适用于应用软件的 PCI DSS 合规要求

作者：atsec 高向东，转载请注明文章出处以及作者信息

本文所指的应用软件，最直接适用的情况是支付环境中处理持卡人数据（CHD: Cardholder Data）/敏感认证数据（SAD: Sensitive Authentication Data）的、机构自行开发或通过外部资源开发的软件。在应用软件不涉及 PCI DSS 所关注的持卡人数据/敏感认证数据的情况下，也推荐借鉴本文所梳理的要求点进行数据安全保护方面的工作。

在机构需要合规支付卡产业数据安全标准（PCI DSS: Payment Card Industry Data Security Standard）时，往往较难梳理清楚机构内部的各种应用软件适用于哪些要求点。从 PCI DSS 标准的章节安排来看，也很难准确定位哪些 PCI DSS 要求点是需要从应用开发和设计角度需要关注的。因此，atsec 作者基于对现行 PCI DSS 标准 V3.2.1 的理解，对相应的具体要求进行了梳理和汇总，以体系化的方法来展现应用软件合规所需要重点关注的技术要求。

此外，支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）发布了软件安全框架（SSF：Software Security Framework）体系的两个标准，一个是安全生命周期（Secure SLC）标准，旨在面向支付产业开发软件的软件供应商，验证其生命周期的实践。该标准为支付软件供应商提供了安全要求，以便在整个软件生命周期中整合安全性，从而使软件在设计上是安全的，并且能够抵御攻击。另一个是安全软件标准（Secure Software Standard），该标准规定了构建安全支付软件的安全要求，以保护与支付交易相关的存储、处理或传输的敏感数据的完整性和机密性。他们和 PCI DSS 相辅相成可以作为软件开发机构的最佳实践，必要时也建议获得 atsec 的评估以及针对软件产品本身的产业验证。本文将主要基于 PCI DSS 的软件开发合规要求进行展开。

1 应用软件对持卡人数据与敏感认证数据的存储要求

1.1 支付授权后不存储敏感认证数据

PCI DSS 的根本要求，是不允许在授权完成后存储敏感验证数据。例外的情况是发卡机构/支持发卡的处理商在有明确需要的情况下进行最小化存储。

PCI DSS 要求 3.2：授权之后，不要存储敏感验证数据(即使已加密)。如果收到敏感验证数据，在完成验证流程后使所有数据不可恢复。

应通过对应用软件及技术架构的了解，识别每个数据存储的位置，包括但不限于：

- 输入的交易数据
- 所有日志(例如交易、历史、除错、错误)
- 存档文件
- 跟踪文件

• 几种数据库架构
• 数据库内容。

PCI DSS 要求 3.2.1 切勿在授权后存储卡片背面磁条上任何磁道的完整内容、芯片或其他地方上的等效数据。此类数据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。

PCI DSS 要求 3.2.2 切勿在授权后存储用于确认无实卡交易的卡验证代码或值(印在支付卡正面或背面的三或四位数值)。

PCI DSS 要求 3.2.3 授权后，请勿存储个人识别码（PIN）或经加密的 PIN 数据块。

1.2 落实持卡人数据的识别、最小化及业务必要性论证的流程

对于这个流程，首先需要梳理和识别出每个数据存储的位置，包括但不限于上述提及的位置。然后，对每个位置做最小化处理和业务必要性论证，仅在必要的位置存储持卡人数据且该位置的存储是业务所必须的。最后，需要每季度梳理过期的持卡人数据，并使用安全（不可恢复）的机制进行删除。

PCI DSS 要求 3.1 通过实施数据保留和处理政策、程序和流程最大限度地减少持卡人数据存储，对所有持卡人数据（CHD）存储而言，这些政策、程序和流程至少应包含以下方面:

- *将数据存储量和保留时间限制在法律、法规和/或业务要求的范围内。*
- *持卡人数据的具体保留要求。*
- *不再需要时安全删除数据的流程。*
- *按季度查找并安全删除所存储的超过规定保留期限的持卡人数据的流程。*

1.3 对需要存储的持卡人数据进行存储保护

如果论证后是需要存储持卡人数据的，建议优先使用截断、哈希或令牌化的方法进行保护。如需要还原真实卡号，则使用强加密的方法进行存储保护。

PCI DSS 要求 3.4 通过采取下列任一方法使所有位置(包括便携式数字媒介上、备份媒介上和日志中)存储的 PAN 均不可读:

- *基于强效加密法的单向散列函数(散列必须要有完整的 PAN)。*
- *截词(不能用散列代替 PAN 被截词的部分)。*
- *索引令牌与索引簿(索引簿必须安全地存储)。*
- *具有相关密钥管理流程和程序的强效加密法。*

在使用强加密手段进行保护的情况下，则需要机构落实一整套完整的加密密钥管理体系、流程和方法对加密机制进行管理。通常情况下，可借助于加密机进行实现。业界也存在使用密钥管理系统（KMS）进行管理的情况。无论是哪种情况，具体要求请参考 3.4.1-3.6.8 的要求。

2 应用软件对持卡人数据与敏感认证数据的访问要求

2.1 以掩盖的形式显示全卡号

对于持卡人数据展示给内外部人员时，需要以掩盖（来自 VISA 最佳实践要求：卡 BIN 和后 4 位）的形式。如因业务的必要性需要展示卡号的更多信息时，需要将正当业务访问的人员及显示的位置最小化。需要提醒的是，如果应用界面涉及下载、打印、导出含全卡号的信息，也需要进行掩盖处理。

PCI DSS 要求 3.3 显示 PAN 时予以掩盖(最多显示前六位和后四位数字)，以便仅限具有正当业务需要的工作人员查看除前六位/后四位以外的 PAN。

2.2 对持卡人数据的访问进行记录

PCI DSS 要求对持卡人数据的访问（包括但不限于查询、修改、删除等）应被记录下来。记录的要求点如下：

PCI DSS 要求 10.2 对所有系统组件实施自动检查记录以重建以下事件:
PCI DSS 要求 10.2.1 对持卡人数据的所有个人用户访问。

3 应用软件对持卡人数据与敏感认证数据的传输要求

3.1 区分公共网络和非公共网络传输

对于非公共网络（如内部网、专线、电话线等），不强制但建议使用强加密算法进行传输保护。对于公共网络传输（互联网、GRPS 等），则要求传输过程中的数据必须是强加密保护。标准原文中对开放式公共网络的举例如下：

- 互联网
- 无线技术，包括802.11和蓝牙
- 蜂窝技术，例如，全球移动通信系统(GSM)、码分多址 (CDMA)
- 通用分组无线业务(GPRS)
- 卫星通信

具体可接受的实现方式包括数据包完整加密、应用层协议内加密、仅加密持卡人数据/敏感认证数据。加密算法中，应确认数据传输所用的加密算法是强算法。对于涉及到开放式公共网络，具体要求点如下：

PCI DSS 要求 4.1 使用强效加密法和安全协议来保护经由公开、公共网络传输的敏感持卡人数据，包括:
- *只接受可信的密钥和证书。*
- *使用的协议只支持安全的版本或配置。*
- *加密强度适合所使用的加密方法。*

3.2 常见传输协议的安全传输设置

3.2.1 HTTP 协议的传输安全

如传输中使用的是 HTTP 协议，需要确认公共网络链路中的持卡人数据/敏感认证数据是使用强加密算法保护，比如在 HTTP 协议的应用层实现的传输加密控件等。

3.2.2 HTTPS 协议的传输安全

如传输中使用的是 HTTPS 协议，需要确认使用了第三方可信的证书。需要确认仅支持 TLS1.2/TLS1.3 版本，不支持 TLS1.0/TLS1.1/SSL3.0/SSL3.0 等不安全版本。需要确认对应的加密套件，确认传输加密部分的协议是强加密算法，套件的其它部分推荐使用 DHE 密钥交换方式，推荐 SHA 256/512，不建议出现 MD5,SHA1,RSA,3DES 算法。

3.2.3 IPSEC VPN 协议的传输安全

如传输中使用 IPSEC VPN 协议，需要确认传输用的加密算法是强算法。不要出现 IKE V1 和

野蛮模式，不要出现 DH group 1/2/5。

3.2.4 FTP/SFTP 协议的传输安全

如内部或公网传输中出现 FTP 协议，因 FTP 涉及明文密码传输，不允许用于 CHD/SAD 传输。除非对该协议进行了密码传输的改造。

如内部或公网传输中出现 SFTP 协议，需要确认至少公共网络传输的 CHD/SAD 是强加密保护的。如使用 SFTP 协议本身的加密，需要确认到具体的加密算法的配置，均使用强加密算法。同时，如果涉及到 SFTP 客户端自动进行传输的情况，需要确认 SFTP 客户端的密码进行了强加密保护（至少不能出现密码明文的出现在 SFTP 客户端中）。

3.2.5 即时消息协议

基于 PCI DSS 的要求，不允许使用即时通讯等方式传输明文的卡号。通常的做法是进行加密、截断、哈希等方面的处理。

PCI DSS 要求 4.2 不要使用终端用户通讯技术(例如，电子邮件、即时通讯、短信、聊天等)来传送不受保护的 PAN。

4 应用软件的用户认证与密码保护

如果应用软件涉及人机交互的界面，在用户的认证中，能常会涉及到用户帐号及密码的管理。

4.1 用户帐号和密码的管理

对于帐号，需要分配唯一的 ID 且可以追溯至个人。同时，需要对帐号的增删改查进行管理。另外，如果帐号用户长时间（90 天内）不活动，应禁用/删除该帐号。具体要求点如下：

PCI DSS 要求 8.1.1 允许用户访问系统组件或持卡人数据之前，为其分配唯一 ID。
PCI DSS 要求 8.1.2 控制添加、删除和修改用户 ID、凭证和其他标识符对象。
PCI DSS 要求 8.1.3 立即撤销到期用户的访问权限。
PCI DSS 要求 8.1.4 在 90 天内删除/禁用非活动的用户帐户。

4.2 密码的存储与传输保护

如果应用软件涉及机机交互的密码认证，需要确保应用的发起端与接收端的密码在传输中是被强加密保护。同时，须确保使用强加密算法在应用中对用户的密码进行了存储保护。

请注意：应用软件涉及的密码可能会有多类，比如帐户登陆应用软件界面的登陆密码、应用软件调用数据库的数据库密码等。对于每一种需要应用软件处理的密码，均应通过强加密算法进行传输与存储保护。

PCI DSS 要求 8.2.1 使用强效加密法以使所有验证凭证(例如密码/口令)在所有系统组件中传输和存储时均不可读。

4.3 人机交互密码的属性与设置

对于每一处涉及到人机交互的密码，应用软件可以通过硬编码，或者实现密码认证的选项，或者指向内部专用的密码认证平台进行密码属性的强制配置。如应用软件需要自身实现密码属性，则包括了长度、复杂度、有效期、密码历史、无效尝试锁定等。具体要求如下：

PCI DSS 要求 8.2.3 密码/口令必须符合以下要求：
• 要求长度至少为 7 个字符。
• 同时包含数字和字母字符。或者，密码/口令必须具有至少与上面指定参数相当的复杂度和强度。
PCI DSS 要求 8.2.4 至少每 90 天变更一次用户密码/口令。
PCI DSS 要求 8.2.5 不允许个人提交与最近所用的 4 个密码/口令中任何一个相同的新密码/口令。
PCI DSS 要求 8.1.6 在不超过 6 次尝试后锁定用户 ID，从而限制反复的访问尝试。
PCI DSS 要求 8.1.7 将锁定时间设为最少 30 分钟或直到管理员启用用户 ID。

4.4 人机交互密码的管理要求

如应用软件需要自身实现密码属性，应辅助实现用户密码重置前的用户身份验证、设定唯一的初始化密码值等功能。如可行，也推荐在软件界面中指导用户安全地使用密码。具体要求如下：

PCI DSS 要求 8.2.2 在修改任何验证凭证(例如，执行密码重置、提供新令牌或生成新密钥)前验证用户身份。
PCI DSS 要求 8.2.6 将每个用户首次使用的密码/口令和重置密码/口令设为唯一值，并在首次使用后立即变更。
PCI DSS 要求 8.4 为所有用户编写并传达验证政策和程序，包括：
• 选择强效验证凭证的指南。
• 关于用户应如何保护其验证凭证的指南。
• 关于不重用之前用过的密码的说明。
• 在怀疑密码可能受到威胁的情况下更改密码的相关说明。

5 应用软件的访问日志管理要求

5.1 记录登陆用户的认证情况

如果应用软件涉及到用户认证，应记录日志的认证过程，至少记录下无效的登陆尝试。具体要求点如下：

PCI DSS 要求 10.2 对所有系统组件实施自动检查记录。
PCI DSS 要求 10.2.4 无效的逻辑访问尝试。

5.2 应用软件对记录内容的具体要求

在记录的过程中，应记录下事件的相关属性（包括时间、类型、用户、被访问对象等），具体要求点如下：

PCI DSS 要求 10.3 对于每次事件，至少记录所有系统组件的以下检查记录条目：
PCI DSS 要求 10.3.1 用户识别。
PCI DSS 要求 10.3.2 事件类型。
PCI DSS 要求 10.3.3 日期和时间。
PCI DSS 要求 10.3.4 成功或失败指示。

PCI DSS 要求 10.3.5 事件的起因。
PCI DSS 要求 10.3.6 受影响的数据、系统组件或资源的特性或名称。

5.3 事件日志的存储时长要求

应用软件应记录日志，以用于数据泄露事件的追溯需要。要求如下：

PCI DSS 要求 10.7 保留检查记录历史至少一年，其中最少 3 个月的记录可立即访问以供分析（例如，在线、存档或可从备份恢复）。

6 总结

本文从应用软件所涉及的多个层面进行了 PCI DSS 标准要求点的梳理，概括起来主要是持卡人数据的存储与传输、用户的认证与密码管理、应用软件的日志记录三个层面。

合规 PCI DSS 的机构，可基于应用软件的具体情况，参考 PCI DSS 标准要求点及其指南进行应用软件的合规建设。更多标准要求细节欢迎随时联系 atsec 信息安全（www.atsec.cn 或致电+86 10 53056681）沟通交流。