特定的安全目标。基于目标的方法使软件供应商能够选择最符合实体独特业务需求和能力的安全目标的实践和方法，而不必实现更规范的安全标准（如PA-DSS ）中规定的具体实践和方法。例如，PA-DSS要求使用特定的密码复杂度参数，如最小长度和组成，PCI Secure Software标准中相应的控制目标要求认证方法足够强大和健壮，以保护认证凭证不被伪造、欺骗、泄露、猜测，或者按照行业公认的方法进行规避。这使得软件供应商可以选择采用哪种行业认可的认证方法来满足控制目标，而不必实现PA-DSS规定的密码复杂度参数。

PCI Secure Software标准和PA-DSS的不同之处在于PCI Secure Software标准对“模块Module”概念的使用。模块是处理特定用例的需求组。

PCI Secure Software标准中有三个模块，基本信息如下：

核心模块：适用于所有类型的支付软件的一般安全要求。无论该软件的功能或基础技术如何，核心模块的要求则需要满足。	安全目标一： 将攻击面降至最低	控制目标 1：关键资产识别
		控制目标 2：安全默认
		控制目标 3：敏感数据保留
	安全目标二： 软件保护机制	控制目标 4：关键资产识别
		控制目标 5：验证和访问控制
		控制目标 6：敏感数据保护
		控制目标 7：使用加密法
	安全目标三： 安全软件操作	控制目标 8：活动跟踪
		控制目标 9：攻击检测
	安全目标四： 可靠的软件生命周期管理	控制目标 10：威胁和漏洞管理
		控制目标 11：安全的软件更新
		控制目标 12：软件供应商实施指导

模块 A - 账户数据保护模块：对存储、处理或传输帐户数据的支付软件的额外安全要求。	控制目标 A.1：敏感验证数据
	控制目标 A.2：持卡人数据保护
模块 B - 终端软件模块：对在支付终端（即 PCI 认可的 POI 设备）上部署和操作的支付软件的额外安全要求。	控制目标 B.1：终端软件文件
	控制目标 B.2：终端软件设计
	控制目标 B.3：终端软件攻击缓解
	控制目标 B.4：终端软件安全测试
	控制目标 B.5：终端软件实施指南

PCI Secure SLC标准包含以下四个安全目标：

安全目标一： 软件安全管理	控制目标 1：安全职责性和资源
	控制目标 2：软件安全政策和策略
安全目标二： 安全软件工程	控制目标 3：威胁识别与缓解方案
	控制目标 4：漏洞检测和缓解
安全目标三： 安全软件和数据管理	控制目标 5：变更管理
	控制目标 6：软件完整性保护
	控制目标 7：敏感资料保护
安全目标四： 安全通信	控制目标 8：软件供应商实施指引
	控制目标 9：利益相关者沟通
	控制目标 10：软件升级信息

3.2 PA-DSS 与 PCI Secure Software 标准的异同

PCI Secure Software标准扩展了最初在PA-DSS中引入的保护支付应用程序和数据的关键原则，旨在支持一组更大的支付软件架构、功能和软件开发方法。为了更好地理解PA-DSS和PCI Secure Software标准的关系，将两者进行对比是很有帮助的。需要注意的是，在两个标准的安全需求中没有一对一直接对应。这两个标准都是为了促进和解决应用程序和软件设计与开发的安全。

●PA-DSS 和 PCI Secure Software 标准相似性

PA-DSS	PCI Secure Software 标准
旨在促进安全的支付应用程序；	旨在促进安全的软件；

解决安全应用设计与开发；	解决安全应用设计与开发；
支持一个实体的 PCI DSS 合规，但不能保证实体的 PCI DSS 合规。	支持一个实体的 PCI DSS 合规，但不能保证实体的 PCI DSS 合规。

●PA-DSS 和 PCI Secure Software 标准差异性

PA-DSS	PCI Secure Software 标准
单一架构；	模块架构；
主要是根据传统 POS 系统开发的；	旨在支持更广泛的软件类型和平台；
明确地开发以支持 PCI DSS；	支持 PCI DSS，但设计为完全独立（无耦合）；
软件设计和软件开发都在同一标准中处理；	同时处理软件设计和开发，但采用不同的标准；
指定的需求；	基于目标的需求；
有限的可伸缩性。	可伸缩性设计。

经过PA-DSS验证的应用程序的供应商可能需要升级他们的软件或软件开发实践，以满足适用的PCI Secure Software标准需求。SSF体系进一步完善了PA-DSS验证体系多年所积累的价值。考虑到现代软件的日益复杂和现代软件被攻击的复杂性，PCI Secure Software标准包含PA-DSS中没有包含的额外需求（比如目前Module B的引入，以及后续会扩展更多的模块）。

4 SSF 评估流程和验证方法概述

如3.1中所述Secure Software标准包括一套“核心”要求，适用于在PCI软件安全框架下提交验证的所有类型的支付软件，无论软件的功能或底层技术如何。Secure Software标准的当前版本包括一个账户数据保护“模块”，一个终端软件“模块”，如果支付软件不拥有特定的数据或功能，或者不利用触发模块适用性标准的技术，则相应模块内的需求将不作为软件验证的一部分进行评估。将来，还将向安全软件标准添加额外的模块，以处理其他软件类型、用例或技术。atsec也将和产业标准化组织、厂商等积极沟通和交流，致力于新的模块或者标准发展的相关工作，为支付产业进一步做出我们的贡献。

4.1 SSF 评估流程

●Secure Software 标准评估步骤：

- 供应商与 Secure Software 评估实验室签订合同及保密协议
- 确定评估范围与适用的标准要求
- 提交所需要的文档和材料给评估实验室
- 实验室审核人员检查文档、访谈人员、执行相关的测试
- 评估人员记录发现、验证控制
- 评估人员完成 ROV 与 AOV 文档
- 供应商与评估人员签署 AOV

- 评估人员将 ROV、签署的 AOV 与 VRA（Vendor Release Agreement）提交给（支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）
- 供应商支付接受费用给 PCI SSC
- PCI SSC 审核提交的材料、接受和认可 ROV，并添加供应商软件到验证列表

●Secure SLC 标准评估步骤

- 供应商与 Secure SLC 评估实验室签订合同及保密协议
- 确定评估范围与适用的标准要求
- 提交所需要的证据给评估实验室
- 实验室审核人员检查证据、观察流程、访谈人员
- 评估人员记录发现、验证控制
- 评估人员完成 ROC 与 AOC 文档
- 供应商与评估人员签署 AOC
- 评估人员将 ROC、签署的 AOC 与 VRA（Vendor Release Agreement）提交给 PCI SSC
- 供应商支付费用给 PCI SSC
- PCI SSC 审核提交的材料、接受和认可 ROC，并添加软件供应商到验证列表

评估流程可参考如下示意图：

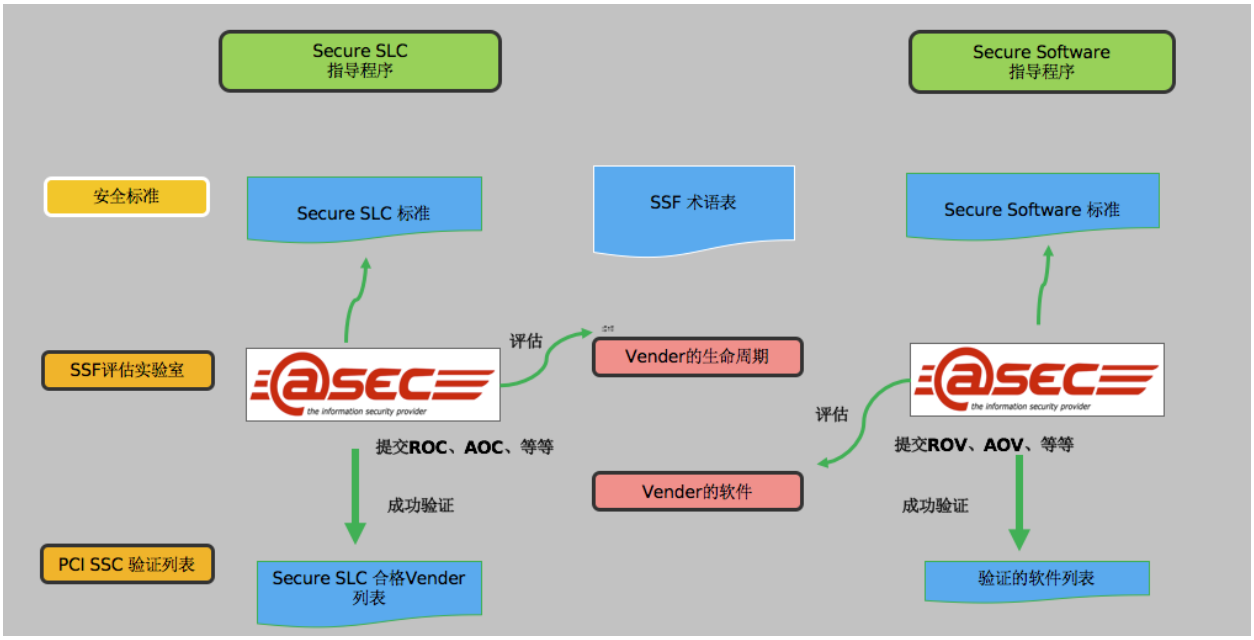

图 2：SSF 评估流程

4.2 PCI Secure Software 标准验证方法

供应商与Secure Software评估实验室签订合同及保密协议后，Secure Software评估人员将收集和分析被评估的支付软件信息，收集的信息包括但不限于以下内容：

- 支付软件名称、版本号、支持的操作系统以及任何硬件或软件要求；
- 功能设计和技术设计文件，包括支付软件数据处理过程、设计模式、数据记录和错误处理行为；
- 支付软件组件的描述；
- 密钥管理操作；
- 与支付软件和开发工具相关的第三方依赖列表；
- 实验室测试可能需要的软件测试工具列表；
- 用于数据处理的软件测试脚本描述和软件测试环境文档。

之后将对收集的信息进行审核，审核支付软件功能，包括端到端的支付功能、输入和输出函数、错误条件、接口、数据流、加密功能、身份验证机制，以及与其他适用文件/系统和组件的连接。与相关人员进行访谈，包括但不限于系统架构师、应用程序开发人员、数据库开发人员、系统管理员、质量保障（QA）、测试人员等。

Secure Software标准验证将在评估实验室或客户现场进行，具体视情况而定。评估实验室将对支付软件进行静态和动态分析，包括使用自动化工具和手动测试技术。该测试包括代码审查、漏洞扫描和渗透测试。

5 结束语

PCI SSF是传统和现代软件安全需求的结合，支持新技术、更广泛的软件类型和开发方法。此外，为了适应不断变化的威胁环境，新标准帮助供应商构建针对新威胁的强大防御。PCI SSF更加侧重于安全实践，可以支持良好应用程序安全性的传统方法和最新的开发实践。相关供应商需要了解SSF与PA-DSS的差别，以便采取相应的措施和必要的步骤，重组业务运营和相关活动，避免给业务发展带来的影响。

目前atsec的SSF软件安全评估人员已经经过了产业的考核，可以提供所有已经发布模块的软件产品的评估服务。

6 参考文献

[1] PCI Secure Software Standard. https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_1.pdf

[2] PCI Secure SLC Standard. https://www.pcisecuritystandards.org/documents/PCI-Secure-SLC-Standard-v1_1.pdf

[3] PCI Secure Software Program. https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Program-Guide-v1_1.pdf

[4] PCI Secure SLC Program. https://www.pcisecuritystandards.org/documents/PCI-Secure-SLC-Program-Guide-v1_1.pdf

[5] Transitioning from PA-DSS to the PCI Software Security Framework. https://www.pcisecuritystandards.org/documents/Transitioning_from_PA-DSS_to_SSF_Resource_Guide.pdf

[6] How to successfully transition software from PA-DSS to the PCI Secure Software Standard. https://blog.pcisecuritystandards.org/

[7] atsec website. https://www.atsec.com/