PCI 安全软件标准 v2.0 解读

作者：atsec 张力

关键词：敏感资产、SAID、SBOM、SDK、Delta 变更、安全软件

atsec information security

Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.com

目录

1 引言

2026 年 1 月，PCI 安全标准委员会（PCI SSC）正式发布了 PCI Secure Software 标准 v2.0 版本及其配套体系指南（Program Guide）。这是该标准自 2019 年推出以来的首次重大修订。

v2.0 并非对 v1.2.1 的增量更新，而是一次全面的结构性重组。此次修订标志着 PCI 安全软件标准从规范性“支付软件”分类向以“敏感资产保护”为中心的原则性方法转型，代表了软件安全理念的进一步成熟。以下系统梳理此次版本变更的核心内容。

2 核心概念的根本性转变：“支付软件”让位于“敏感资产”

2.1 术语移除与概念重塑

v2.0 最根本性的变革在于彻底移除了“支付软件”（Payment Software）这一术语，代之为“敏感资产”（Sensitive Assets）的核心概念。敏感资产被定义为软件产品中任何未经授权访问、使用、修改或披露可能导致支付处理或支付相关数据安全受损的元素，包括软件产品本身。

这一转变意味着标准的适用范围从狭隘的“支付类应用”扩展到更广泛的“敏感资产”保护理念，反映了软件安全在当今互联数字环境中的演进。

2.2 强制性配套文件：敏感资产识别（SAID）

为支持这一框架，标准同步发布了强制性的敏感资产识别文件（Sensitive Asset Identification），要求软件厂商系统性地识别和记录其软件中的四类敏感资产：

资产类别	说明
敏感数据（Sensitive Data）	需保护的支付相关数据
敏感资源（Sensitive Resource）	系统资源层面的保护对象
敏感功能（Sensitive Functionality）	涉及支付处理的关键功能
敏感操作模式（Sensitive Modes of Operation）	需特殊保护的操作场景

该文件并非可选参考文档，而是 PCI 安全软件计划的必要组成部分。对于处理 EMVCo 3DS 相关数据的供应商，标准还引用了 PCI 3DS 数据矩阵文档。

2.3 术语表内化

v2.0 将术语表从外部 SSF 文档移至标准本身的附录 A，所有已定义的术语在安全要求中均有标记以便识别。同时引入了新术语“强认证”（Strong Authentication），并将密码学要求的基准统一为“强密码学”（Strong Cryptography），取代了之前依赖特定有效密钥强度参数的做法。

3 标准结构的重组：从控制目标到安全目标

3.1 11 个安全目标取代控制目标

v2.0 将标准要求全面重组为 11 个安全目标（Security Objectives），取代了原有的控制目标（Control Objectives）术语。这一调整使标准结构更加清晰、逻辑更加连贯。

11 个安全目标覆盖了从架构设计到部署管理的完整生命周期：

编号	安全目标	核心要点
目标 1	软件架构、组合和版本控制	包括软件物料清单（SBOM：Software Bill of Materials）、版本控制实践及通配符使用
目标 2	敏感资产识别	依赖 SAID（Sensitive Asset Identification Document）配套文件，涵盖四类敏感资产的识别
目标 3	敏感资产的存储和保留	存储与保留的安全控制
目标 4	敏感操作模式	引入“强认证”要求，适用于存在敏感操作模式的场景
目标 5	敏感资产保护	将软件设计本身视为敏感资产，引入“异常行为”概念
目标 6	敏感资产输出	正式确立安全通道要求
目标 7	随机数	涵盖外部 RNG 使用与内部 RNG 实现
目标 8	密钥管理	密钥全生命周期管理
目标 9	密码学	涵盖其他领域未覆盖的综合性密码学要求
目标 10	威胁和漏洞	威胁建模与漏洞管理
目标 11	安全部署和管理	包括实施指南和软件版本控制

3.2 测试方法的三支柱重构

v2.0 将所有测试需求围绕三种核心方法进行了重写：

- 文档审查（Documentation Review）：评估安全策略和设计记录。
- 静态分析（Static Analysis）：在不运行代码的情况下检查代码漏洞。
- 动态分析（Dynamic Analysis）：在软件运行时观察其行为，以确保其能够正确处理正常输入和恶意输入。

3.3 强制性源代码审查

标准中明确规定：软件供应商应根据评估人员的需要，提供其被评估软件产品的源代码。如果没有提供相关的源代码，软件产品将无法按照此标准进行评估。源代码提供从隐含要求升级为明确的强制性要求。

4 模块体系的演进与扩展

4.1 核心部分更名与精简

原“核心”部分更名为“核心——所有软件”，以强调这些要求普遍适用于根据该标准评估的所有软件。标准已删除与 SLC 相关的要求，因为这些内容现已纳入 PCI Secure SLC 标准。

4.2 模块 A：账户数据保护

要求已修订为仅聚焦于 PCI DSS 中的 PAN（Primary Account Number）和 SAD（Sensitive Authentication Data），SAID 文档提供了更多背景信息。

4.3 模块 B：POI 设备软件

原“终端软件需求”更名为“POI 设备软件”（Point of Interaction 设备软件），需求大幅精简。多项原属模块 B 的要求（B1.1、B1.2、B1.3、B3.x、B5.x）已并入核心部分，SRED（Secure Reading and Exchange of Data）需求同步修订。

4.4 模块 C：公开可访问软件

原“Web 软件需求”更名为“公开可访问软件”（Publicly Accessible Software），以更准确地表达其适用于任何可通过公共网络访问的软件。原 C.1 部分的多项要求已移至核心部分，C.1.5 和 C.1.6 因已包含在 PCI Secure SLC 标准中而被移除。

4.5 模块 D：软件开发工具包（SDK）（新增）

这是 v2.0 最重要的新增内容之一。模块 D 专门针对 SDK 评估引入了全新的安全目标和要求。

该模块的推出使得 v2.0 能够对 SDK 进行通用评估，包括 EMVCo 3DS SDK。PCI SSC 计划最终用安全软件标准 v2.0 及后续版本取代独立的 PCI 3DS SDK 标准，因为安全软件标准更加客观，能为所有安全软件供应商（包括 3DS SDK 供应商）提供更大的灵活性。

5 变更流程的重构

v2.0 对变更管理体系进行了较为全面重构。在 v1.x 版本中，变更已确立管理变更（Administrative Change）、低影响变更（Low Impact Change） 和高影响变更（High Impact Change） 三大类别。v2.0 在此基础上进行了重新梳理与细化，正式移除了“低影响变更”和“高影响变更”的表述，代之为管理变更、通配符合格变更（Wildcard Eligible Changes） 和两级 Delta 变更（Tier 1 / Tier 2 Delta Changes） 的新体系。这一调整旨在使变更评估流程更加精简、清晰和易于管理，降低软件厂商在维护已验证产品时的合规负担。

v2.0 将所有变更划分为以下三大类别：

变更类别	核心特征	是否需要提交 PCI SSC
管理变更（Administrative Change）	仅更新已列出的通过验证的安全软件产品的供应商公司名称或产品名称。	需要，通过 Portal 提交。
通配符合格变更（Wildcard Eligible）	对已验证产品的非安全影响变更，且版本号中使用已验证的通配符。 通配符不能用于属于 Delta 变更（Tier 1 或 Tier 2）的软件变更。	不需要
Tier 1 Delta 变更	非安全影响的版本号变更（未使用通配符）；或 SSLC（Secure SLC）合格供应商的安全漏洞修复/补丁。	SSLC 合格供应商无需评估人员介入；非 SSLC 合格供应商需评估人员进行评估，评估结果通过 Portal 提交。
Tier 2 Delta 变更	安全影响的变更（含引入新敏感资产类型、修改依赖项等 8 类情形）。	必须使用评估人员进行评估，评估结果通过 Portal 提交。

6 安全要求的显著强化

6.1 软件物料清单（SBOM）强制化

标准要求强制提供软件物料清单（SBOM）并对软件架构进行完整文档化。

6.2 敏感操作模式的多因素认证

对敏感操作模式强制实施多因素认证（MFA/强认证）。

6.3 日志与监控增强

- 生成的日志需要更细粒度
- 导出的日志必须加密
- 必须生成并加密可疑事件日志

7 过渡期安排

PCI SSC 已于 2026 年 1 月 16 日发布的技术常见问题解答中明确了过渡期安排：

12 个月的共存期：v1.2.1 和 v2.0 均可用于向 PCI SSC 提交评估和申请。

v1.2.1 版本的截止日期：

- 完整的评估报告提交截止日期为 2027 年 4 月 30 日
- 提交材料必须在 2027 年 7 月 31 日之前通过 PCI SSC 的质量管理流程（AQM）
- 根据 v1.2.1 版本审核通过并上架的产品，其上架有效期为 3 年
- ROV v1.x 和 AOV v1.x 将继续使用

v2.0 版本的启用：

- v2.0 评估将在安全软件评估员完成新版本培训后开放
- 自 2027 年 5 月 1 日起，所有已验证安全软件产品的新全面评估必须使用 v2.0
- 增量变更须使用 ROV v2.x、AOV v2.x 和新的变更影响模板

重要澄清：2.0 版本不会影响已在 1.x 版本标准下列出的产品的年度重新验证日期或重新评估日期。对于已通过 v1.2.1 验证的产品，年度重新验证和定期重新评估义务将继续按照既定时间表执行。

8 总结

PCI 安全软件标准 v2.0 标志着该框架的根本性成熟，其核心变化集中体现了从规范性“支付软件”分类向以“敏感资产保护”为中心的原则性方法转型。这一转型以“敏感资产”概念全面取代“支付软件”为起点，并配套发布强制性的敏感资产识别文件作为评估基础。在标准架构层面，v2.0 以 11 个安全目标取代原有的控制目标，并将测试方法重构为文档审查、静态分析和动态分析三大支柱；在适用范围上首次新增模块 D 将 SDK 纳入评估，涵盖 EMVCo 3DS SDK。变更管理流程得到系统化精简，以两级 Delta 变更取代原有的低/高影响分类，同时正式化通配符版本管理以降低非安全变更的行政负担。安全要求层面显著强化，包括 SBOM 和源代码审查的强制化，以及对敏感操作模式实施多因素认证。在此基础上，已通过 Secure SLC 认证的供应商在 Tier 1 Delta 变更中享有自我证明的程序性便利，进一步优化了维护成本与响应效率。

atsec 将凭借丰富的 PCI 安全软件评估经验和专业技术团队，深入解读新版标准在敏感资产识别、SDK 评估、安全架构文档化等方面的核心要求，协助客户完成从 v1.2.1 到 v2.0 的平稳迁移，在全新的安全框架下持续提升软件产品的安全水平。

9 参考文献

[1] PCI-Secure-Software-Standard-v2.0. https://docs-prv.pcisecuritystandards.org/Software%20Security/Standard/PCI-Secure-Software-Standard-v2.0.pdf

[3] PCI-Secure-Software-Program-Guide-v2.0. https://docs-prv.pcisecuritystandards.org/Software%20Security/Program%20Documents/PCI-Secure-Software-Program-Guide-v2.0.pdf

[4] PCI-Secure-Software-Standard-Sensitive-Asset-Identification_v1.0. https://docs-prv.pcisecuritystandards.org/Software%20Security/Standard/PCI-Secure-Software-Standard-Sensitive-Asset-Identification_v1.0.pdf

[5] PCI-Secure-Software-Standard-v2.0-Summary-Of-Changes. https://docs-prv.pcisecuritystandards.org/Software%20Security/Standard/PCI-Secure-Software-Standard-v2.0-Summary-Of-Changes.pdf

[6] Secure Software v2.x Technical FAQs. https://docs-prv.pcisecuritystandards.org/Software%20Security/Standard/PCI-SecSW_v2.x_TechFAQs_June2026.pdf

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