PA DSS 3.0 标准更新解读

作者：张力（atsec 中国）

2015 年 4 月 8 日

关键词：PCI -DSS、PA-DSS、安全评估

atsec (Beijing) Information Technology Co., Ltd

Floor 3, Block C, Building 1, Boya C-Center,
Beijing University Science Park, Life Science Park,
Beijing, P.R.China. 102206
Tel: +86 10 5305 6680
Fax: +86 10 5305 6678
www.atsec.com

1. PCI-DSS标准家族介绍

如我们所知，PCI-DSS标准家族主要由三部分组成，分别是PCI-DSS（Payment Card Industry Data Security Standard）、PA-DSS（Payment Application DataSecurity Standard）与PTS（PIN Transaction Security），PCI-DSS标准主要关注于持卡人数据环境的安全，PTS关注于ATM或POS机进行支付交易处理时PIN码及其相关密钥的保护，而PA-DSS则关注于整个支付应用软件的安全，使其更容易地部署在持卡人数据环境中，以支持持卡人数据环境合规于PCI-DSS的安全要求。

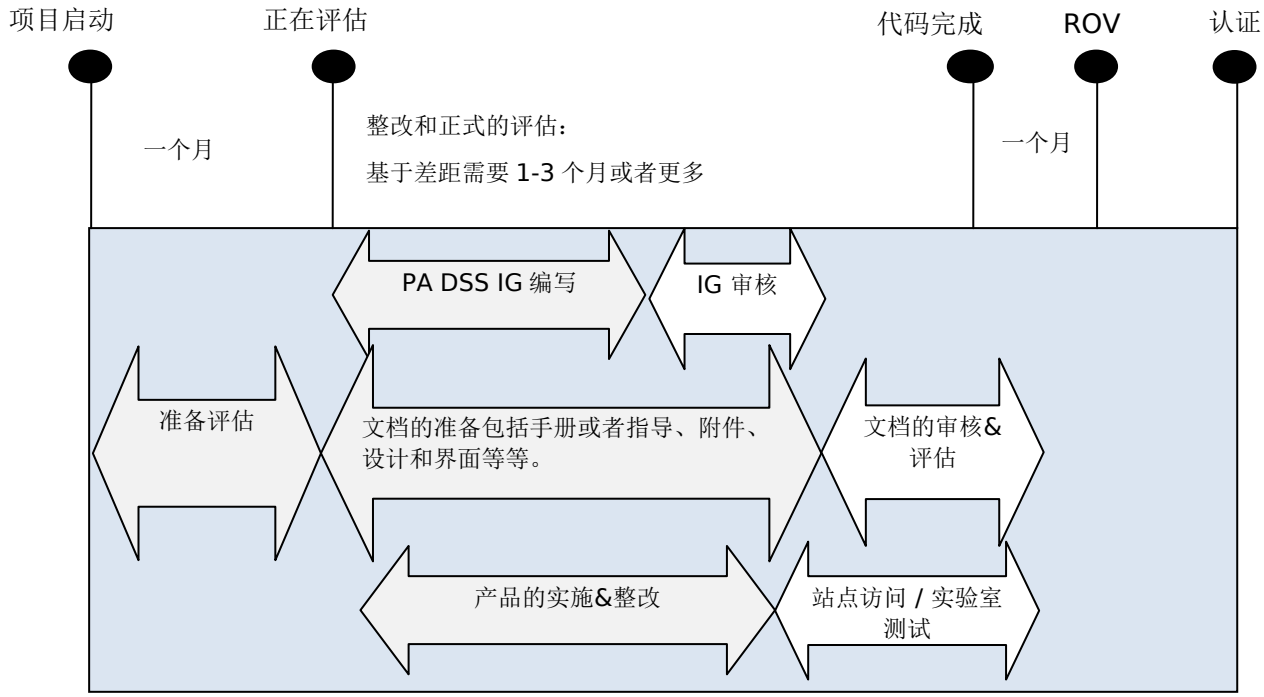
2. PA-DSS 3.0 适用场景

如果商用的支付应用软件存储、处理或传输持卡人数据，并且将其作为授权或结算操作的部分，则适用于PA-DSS标准。

支付应用类型	PA-DSS 适用吗?
非定制的商用支付应用软件	适用
支付应用模块	适用 注：通常是基于最佳实践的考虑，将支付功能集中到一个或少量的基本模块，而其他模块执行非支付功能。
支付应用是提供给客户的一种服务，为服务提供商所拥有。客户没有能力管理、安装或控制这种支付应用或它的环境。这种支付应用不被销售或授权给第三方。	不适用 注：此种支付应用应由服务提供商自己的PCI-DSS审核所覆盖。
为某一客户定制开发的支付应用	不适用
由商户或服务提供商开发内部使用、不销售给第三方的支付应用	不适用 注：此种支付应用应由商户或服务提供商自己的PCI-DSS审核所覆盖。
安装支付应用的支持系统，比如数据库、操作系统、平台系统等。	不适用

3. PA-DSS评估简介

如下图所示，PA-DSS评估大体可以分为四个阶段。第一个阶段是准备评估阶段，atsec开发了完整先进的准备评估的方法论，可以协助客户明确支付应用的审核边界，并共同识别差距，提出详细的整改建议。第二个阶段是基于差距的整改以及实施指南IG（Implementation Guide）的编写，这个阶段的周期通常根据支付应用的现状差距和整改的工作量等因素有所不同。第三个阶段是正式评估阶段，具有资质的评估人员QSA将开展全面的合规评估，之后出具ROV（Report On Validation）报告和AOC (Attestation Of Validation)证明。第四阶段是提交IG、ROV与AOC给PCI标委会审核，审核通过后PCI标委会将通过PCI官网发布认证结果。



图：PA-DSS 评估参考示意

4. PA-DSS 3.0 相对2.0的更新

PCI安全标准委员会于2014年初发布了PA-DSS 2.0的更新版本PA-DSS 3.0，相比PA-DSS 2.0，PA-DSS 3.0做了一些重要的变化与补充以适应不断发展的风险管理，融入了安全的最佳实践。在PCI 安全标准委员会的官方网站上，有一个标题为“PA-DSS 2.0到3.0变化概要”的文档，包含了标准变化有价值的信息。PA-DSS 3.0增加了一些新的要求，取消了一项旧的要求，并对其中的一些要求做了改进。为了您理解方便，这里对标准变化做一简要的总结。

增加的要求：

要求 3.4：支付应用必须限制对必需功能/资源的访问并对内置应用程序帐户执行最小权限。

应用程序安装需要确保其使用或设置了所需的权限，而没有给予额外的许可。这适用于内置帐户和服务帐户。确保你已文档化了任何缺省或服务帐户所需的权限。审核员需要验证这些文档，以验证相应的实现。

要求 5.1.5：支付应用开发人员验证整个开发过程中源码的完整性

需要确保所有的源码控制工具（例如SVN、SourceSafe、ClearCase等）被配置为仅相关开发人员能更改代码，这不排除给予某些人读的访问权限，但是需要最小化写的访问权限。

要求 5.1.6：根据安全编码技术的行业最优方法开发支付应用程序。

必须用最小特权来开发应用以确保不安全的假设不被引入到应用。为了防止攻击者获取关于应用程序故障的敏感信息，以便用来创建后续攻击。还必须确保安全应用于所有的访问和对应用的输入，以避免输入通道被破坏。这包括敏感数据和PAN在内存中怎样被处理，尝试在内存中加密这些数据与保持它在内存仅很短的一段时间。

要求 5.2.10：失效的验证和会话管理

- 将会话令牌（如 cookie）标记为“安全”
- 不要暴露 URL 中的会话ID

- 成功登录后添加适当超时和轮换会话 ID

要求 5.4：支付应用程序供应商必须将软件版本控制方法作为系统开发生命周期的一部分来进行记录和遵循。

要求 5.5：在软件开发流程中使用风险评估技术（例如，应用程序威胁建模）来识别潜在的应用程序安全设计攻击和漏洞。

要求 5.6：软件供应商必须实施流程来记录和授权应用程序和任何应用程序更新的最终发布。

要求 7.3：所有应用程序更新应包含发布说明，包括该更新的详情及影响，以及版本号的变更如何体现应用程序的更新。

要求 10.2.2：如果供应商或集成商/经销商可以对客户的支付应用程序进行远程访问，则必须使用每个客户独有的验证凭证（例如密码/口令）。

要求 13.1.1：向客户、经销商和集成商提供适用于其所使用应用程序的相关信息。

要求 14.1：每年向负责PA-DSS 的供应商工作人员提供至少一次有关信息安全和PA-DSS 的培训。

要求 14.2：向供应商工作人员分配角色和职责，包括以下各项：

- 全面负责满足 PA-DSS 的各项要求
- 与 PCI SSC《PA-DSS 计划指南》的变更情况保持同步
- 确保遵循安全编码实践
- 确保集成商/经销商接受培训并获得配套材料
- 确保所有负责 PA-DSS 的供应商工作人员（包括开发人员）接受培训

删除的需求：

要求 2.4：如果磁盘加密被使用（而不是文件加密或级别的数据库加密），逻辑访问必须单独管理以独立于本地操作系统的访问控制机制（例如，不使用本地用户帐户数据库）。解密密钥不能关联到用户帐户。

改进的需求：

要求 3.3.2：使用强效单向加密算法，基于许可标准使所有支付应用程序密码在存储期间不可读。

在应用加密算法之前，每个密码都必须组合一个唯一的输入变量。看来，加密的密码是不可接受的。在你的应用程序，你必须使用一个强的、单向加密算法（hash）与盐值。审核你的应用存储以确保您使用的是带盐的哈希算法。

要求 4.2.5：支付应用程序必须提供自动检查记录以便重建事件“通过root 权限或管理员权限对应用程序的身份识别和验证机制（包括但不限于创建新帐户、提升权限等）进行使用和更改，并对应用程序帐户进行任何更改、增加、删除。”

5. 结束语

支付应用软件在处理、传输与存储持卡人数据中扮演着非常重要的角色，PA-DSS标准为商户或收单机构在选择支付应用软件时提供了全球级别的安全评判标准，通过PA-DSS认证的支付应用软件将大大降低了商户环境中数据违背的风险，也为整个持卡人数据环境获得与维护PCI-DSS合规认证提供了保障。

参考文档和链接

[1] PA-DSS Requirement and Security Assessment Procedures Version 3.0

[2] PA-DSS Summary of changes v 2.0 to v3.0

[3] QSA Validation Requirements - PA-QSA

[4] PA-DSS Program Guide Version 3.0