支付卡行业 (PCI)
支付应用程序数据安全标准

要求和安全评估程序

3.2 版

2016 年 5 月

文档变更记录

日期	版本	描述	页码
2008 年 10 月 1 日	1.2	根据新的 PCI DSS 1.2 版调整内容并实施原始 1.1 版中标出的微小变更。	
2009 年 7 月	1.2.1	在“PA-DSS 的范围”中，根据《PA-DSS 计划指南》（1.2.1 版）对内容进行调整，以明确 PA-DSS 所适用的应用程序。	v、vi
		在“实验室要求 6”中，更正了“OWASP”的拼写。	30
		在“认证证明第 2a 部分”中，对“支付应用程序功能”进行了更新，以便与《PA-DSS 计划指南》中列出的应用程序类型保持一致，并在第 3b 部分中明确了年度重新认证程序。	32、33
2010 年 10 月	2.0	更新和实施针对 1.2.1 版的微小变更，并根据新的 PCI DSS 2.0 版进行调整。有关详细信息，请参阅 *PA-DSS – PA-DSS 1.2.1 版到 2.0 版的变更汇总*。	
2013 年 11 月	3.0	从 PA-DSS 2.0 版更新。有关变更详情，请参阅 *PA-DSS – PA-DSS 2.0 版到 3.0 版的变更汇总*。	
2015 年 5 月	3.1	从 PA-DSS 3.0 版更新。有关变更详情，请参阅 *PA-DSS – PA-DSS 3.0 版到 3.1 版的变更汇总*。	
2016 年 5 月	3.2	从 PA-DSS 3.1 版更新。有关变更详情，请参阅 *PA-DSS – PA-DSS 3.1 版到 3.2 版的变更汇总*。	

目录

简介

文件目的

PCI 支付应用程序数据安全标准 (PA-DSS) 要求和安全评估程序定义了适用于支付应用程序软件供应商的安全要求和评估程序。本文件供支付应用程序合格安全性评估商 (PA-QSA) 执行支付应用程序评估，以验证支付应用程序符合 PA-DSS 要求。有关如何记录 PA-DSS 评估并创建认证报告 (ROV) 的详细信息，PA-QSA 应该参阅位于 PCI 安全标准委员会 (PCI SSC) 网站 (www.pcisecuritystandards.org*) 上的 PA-DSS ROV 报告模板*。

PCI 安全标准委员会 (PCI SSC) 网站 (www.pcisecuritystandards.org) 还提供了其他资源，包括认证证明、常见问题 (FAQ) 和 *《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》*。

PCI DSS 与 PA-DSS 的关系

使用符合 PA-DSS 要求的应用程序并不意味着实体也符合 PCI DSS 要求，因为必须将应用程序实施到符合 PCI DSS 要求的环境中，并且需要按照支付应用程序供应商提供的 *《PA-DSS 实施指南》*（按照 PA-DSS 要求 13）进行应用。PA-DSS 要求基于 *支付卡行业数据安全标准 (PCI DSS) 要求和安全评估程序*而制定，其中规定了哪些方面需要符合 PCI DSS 的要求（以及支付应用程序必须支持哪些功能以实现客户的 PCI DSS 遵从性）。PCI DSS 可在 www.pcisecuritystandards.org 找到。

凡存储、处理或传输持卡人数据的应用程序均在实体的 PCI DSS 评估范围内，包括已按照 PA-DSS 验证的应用程序。PCI DSS 评估应该确认 PA-DSS 支付应用程序已按照 PCI DSS 要求正确配置并安全实施。如果支付应用程序已经过任何定制，在 PCI DSS 评估期间则需开展更深入的审核，因为该应用程序可能已经不再能代表经 PA-DSS 认证的版本

除非支付应用程序供应商可以存储、处理或传输持卡人数据或有权访问其客户的持卡人数据，否则不能将 PCI DSS 直接应用到该供应商。然而，由于应用程序供应商的客户使用此类支付应用程序来存储、处理和传输持卡人数据，并且也要求其遵守 PCI DSS 要求，因此这些支付应用程序应该可以促进而非妨碍客户实现 PCI DSS 遵从性。非安全支付应用程序只能通过以下几种方式妨碍实现遵从性：

1. 授权之后，将磁条数据和/或芯片上的等效数据存储在客户网络中；
2. 应用程序要求客户禁用“PCI 数据安全标准”所要求的其他功能（例如杀毒软件或防火墙），以便使支付应用程序正常运行；以及
3. 供应商使用不可靠的方式连接至应用程序，以便为客户提供支持。

在符合 PCI DSS 的环境中使用安全支付应用程序，可最大限度减少潜在的安全漏洞，从而防止主帐户 (PAN)、全磁道数据、卡验证码与验证值（CAV2、CID、CVC2、CVV2）、PIN 和 PIN 数据块遭受威胁并避免因安全漏洞所造成的严重欺诈行为。

集成商与经销商

应用程序供应商可能会授权集成商和经销商代表他们销售、安装和/或维护支付应用程序。集成商/经销商需要承担相应的职责以确保支付应用程序的安全安装和运行，因为他们通常可以为供应商的客户提供现场服务并帮助安装经过认证的 PA-DSS 支付应用程序。错误的应用程序配置、维护或支持可能会在客户的持卡人数据环境中造成安全漏洞，而这些漏洞随后可能会被攻击者利用。应用程序供应商应该就如何以符合 PCI DSS 要求的方式安装和配置支付应用程序，对客户、集成商与经销商进行培训。

PCI DSS 和 PA-DSS 委员会应该对合格的 PCI 集成商和经销商 (QIR) 进行培训，以便于安全地实施支付应用程序。有关 PCI QIR 计划的更多信息，请访问 www.pcisecuritystandards.org。

PCI DSS 适用性信息

PCI DSS 适用于参与支付卡处理的所有实体 — 包括商户、处理商、收单机构、发卡机构和服务提供商。PCI DSS 还适用于存储、处理或传输持卡人数据和/或敏感验证数据的所有其他实体。

持卡人数据和敏感验证数据的定义如下：

帐户数据	
持卡人数据包括：	**敏感验证数据包括：**
▪ 主帐户 (PAN) ▪ 持卡人姓名 ▪ 失效日 ▪ 业务码	▪ 全磁道数据（磁条数据或芯片上的等效数据） ▪ CAV2/CVC2/CVV2/CID ▪ PIN/PIN 数据块

主帐户 (PAN) 是持卡人数据的决定性因素。如果持卡人姓名、业务码和/或失效日与 PAN 一起存储、处理或传输，或以其他方式出现在持卡人数据环境 (CDE) 中，则必须按照适用的 PCI DSS 要求予以保护。

下页中的表格列举了持卡人数据和敏感验证数据的常用元素、是否允许存储这些数据，以及是否需要保护这些数据。该表格的内容并非详尽无遗，只用于列举适用于每种数据元素的不同类型的要求。

		数据元素	允许存储	按照 PA-DSS 要求 2.3 实现存储数据的不可读性
帐户数据	**持卡人数据**	主帐户 (PAN)	是	是
		持卡人姓名	是	否
		业务码	是	否
		失效日	是	否
	敏感验证数据 [1]	全磁道数据 [2]	否	按照 PA-DSS 要求 1.1 规定不能存储
		CAV2/CVC2/CVV2/CID[3]	否	按照 PA-DSS 要求 1.1 规定不能存储
		PIN/PIN 数据块 [4]	否	按照 PA-DSS 要求 1.1 规定不能存储

PA-DSS 要求 2.2 和 2.3 仅适用于 PAN。如果 PAN 与持卡人数据的其他元素一起存储，仅 PAN 必须按照 PA-DSS 要求 2.3 实现不可读性。授权之后，即使已加密，也不允许存储敏感验证数据。即使环境中没有 PAN，该规定仍适用。

1 *授权之后，不允许存储敏感验证数据（即使已加密）。*

2 *磁条上的全磁道数据，芯片或其他地方上的等效数据*

3 *印在支付卡正面或背面的三位或四位数值*

4 *数据持卡人在需要实卡交易中输入的个人识别码，和/或出现在交易信息中已加密的 PIN 数据块*

PA-DSS 的范围

PA-DSS 适用于软件供应商和开发用于存储、处理或传输持卡人数据和/或敏感验证数据的支付应用程序的其他机构。有关不同类型应用程序资格的相关信息，请参阅*《PA-DSS 计划指南》*。

PA-DSS 评估范围应该包括以下方面：

- 涵盖所有支付应用程序功能，包括但不限于：
  1) 端到端支付功能（授权和结算）、
  2) 输入和输出、
  3) 错误条件、
  4) 与其他文件、系统和/或支付应用程序或应用程序组件之间的接口和连接、
  5) 所有持卡人数据流、
  6) 加密机制，以及
  7) 验证机制。
- 支付应用程序供应商应该向客户和集成商/经销商提供指南的涵盖范围（请参阅本文件稍后部分的*《PA-DSS 实施指南》*），以确保：
  1) 客户知道如何以符合 PCI DSS 的方式实施支付应用程序，以及
  2) 明确告知客户，某些支付应用程序和环境设置可能会导致他们破坏 PCI DSS 遵从性。

  请注意，如果特定设置满足以下条件，支付应用程序供应商可能需要提供此类指南：
  1) 当客户安装应用程序之后，支付应用程序供应商无法控制特定设置；或者
  2) 由客户承担责任，而不是由支付应用程序供应商承担。
- 涵盖为接受审查的支付应用程序版本选定的所有平台（应当明确指出所包含的平台）。
- 涵盖支付应用程序所含或所使用的用以访问和/或查看持卡人数据的工具（报告工具、记录工具等）
- 涵盖所有与支付应用程序相关的软件组件，包括第三方软件要求和依赖关系
- 涵盖进行全面实施所需的所有其他类型的支付应用程序
- 涵盖供应商的版本控制方法

PA-DSS 对终端硬件上的支付应用程序的适用性

本部分为希望对终端硬件（也称为独立式或专用支付终端）上安装的支付应用程序进行 PA-DSS 认证的供应商提供指导。

终端硬件上安装的支付应用程序可以通过两种方式获得 PA-DSS 认证：

1. 安装的支付应用程序直接满足所有 PA-DSS 要求并且根据标准 PA-DSS 程序进行认证。
2. 安装的支付应用程序不符合所有 PA-DSS 要求，但是安装应用程序的硬件作为目前通过 PCI PTS 批准的交互点 (POI) 设备列在 PCI SSC 的“批准的 PIN 交易安全 (PTS) 设备列表”中。在这种情况下，应用程序可能需要通过结合 PA-DSS 和 PTS 已认证的控制措施来达到 PA-DSS 的要求。

本部分的剩余内容仅适用于经过认证并且获得 PCI PTS 批准的 POI 设备上安装的支付应用程序。

如果一项或多项 PA-DSS 要求无法由支付应用程序直接满足，那么可以通过控制措施（作为 PCI PTS 认证过程的组成部分进行测试）间接满足。对于认为应该包含在 PA-DSS 审查中的硬件设备，硬件设备必须经认证成为 PCI PTS 批准的 POI 设备，并且列在 PCI SSC 的“批准的 PTS 设备列表”中。经 PTS 认证的 POI 设备可以提供可信的计算环境，将会成为支付应用程序“***必需的依赖条件***”，而应用程序和硬件将共同列在“PA-DSS 认证支付应用程序列表”中。

在进行 PA-DSS 评估时，PA-QSA 必须根据 PA-DSS 的所有要求对支付应用程序及其所依赖的硬件进行全面的测试。如果 PA-QSA 确定安装的支付应用程序无法满足一项或多项 PA-DSS 要求，但是可以通过 PCI PTS 认证的控制措施来满足要求，那么 PA-QSA 必须：

1. 清晰记录满足了 PA-DSS 中标明的哪些要求（正常条件下）；
2. 清晰记录哪些要求是通过该要求的“到位”栏中的 PCI PTS 来满足的；
3. 详细解释支付应用程序为什么无法满足 PA-DSS 要求；
4. 记录所执行的程序，以确定如何通过 PCI PTS 已认证的控制措施来充分满足该要求；
5. 将 PCI PTS 已认证的硬件终端作为必需的依赖条件，列在认证报告的实施概要中。

在 PA-QSA 完成对支付应用程序的认证并且 PCI SSC 接受认证结果之后，PTS 已认证的硬件设备将会作为支付应用程序的依赖条件列在“PA-DSS 已认证应用程序列表”中。

通过 PA-DSS 和 PCI PTS 控制措施组合认证的终端硬件上安装的支付应用程序必须满足以下标准：

1. 如果同时向客户提供（终端硬件和应用程序），或者如果单独提供，应用程序供应商和/或集成商/经销商必须对应用程序进行封装才能分发，以便仅在经认证可行的终端硬件上运行。
2. 以默认方式启用以支持客户的 PCI DSS 遵从性。
3. 提供用于保持 PCI DSS 遵从性的持续支持和更新。
4. 如果将应用程序单独出售、分发或授权给客户，供应商必须根据应用程序的 PA-DSS 认证列表，提供使用应用程序时必须具备的依赖性硬件的详细信息。

《PA-DSS 实施指南》

通过认证的支付应用程序必须能以符合 PCI-DSS 的方式进行实施。软件供应商需提供*《PA-DSS 实施指南》*，以便指导客户与集成商/经销商实现产品的安全实施，记录本文件中所有提及的安全配置的详细情况，以及清晰说明供应商、集成商/经销商与客户各自在满足 PCI DSS 要求方面的责任。指南应详述客户和/或集成商/经销商该如何在客户网络中启用安全设置。例如，*《PA-DSS 实施指南》*应当涵盖 PCI DSS 密码安全性的责任与基本功能，即使这并不由支付应用程序控制，从而让客户或集成商/经销商知道该如何实施安全的密码，以实现 PCI DSS 遵从性。

*《PA-DSS 实施指南》*必须提供如何配置支付应用程序以满足要求的详细信息，而不能简单重复 PCI DSS 或 PA-DSS 中的要求。在评估期间，PA-QSA 必须确认说明准确并且有效。PA-QSA 还必须确认将*《PA-DSS 实施指南》*分发给客户和集成商/经销商。

当已按照*《PA-DSS 实施指南》*在符合 PCI DSS 的环境中实施了支付应用程序时，该程序应当促进并支持实现客户的 PCI DSS 遵从性。

请参阅*《附录 A：PA-DSS 实施指南的内容总结》*，对比了解*《PA-DSS 实施指南》*中规定的有关实施控制措施的责任。

支付应用程序合格安全性评估商 (PA-QSA) 要求

仅允许支付应用程序合格安全性评估商 (PA-QSA) 公司雇用的支付应用程序合格安全性评估商 (PA-QSA) 执行 PA-DSS 评估。请参阅 www.pcisecuritystandards.org 上的支付应用程序 QSA 列表，以获取有资格执行 PA-DSS 评估的公司列表。

- PA-QSA 必须采用“支付应用程序数据安全标准”文件中所记录的测试程序。
- PA-QSA 必须具备适于开展认证流程的实验室设施。

测试实验室

- 测试实验室可以位于两个位置：PA-QSA 场所现场，或软件供应商场所现场。
- 测试实验室应当能够模拟支付应用程序的真实使用情况。
- PA-QSA 必须验证实验室环境是否为全新安装，以确保环境能够真正模拟真实使用场景，并确保供应商没有以任何方式修改或篡改环境。
- 有关实验室与实验室相关流程的详细要求，请参阅本文件中的*《附录 B：对针对 PA-DSS 评估的测试实验室配置的确认》*。
- PA-QSA 必须针对接受审查的支付应用程序所使用的特定实验室，填写完成*《附录 B》*，并将其作为完整的 PA-DSS 认证报告 (ROV) 的组成部分进行提交。

认证报告的说明与内容

*PA-DSS ROV 报告模板中提供了 PA-DSS 认证报告 (ROV) 的说明和内容。*必须使用 *PA-DSS ROV 报告模板*来创建认证报告。只能向 PCI SSC 提供符合要求的支付应用程序 ROV。有关 ROV 提交流程的详细信息，请参阅*《PA-DSS 计划指南》*。

PA-DSS 实施步骤

此文件包含“要求和安全评估程序”表以及*《附录 B：针对 PA-DSS 评估的测试实验室配置》*。“要求和安全评估程序”详细介绍了 PA-QSA 必须执行的程序。

PA-QSA 必须执行以下步骤：

1. 确认 PA-DSS 的评估范围。
2. 执行 PA-DSS 评估。
3. 使用 *PA-DSS ROV 报告模板*来填写认证报告 (ROV)，包括确认用于 PA-DSS 评估的测试实验室配置。
4. 填写“认证证明”并签名（PA-QSA 和软件供应商都需要签名）。PCI SSC 网站 (www.pcisecuritystandards.org) 上提供“认证证明”。
5. 填写完成之后，根据*《PA-DSS 计划指南》*将上述所有文件和《PA-DSS 实施指南》*提交给 PCI SSC*。

注：

除非可以证明符合所有 PA-DSS 要求，否则请不要提交 PA-DSS。

《PA-DSS 计划指南》

有关 PA-DSS 计划管理的具体内容，请参阅*《PA-DSS 计划指南》*中的以下主题信息：

- 不同 PA-DSS 版本的详情及其生效日
- PA-DSS 对于不同应用程序类型的适用性；
- PA-DSS 报告的提交与认可流程；
- “已认证支付应用程序清单”中列出的支付应用程序的年度续期流程；
- 确定清单所列支付应用程序出错或受到威胁时的通知义务。

如果“支付应用程序数据安全标准”发生重大变更，和/或在清单所列支付应用程序中明确发现有任何漏洞，则 PCI SSC 有权要求实施重新认证。

PA-DSS 要求和安全评估程序

下面提供了《PA-DSS 要求和安全评估程序》表格列标题的定义：

- **PA-DSS 要求** – 此列定义了对支付应用程序进行认证需遵循的安全要求
- **测试程序** – 此列定义了 PA-QSA 在验证是否满足 PA-DSS 要求时需要遵循的测试流程
- **指南** – 此列说明每项 PA-DSS 要求的目的或安全目标，旨在帮助理解各项要求。本列中的指南并不替代或扩充 PA-DSS 要求和测试程序。

注：

如果有任何控制措施尚未实施就位或尚未计划在将来某个日期完成实施，则不能认为达到了 PA-DSS 的要求。

要求 1：　不要保留全磁道数据、卡验证代码或值（CAV2、CID、CVC2、CVV2）或 PIN 数据块

PA-DSS 要求	测试程序	指南
1.1 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。 敏感验证数据包括下文第 1.1.1 至 1.1.3 要求中列举的数据类型。 ***符合 PCI DSS 要求 3.2***	**1.1.a** 如果此支付应用程序存储了敏感验证数据，请确认应用程序仅供发卡机构和/或支持发卡服务的公司使用。	敏感验证数据包括全磁道数据、卡验证代码或值以及 PIN 数据。禁止在授权后存储敏感验证数据。这类数据对恶意个人非常重要，因为他们可借此生成假冒支付卡，进行欺诈性交易。 发行支付卡的实体或者提供或支持发行服务的实体通常会将创建和控制敏感验证数据作为发行功能的一部分。如果有合理的业务需求并且数据已经安全地存储，那么可以允许发卡机构和支持发卡服务的公司存储敏感验证数据。 对于非发卡实体，不允许在授权后保留敏感验证数据，应用程序必须具有用于安全删除数据并且使数据不可恢复的机制。
	1.1.b 对于所有其他支付应用程序，如果在授权之前已存储敏感验证数据（见下文 1.1.1 – 1.1.3），则需要获取并审查安全删除数据的方法，以确认数据不可恢复。	

PA-DSS 要求	测试程序	指南
1.1.1 授权之后，不要存储磁条中任意磁道上的完整内容（位于卡的背面，芯片或其他位置中包含的等效数据）。此类据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。 ***注：****在正常业务过程中，以下磁条数据元素可能需要保留：* • *帐户持有人姓名，* • *主帐户 (PAN)，* • *失效日，以及* • *业务码* *为将风险降至最低，只能存储业务所需的数据元素。* ***符合 PCI DSS 要求 3.2.1***	**1.1.1** 安装支付应用程序并执行能够模拟支付应用程序所有功能的多次测试交易，包括生成错误状态和日志条目。使用取证工具和/或方法（商业工具、脚本等）[5] 检查所有由支付应用程序生成的输出，确认在授权后，支付卡背面磁条任意磁道上的完整内容或芯片上的等效数据未被存储。至少包括以下文件类型（以及由支付应用程序生成的任何其他输出）： • 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 • 非易失性记忆体，包括非易失性缓存 • 数据库架构 • 数据库内容。	如果已存储全磁道数据，恶意个人在获得这些数据后便可借此复制支付卡，完成欺诈性交易。

[5] *取证工具或方法：是指用于发现、分析与提出取证数据的工具或方法，它能提供一条有效的途径用于快速、彻底地验证、搜寻与再现电脑证据。当取证工具或方法由PA-QSA 使用时，这些工具或方法应能准确地找到由支付应用程序写入的任何敏感的验证数据。这类工具可以是商业性的、开源性的或是由 PA-QSA 内部开发的。*

PA-DSS 要求	测试程序	指南
1.1.2 授权之后，不要存储卡验证值或代码（印在支付卡正面或背面的用于验证无实卡交易的三或四位数值）。 ***符合 PCI DSS 要求 3.2.2***	**1.1.2** 安装支付应用程序并执行能够模拟支付应用程序所有功能的多次测试交易，包括生成错误状态和日志条目。使用取证工具和/或方法（商业工具、脚本等） 检查所有由支付应用程序生成的输出，确认在授权后支付卡正面或签名方格上所印的三位或四位卡验证代码（CVV2、CVC2、CID、CAV2 数据）未被存储。至少包括以下文件类型（以及由支付应用程序生成的任何其他输出）： • 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 • 非易失性记忆体，包括非易失性缓存 • 数据库架构 • 数据库内容。	卡验证代码主要用于保护消费者和卡都不在交易现场的“无实卡”交易—互联网或邮件命令/电话命令 (MO/TO) 交易。如果这些数据被盗，恶意个人便能实施互联网和 MO/TO 欺诈交易。
1.1.3 授权之后，不要存储个人识别码 (PIN) 或经加密的 PIN 数据块。 ***符合 PCI DSS 要求 3.2.3***	**1.1.3** 安装支付应用程序并执行能够模拟支付应用程序所有功能的多次测试交易，包括生成错误状态和日志条目。使用取证工具和/或方法（商业工具、脚本等） 检查所有由支付应用程序生成的输出，确认在授权后 PIN 与加密的 PIN 数据块未被存储。至少包括以下文件类型（以及由支付应用程序生成的任何其他输出）。 • 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 • 非易失性记忆体，包括非易失性缓存 • 数据库架构 • 数据库内容。	仅持卡人或发卡银行可知道这些数值。如果这些数据被盗，恶意个人便能实施基于 PIN 的欺诈性借方交易（例如 ATM 取款）。

PA-DSS 要求	测试程序	指南
1.1.4 安全删除由支付应用程序以前版本存储的所有磁道数据（来自于磁条或芯片上包含的等效数据）、卡验证值或代码以及 PIN 或 PIN 数据块。删除时须遵循行业认可的安全删除标准，例如由美国国家安全局管理的认可产品清单或由其他州或国家标准或规章所规定的删除标准。 ***注：****此要求仅适用于支付应用程序的以前版本存储敏感验证数据的情况。* ***符合 PCI DSS 要求 3.2***	**1.1.4.a** 审查由供应商编制的*《PA-DSS 实施指南》*，确认其已向客户与集成商/经销商作了如下说明： • 必须移除历史数据（由支付应用程序以前版本存储的磁道数据、卡验证代码、PIN 或 PIN 数据块）。 • 如何移除历史数据。 • 上述移除对于 PCI DSS 遵从性来说是绝对必需的。	授权后不允许存储任何敏感验证数据元素。如果支付应用程序的旧版本中存储了此类信息，支付应用程序供应商必须在*《PA-DSS 实施指南》*中提供说明以及安全擦除工具或程序。如果未安全删除，这些数据可能隐藏在客户的系统中，获得该信息访问权限的恶意个人可能会使用这些数据生成假冒支付卡和/或进行欺诈性交易。
	1.1.4.b 检查支付应用程序软件文件和配置文档，以确认供应商提供了安全的擦除工具或程序来移除数据。	
	1.1.4.c 通过使用取证工具和/或方法，确认由供应商提供的安全擦除工具或程序已按照行业认可的数据安全删除标准安全地移除了数据。	

PA-DSS 要求	测试程序	指南
1.1.5 不要在供应商系统上存储敏感验证数据。如果必须使用任何敏感验证数据（预授权数据）进行除错或故障排除，请确保采取以下措施： • 仅在解决特定问题时，才收集必要的敏感验证数据。 • 仅在特定的、已知的、有访问限制的位置存储此类数据。 • 在解决特定问题时，仅收集最低数量的必要数据。 • 存储时，使用强效加密法对敏感验证数据进行加密。 • 使用后即刻安全地删除数据，包括来自于以下位置的数据： - 日志文件 - 除错文件 - 从客户接收的其他数据来源。 ***符合 PCI DSS 要求 3.2。***	**1.1.5.a** 检查*软件供应商*所提供的客户问题解决程序，确认程序包括如下内容： • 仅在解决特定问题时，才收集必要的敏感验证数据。 • 仅在特定的、已知的、有访问限制的位置存储此类数据。 • 在解决特定问题时，仅收集有限的必要数据。 • 存储时，对敏感验证数据进行加密。 • 使用后，即刻安全地删除此类数据。 **1.1.5.b** 选取部分最近由客户提出的故障排除请求，确认每次事件均遵循了 1.1.5.a 所审查的程序。 **1.1.5.c** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商作了如下说明： • 仅在解决特定问题时，才收集必要的敏感验证数据。 • 仅在特定的、已知的、有访问限制的位置存储此类数据。 • 在解决特定问题时，仅收集有限的必要数据。 • 存储时，对敏感验证数据进行加密。 • 使用后，即刻安全地删除此类数据。	如果供应商向其客户提供了可能会导致收集敏感验证数据的服务（例如，用于排除故障或除错），供应商必须将收集的数据量降到最低，并确保数据得到保护并在不再需要时进行安全地删除。 如果对问题进行故障排除时要求将应用程序暂时配置为捕获敏感验证数据 (SAD)，那么在完成必需的数据捕获之后，应立即将应用程序恢复为常规安全配置（即，禁用对 SAD 的收集）。 当不再需要之后，应该根据行业认可的标准来删除 SAD（例如，使用可以确保永远无法检索到数据的安全擦除程序）。

要求 2：　　保护存储的持卡人数据

PA-DSS 要求	测试程序	指南
2.1 软件供应商必须指导客户在其自定义的保留期过期之后安全删除持卡人数据。 ***符合 PCI DSS 要求 3.1***	**2.1** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商提供如下指导： • 必须安全删除超过客户自定义保留期的持卡人数据。 • 包括支付应用程序存储持卡人数据的所有位置的清单（以便客户了解哪些位置存储的数据需要删除）。 • 客户不再需要将持卡人数据用于法律、法规或业务目的时进行安全删除所需的说明。 • 如何安全删除支付应用程序存储的持卡人数据的说明，包括底层软件或系统上存储的数据（例如操作系统、数据库等） • 用于配置底层软件或系统的说明（例如操作系统、数据库等） 以防止意外捕获或保留持卡人数据 — 例如，系统备份或复原点。	为了满足 PCI DSS 要求 3.1，供应商必须提供支付应用程序可能存储持卡人数据的所有位置的详细信息，包括底层软件或系统中的位置（例如操作系统、数据库等），以及在数据超过客户定义的保留期限之后从这些位置安全删除数据的说明。 同时，也必须向客户和集成商/经销商提供应用程序运行所在的底层系统和软件的配置详细信息，以确保这些底层系统不会在客户不知情的情况下捕获持卡人数据。客户需要了解底层系统如何从应用程序捕获数据，以便于他们防止底层系统捕获持卡人数据或确保数据得到适当的保护。
2.2 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。 ***注：****该要求不能取代现行更严格的有关持卡人数据显示的要求，例如法律或支付卡品牌对销售点 (POS) 收据的要求。* ***符合 PCI DSS 要求 3.3***	**2.2.a** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商提供如下指导： • 显示 PAN 的所有情形的详细信息，包括但不限于 POS 设备、显示屏、日志和收据。 • 确认支付应用程序默认情况下在所有显示中掩盖 PAN。 • 如何配置支付应用程序的说明，以便于仅限具有合理业务需求的工作人员查看除前六位/后四位以外的 PAN（包括显示完整的 PAN）。	在计算机显示屏、支付卡收据、传真或纸质报告等物品上显示完整的 PAN 可能导致此类数据被无授权个人获取并用于欺诈。 掩盖方法应始终确保必要时仅显示尽可能少的位数，以便履行特定业务职能。例如，如果仅需要后四位数即可履行业务职能，则可掩盖 PAN，以便履行该职能的个人仅查看后四位数。 *（接下页）*
	2.2.b 安装支付应用程序并检查显示 PAN 数据的所有位置，包括但不限于 POS 设备、显示屏、日志和收据。对于显示 PAN 的每个情形，请确认所显示的 PAN 已进行掩盖。	再如，如果某项职能出于发送目的需要访问银行识别号 (BIN)，则在履行该职能期间可选择仅取消掩盖 BIN 数字（一般为前六位数）。

PA-DSS 要求	测试程序	指南
	2.2.c 根据*《PA-DSS 实施指南》*配置支付应用程序，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。针对显示 PAN 的每个示例，请检查应用程序配置和显示的 PAN，以确认 PAN 的掩盖说明正确无误，且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。	该要求涉及保护在显示屏、纸质收据、打印材料等上面显示的 PAN，切勿与 PA-DSS 要求 2.3 中保护文件、数据库中存储的 PAN 的措施相混淆。
2.3 通过采取下列任一方法使所有位置存储的 PAN 均不可读（包括便携式数字媒介、备份媒介与日志中的数据）： • 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） • 索引记号与索引簿（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。 *（接下页）*	**2.3.a** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商提供如下指导： • 详细介绍应用程序用于使持卡人数据不可读的每种方法的所有可配置选项，并指示如何针对支付应用程序存储持卡人数据的所有位置来配置每种方法（根据 PA-DSS 要求 2.1）。 • 客户可能输出持卡人数据以存储到支付应用程序外部的所有情形的清单，以及客户负责在所有此类情形中使 PAN 不可读的说明。 • 如果已启用除错日志（例如，为了进行故障排除而启用），且日志包含 PAN，则须根据 PCI DSS 保护日志、在完成故障排除后尽快禁用日志，并在不再需要使用时安全删除日志的相关说明。	缺少对 PAN 的保护将会导致恶意个人查看或下载该数据。 可采用基于强效加密法的单向散列函数令持卡人数据不可读取。在无需检索原始数字时适于采用散列函数（单向散列不可逆）。 截词的目的在于仅存储部分 PAN（最多前六位和后四位数字）。 索引记号是根据特定索引用一个不可预测的值替代 PAN 的密码符号。一次性索引簿是一个系统，在这个系统中，使用（只可使用一次）随机生成的私人密钥为消息加密，然后使用匹配的一次性索引簿和密钥为消息解密。 *（接下页）*
注意： • 对恶意个人而言，如果能访问被截词和散列的 PAN，要重建原始 PAN 数据是件相当轻松的事。如果支付应用程序生成同一个 PAN 的散列版本和截词版本，则须采取额外控制措施，确保无法通过关联散列版本和截词版本来重建原始 PAN。 • 在任何存储 PAN 的位置都必须使 PAN 显示为不可读，即使在支付应用程序之外（例如，用于存储在客户环境中的应用程序日志文件输出）。 ***符合 PCI DSS 要求 3.4***	**2.3.b** 检查用于保护 PAN 的方法，包括加密算法（如果适用）。确认通过以下任一方法使 PAN 不可读： • 基于强效加密法的单向散列函数 • 截词 • 索引记号与索引簿（索引簿存储安全） • 具有相关密钥管理流程和程序的强效加密法。 **2.3.c** 如果应用程序同时创建了同一个 PAN 的散列版本和截词版本，请检查上述散列版本和截词版本的创建方法，以确认无法通过关联该散列版本和截词版本来重建原始 PAN。 **2.3.d** 检查应用程序创建或生成的数据储存库中的多个表格或文件，以确认 PAN 显示为不可读。	强效加密法（请参阅*《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》*中的定义）的目的是根据经行业测试并认可的算法（非专有或“自行开发”的算法）采用强效加密密钥进行加密。

PA-DSS 要求	测试程序	指南
	2.3.e 如果应用程序创建或生成了文件以供在应用程序外部使用（例如，针对导出或备份生成的文件），包括在可移动媒介上存储，请检查部分生成的文件，包括在可移动媒介上生成的文件（例如备份磁带），以确认 PAN 显示为不可读。	
	2.3.f 检查应用程序创建或生成的部分检查日志，确认 PAN 显示为不可读或已从日志中删除。	
	2.3.g 如果软件供应商以任何理由存储了 PAN（例如，将从客户处收到的日志文件、除错文件和其他数据源用于除错或故障排除），请确认已根据上述要求 2.3.b 到 2.3.f 使 PAN 显示为不可读。	
2.4 支付应用程序必须保护用于保护持卡人数据的密钥，以免遭到泄露与误用。 ***注：****此要求适用于用来加密所存储的持卡人数据的密钥，以及用于保护数据加密密钥的密钥加密密钥。此类密钥加密密钥至少要与数据加密密钥一样强效。* ***符合 PCI DSS 要求 3.5***	**2.4.a** 检查产品文档并访问负责人员，确认已实施用于限制访问应用程序所使用的加密密钥的控制措施。	必须大力保护加密密钥，因为获得密钥访问权者能够解密数据。 要求应用程序保护密钥以防止泄露和滥用的规定，同时适用于数据加密密钥和密钥加密密钥。原本并不打算对密钥加密密钥进行加密，但将按照要求 2.4 中的规定对它们予以保护，防止其遭到泄露和误用 应只有极少数的人能访问加密密钥，通常只有负责保管密钥的人才有权访问。
	2.4.b 检查系统配置文件，以确认： • 密钥以加密格式存储 • 密钥加密密钥与数据加密密钥单独存储 • 密钥加密密钥至少要与其保护的数据加密密钥一样强效。	
	2.4.c 审查由供应商编制的*《PA-DSS 实施指南》*，确认其指示客户与集成商/经销商： • 限制只有极少数必需的保管人才能访问密钥。 • 尽量减少密钥安全存储的位置和形式。	
2.5 支付应用程序必须对用于加密持卡人数据的密钥实施密钥管理流程与程序，至少应该包括以下方面： ***符合 PCI DSS 要求 3.6***	**2.5** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户和集成商/经销商作了如下说明： • 如何安全生成、分发、保护、更改、存储和注销/替换密钥，以及客户或集成商/经销商在哪些领域参与了这些密钥管理活动。 • 密钥保管人用于确认其理解并接受密钥保管责任的“密钥保管表格”样本。	加密密钥的管理方式是确保支付应用程序持续安全的关键部分。良好的密钥管理流程作为加密产品的一部分，无论是手动或自动均以行业标准为基础并涵盖要求 2.5.1 至 2.5.7 中的所有密钥要素。 指导客户如何安全地传输、存储并更新密钥有助于防止密钥管理不善或泄露给非授权实体。 本要求适用于用来加密所存储持卡人数据的密钥以及任何相关的密钥加密密钥。

PA-DSS 要求	测试程序	指南
2.5.1 生成强效加密密钥	**2.5.1.a** 审查*《PA-DSS 实施指南》*并确认其中包括指导客户和集成商/经销商安全生成加密密钥的说明。	支付应用程序必须按照“强效加密”下*《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》*中的定义生成强效密钥。
	2.5.1.b 测试应用程序（包括用于生成密钥的方法），以确认*《PA-DSS 实施指南》*中的说明可以生成强效加密密钥。	
2.5.2 安全的加密密钥分发	**2.5.2.a** 审查*《PA-DSS 实施指南》*并确认其中包括指导客户和集成商/经销商安全分发加密密钥的说明。	支付应用程序必须安全地分发密钥，这意味着不能以明码方式分发密钥，必须通过获得授权的过程来进行。
	2.5.2.b 测试应用程序（包括用于分发密钥的方法），确认*《PA-DSS 实施指南》*中的说明可以安全地分发密钥。	
2.5.3 安全的加密密钥存储	**2.5.3.a** 审查*《PA-DSS 实施指南》*并确认其中包括指导客户和集成商/经销商安全存储加密密钥的说明。	支付应用程序必须安全地存储密钥（例如，通过使用密钥加密密钥来加密它们）。
	2.5.3.b 测试应用程序（包括用于存储密钥的方法），确认*《PA-DSS 实施指南》*中的说明可以安全地存储密钥。	
2.5.4 根据相关应用程序供应商或密钥所有人的规定并基于行业最优方法和指南（例如，*《NIST 特别出版物 800-57》*），在密钥周期结束时（例如，指定期限过后和/或给定密钥产生一定量的密文后）对密钥进行的变更。	**2.5.4.a** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商作了如下说明： • 针对应用程序使用的每种密钥类型定义了密钥周期。 • 用于在定义的密钥周期结束时实施密钥更改的程序。	密钥周期是指特定密钥用于指定目的的时间段。定义密钥周期要考虑的因素包括但不限于基础算法的强度、密钥的大小或长度、密钥遭受威胁的风险以及被加密数据的敏感性。 加密密钥必须在加密周期结束后定期更改，这样可将他人获取加密密钥并用其解密数据的风险降到最低。
	2.5.4.b 测试应用程序（包括用于更改加密密钥的方法），确认*《PA-DSS 实施指南》*中的说明可以在定义的密钥周期结束时更改密钥。	

PA-DSS 要求	测试程序	指南
2.5.5 密钥的完整性变弱（例如，知道明文密钥部分的员工离职）或怀疑密钥遭受威胁时，认为有必要注销或替换密钥 （例如，在适用时进行存档、销毁和/或撤销）。 ***注：****如果需要保留注销或替换的加密密钥，则必须对其进行安全存档（例如，使用密钥加密密钥进行存档）。存档的加密密钥只能用于解密/验证。*	**2.5.5.a** 审查*《PA-DSS 实施指南》*，确认其中已向客户与集成商/经销商提供如下指导： • 有关在密钥的完整性变弱或者密钥受到已知或怀疑的威胁时，必须注销或替换密钥的说明。 • 用于注销或替换密钥的程序（例如，在适用时进行存档、销毁和/或撤销）。 • 确保已经注销或替换的密钥不再用于加密操作的程序。	不再使用或需要的密钥或者确定或怀疑受到威胁的密钥应予以撤销和/或销毁，以确保不再使用。若需要保留这种密钥（例如，用来支持已存档的加密数据），则应为其提供强效保护。 支付应用程序应规定并简化已到期或者确定或怀疑受到威胁的密钥的替换流程。
	2.5.5.b 测试应用程序（包括用于注销或替换密钥的方法），确认*《PA-DSS 实施指南》*中的说明可以注销或替换密钥（例如，在适用时进行存档、销毁和/或撤销）。	
	2.5.5.c 测试具有已注销/已替换密钥的应用程序，确认*《PA-DSS 实施指南》*中的说明可以确保应用程序不会使用已注销或已替换的密钥来执行加密操作。	
2.5.6 如果支付应用程序支持使用手动明文加密密钥管理操作，则这些操作必须实施分割知识和双重控制。 ***注：****手动密钥管理操作示例包括但不限于：密钥生成、传输、加载、存储和销毁。*	**2.5.6.a** 审查*《PA-DSS 实施指南》*，确认其中已向客户与集成商/经销商提供如下指导： • 有关应用程序支持的任何手动明文加密密钥管理操作的详细信息。 • 针对所有此类操作实施分割知识和双重控制的说明。	密钥的分割知识和双重控制确保没人知道完整的密钥。此控制措施适用于手动密钥管理操作。 分割知识是由两个或更多人分别掌握部分密钥且根据密钥的每个部分都无法得知整个密钥的方法；每个人只知道自己的密钥部分，且根据单个密钥部分无法得知整个密钥）。 双重控制需要两个或更多的人共同完成且他们无法访问或使用对方的验证材料。
	2.5.6.b 测试应用程序（包括所有手动明文加密密钥管理操作），确认*《PA-DSS 实施指南》*中的说明可以针对所有手动明文密钥管理程序所需的密钥采用分割知识和双重控制。	
2.5.7 防止对加密密钥进行未授权的替换	**2.5.7.a** 审查*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商提供指导方法，以防止对密钥进行未授权的替换。	支付应用程序应该定义适用于应用程序用户的方法，确保仅能进行获得授权的密钥替换。应用程序配置应该禁止允许或接受来自未授权来源或意外进程的密钥替换。
	2.5.7.b 测试应用程序（包括所有用于替换密钥的方法），确认*《PA-DSS 实施指南》*中的说明可以防止对加密密钥进行未授权的替换。	

PA-DSS 要求	测试程序	指南
2.6 根据行业认可的标准提供一种机制，使支付应用程序存储的所有加密密钥材料或密文不可检索。 这些密匙用于对持卡人数据进行加密或确认。 ***注：****仅当支付应用程序或之前版本的支付应用程序使用密钥材料或密文来加密持卡人数据时，此要求才适用。* ***符合 PCI DSS 要求 3.6***	**2.6.a** 审查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已向客户与集成商/经销商作了如下说明： • 详细介绍如何使用应用程序随附的工具或程序使加密材料不可检索的程序。 • 无论何时不再使用密钥，都应该根据 PCI DSS 中的密钥管理要求使密钥材料不可检索。 • 用于使用新密钥重新加密历史数据的程序，包括用于在加密/重新加密过程中保持明文数据安全性的程序。	供应商应该提供一种机制，以便于客户在不再需要旧加密材料时可以安全地进行删除。请注意，是否删除旧加密材料完全由客户自行决定。 通过使用工具或过程可以使加密密钥材料和/或密文不可检索，这些工具和过程包括但不限于： • 安全删除，例如，以美国国家安全局管理的认可产品清单或其他州或国家标准或规章所规定的删除标准为依据。 • 删除密钥加密密钥 (KEK)，前提是剩余的数据加密密钥仅以加密形式存在于已删除的 KEK 下。
	2.6.b 检查最终应用程序产品，确认供应商随应用程序提供了工具和/或程序以便于使加密材料不可检索。	
	2.6.c 测试应用程序，包括提供的使加密密钥材料不可检索的方法。通过使用取证工具和/或方法，根据行业认可的标准，确认由供应商提供的安全擦除工具或程序可以使加密材料不可检索。	
	2.6.d 测试使用新密钥重新加密历史数据的方法，确认*《PA-DSS 实施指南》*中的说明可以使用新密钥成功地重新加密历史数据。	

要求 3：　　提供安全的验证功能

PA-DSS 要求	测试程序	指南
3.1 支付应用程序必须支持和实施使用唯一的用户 ID，以及对所有管理访问权限和持卡人数据访问权限进行安全的验证。必须通过完成安装并在安装之后进行后续的更改，对应用程序生成或管理的所有帐户实施安全的验证。 应用程序必须实施以下 3.1.1 至 3.1.11 的要求： ***注：****要求 3 中大量使用的术语"后续更改"是指导致用户帐户恢复为默认设置的任何应用程序更改、对现有帐户配置的更改以及生成新帐户或重新创建现有帐户的更改。* ***注：****此类密码控制并不适用于一次只能访问一个卡号的员工来促成单笔交易，而适用于具备管理能力的员工的访问、对存有持卡人数据的系统的访问、以及受支付应用程序控制的访问。* *此要求适用于支付应用程序，以及所有用于查看或访问持卡人数据的相关工具。* ***符合 PCI DSS 要求 8.1 和 8.2***	**3.1.a** 检查由供应商创建的*《PA-DSS 实施指南》*，确认客户与集成商/经销商： • 就支付应用程序如何针对应用程序生成或管理的所有验证凭证实施强效验证，提供了清晰明确的方向，具体方法包括： - 根据要求 3.1.1 到 3.1.11 来完成安装，对验证凭证实施安全更改。 - 根据要求 3.1.1 到 3.1.11 对验证凭证的任何后续更改（安装之后）实施安全更改。 • 为了保持 PCI DSS 遵从性，建议在提供验证方法时对验证配置方面的任何更改都进行确认，验证方法的严格程度应该至少与 PCI DSS 的要求相同。 • 建议向该环境中的所有默认帐户分配安全验证。 • 针对不使用的任何默认帐户，分配安全验证，然后禁用或不使用这些帐户。 • 针对支付应用程序使用的所有验证凭证（但不是由应用程序生成或管理）提供清晰明确的指导，指示如何根据下面的要求 3.1.1 到 3.1.11，针对所有具有管理访问权限的应用程序级别和用户帐户以及具有持卡人数据访问权限的所有帐户，通过完成完成安装以及在安装之后进行更改来更改验证凭证并创建强效认证。 • 通过管理访问识别应用程序中的所有角色和默认帐户。	通过确保为每位用户分配唯一 ID 而非多位员工共用一个 ID，应用程序可以满足 PCI DSS 对于保持个人对操作负责及维护每个员工的有效审核跟踪方面的要求。这有助于在出现误用或恶意目的时加快问题的解决和控制。 当与唯一 ID 配合使用时，安全验证有助于防止用户 ID 受到威胁，因为任何尝试威胁帐户的人都需要同时知晓唯一 ID 和密码（或使用的其他验证）。
3.1.1 支付应用程序不针对其他必需的软件使用（或要求使用）默认的管理帐户（例如，支付应用程序不能使用数据库默认管理帐户）。 ***符合 PCI DSS 要求 2.1***	**3.1.1** 根据*《PA-DSS 实施指南》*安装和配置支付应用程序，包括针对所有必需的软件配置任何管理帐户。测试支付应用程序，确认支付应用程序不针对必需的软件使用（或要求使用）默认的管理帐户。	默认管理帐户（和密码）是公共常识，任何熟悉支付应用程序或底层系统组件的人都知道。如果使用了默认的管理帐户和密码，未经授权的个人只要使用众人皆知的凭证登录，就可以访问应用程序和数据。
3.1.2 应用程序必须通过完成安装并在安装后进行后续的更改，针对应用程序生成或管理的所有帐户实施所有默认应用程序密码的修改。	**3.1.2** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	如果应用程序未实施默认密码更改，应用程序可能会受到知晓默认设置的任何人的未授权访问。

PA-DSS 要求	测试程序	指南
这适用于包括用户帐户、应用程序和服务帐户，以及供应商用于提供支持的帐户在内的所有帐户。 ***注：**通过指定用户过程或在《PA-DSS 实施指南》中提供说明，无法满足此要求。完成安装时以及进行后续更改时，应用程序必须采取技术手段防止在修改默认密码前使用任何默认或内置的帐户。* ***符合 PCI DSS 要求 2.1***	**3.1.2.a** 根据*《PA-DSS 实施指南》*的要求安装应用程序，检查帐户和密码设置并尝试使用所有默认密码，以确认应用程序通过完成安装过程实施了对任何默认支付应用程序密码的更改。	
	3.1.2.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，检查帐户和密码设置并尝试使用所有默认密码来确认应用程序在完成更改时对所有默认密码实施了更改。	
3.1.3 支付应用程序为用户帐户分配了唯一 ID。 ***符合 PCI DSS 要求 8.1.1***	**3.1.3** 对于应用程序生成或管理的所有帐户，按照以下方式测试应用程序：	当每个用户都分配了唯一用户 ID 时，他们对于支付应用程序的访问以及在支付应用程序中的活动都可以追踪到执行这些操作的个人。
	3.1.3.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并尝试使用相同的用户 ID 来创建不同的应用程序帐户，以确认应用程序仅在完成安装过程后分配唯一的用户 ID。	
	3.1.3.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，检查帐户设置并测试应用程序功能来确认在完成更改时为所有帐户分配了唯一用户 ID。	
3.1.4 支付应用程序采用了以下至少一种方法来验证所有用户： ▪ 所知，如密码或口令等 ▪ 所有，如令牌设备或智能卡等 ▪ 个人特征，如生物特征。 ***符合 PCI DSS 要求 8.2***	**3.1.4** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	当与唯一 ID 配合使用时，这些验证方法有助于防止用户 ID 受到威胁，因为尝试威胁用户 ID 的人必须同时知晓唯一 ID 和密码（或使用的其他验证）。
	3.1.4.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并测试验证方法以确认应用程序在完成安装过程之后要求至少定义一个适用于所有帐户的验证方法。	
	3.1.4.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，测试验证方法以确认应用程序在完成更改之后要求至少定义一个适用于所有帐户的验证方法。	

PA-DSS 要求	测试程序	指南
3.1.5 支付应用程序**不**要求或使用任何群组、共享的或通用的帐户和密码。 ***符合 PCI DSS 要求 8.5***	**3.1.5** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	如果多个用户共享相同的验证凭证（例如，用户帐户和密码），将无法分配个人操作的责任或有效记录个人操作，因为给定的操作可能是由知晓验证凭证的任何人执行的。
	3.1.5.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置和测试应用程序功能，以确认应用程序在完成安装过程之后不要求或使用任何群组、共享的或通用的帐户和密码。	
	3.1.5.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认应用程序在完成更改之后不依赖于或使用任何群组、共享的或通用的帐户和密码。	
3.1.6 支付应用程序要求密码满足以下条件： • 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。	**3.1.6** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	恶意的个人通常会查找密码脆弱或没有密码的帐户，以获得对应用程序或系统的访问权。如果密码简短或易猜，则恶意个人相对更容易找到这些脆弱帐户并在有效用户 ID 的伪装下威胁应用程序或系统。 *（接下页）*
	3.1.6.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序要求密码至少达到以下复杂度和强度要求： • 长度至少为七个字符。 • 同时包含数字和字母字符。	
	3.1.6.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序要求密码至少达到以下复杂度和强度要求： • 长度至少为七个字符 • 同时包含数字和字母字符。	本要求规定密码长度至少为七个字符并且应该同时包含数字和字母字符。如果由于技术限制无法满足这个最低要求，实体可使用“等效强度”来评估其替代选择。NIST SP 800-63-1 将“熵”定义为“猜测或确定密码或密钥的难度衡量指标”。您可以参阅本文档和探讨“密码熵”的其他文档，以了解不同最低限度格式密码的熵值以及等效密码强度的更多信息。
	3.1.6.c 如果应用程序密码使用不同的最小字符集和长度，则需要计算应用程序所需的密码熵，并确认其至少与上述指定参数相当（即长度至少达到 7 个字符，且包含数字和字母字符）。	

PA-DSS 要求	测试程序	指南
3.1.7 支付应用程序要求至少每 90 天更改一次用户密码。 ***符合 PCI DSS 要求 8.2.4***	**3.1.7** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	长时间不更改的有效密码/口令会为恶意个人提供更多时间来破译密码/口令。
	3.1.7.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序要求用户密码至少每 90 天更改一次。	
	3.1.7.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序要求用户密码至少每 90 天更改一次。	

PA-DSS 要求	测试程序	指南
3.1.8 支付应用程序会保存密码历史，并要求新密码与前四次使用的密码不同。 ***符合 PCI DSS 要求 8.2.5***	**3.1.8** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序： **3.1.8.a** 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序会保存密码历史，并要求新密码与前四次使用的密码不同。 **3.1.8.b** 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序会保存密码历史，并要求新密码与前四次使用的密码不同。	如果未维护密码历史记录，则会降低更改密码的效力，因为之前使用的密码可能被反复重用。要求一段时间内不得重用密码可降低在日后使用已猜出或强制获取的密码的可能性。
3.1.9 支付应用程序通过在达到六次登录尝试后锁定用户帐户的方式限制反复访问尝试。 ***符合 PCI DSS 要求 8.1.6***	**3.1.9** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序： **3.1.9.a** 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序会在进行不超过六次的无效登录尝试后锁定用户帐户。 **3.1.9.b** 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序会在达到六次无效的登录尝试后锁定用户帐户。	如果不采用帐户锁定机制，攻击者可通过手动或自动工具（例如，密码破解）不断尝试猜测密码，直到成功猜出密码并访问用户帐户。
3.1.10 支付应用程序可以设置锁定持续至少 30 分钟，或者直到管理员启用该用户 ID。 ***符合 PCI DSS 要求 8.1.7***	**3.1.10** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序： **3.1.10.a** 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序会设置锁定持续至少 30 分钟，或者直到管理员启用该用户 ID。	如果帐户因有人不断尝试猜测密码而锁定，对这些已锁定帐户的延时再激活控制可阻止恶意个人不断猜测密码（在帐户重新激活之前，他们必须停止至少 30 分钟）。另外，如果必须申请再激活，管理员可以验证申请再激活的是实际帐户持有

PA-DSS 要求	测试程序	指南
	3.1.10.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序会设置锁定持续至少 30 分钟，或者直到管理员启用该用户 ID。	人。
3.1.11 如果支付应用程序会话空闲超过 15 分钟，则应用程序会要求用户重新验证或重新激活会话。 ***符合 PCI DSS 要求 8.1.8***	**3.1.11** 对于应用程序生成或管理的所有帐户，请按照以下方式测试应用程序：	当用户在打开访问支付应用程序的会话时离开，其他人可能会在用户离开时使用该连接，从而导致未经授权的帐户访问和/或帐户滥用。
	3.1.11.a 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并检查帐户设置，以确认在安装过程完成之前，应用程序可以设置会话空闲时间为 15 分钟或更短时间	
	3.1.11.b 测试导致用户帐户恢复为默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的所有应用程序功能。 对于已经执行的所有类型的更改，请检查帐户设置并测试应用程序功能，以确认在更改完成之后应用程序会设置会话空闲时间为 15 分钟或更短时间。	
3.2 软件供应商必须向客户提供指导，所有使用支付应用程序对 PC、服务器和数据库进行的访问都必须要求使用唯一的用户 ID 和安全验证。 ***符合 PCI DSS 要求 8.1 和 8.2***	**3.2** 检查由供应商编制的*《PA-DSS 实施指南》*，确认客户和集成商/经销商得到有关通过唯一用户 ID 和符合 PCI DSS 的安全验证控制使用支付应用程序和持卡人数据对任意 PC、服务器和数据库访问方面的指导。	如果应用程序安装在没有使用强效身份验证和验证控制的系统上，或者从这类系统访问应用程序，则应用程序提供的强效验证会被绕过，从而导致不安全访问。
3.3 在传输和存储期间确保所有支付应用程序密码（包括用户和应用程序帐户的密码）安全。 ***符合 PCI DSS 要求 8.2.1***	**3.**3 执行以下操作：	如果支付应用程序密码在没有加密的网络上存储或传输，恶意个人可以使用“嗅探器”轻易地截取密码，或者直接访问存储密码的文件，并使用窃取的数据获取非授权访问。 在使用哈希散列算法之前为每个密码组合
3.3.1 使用强效加密法使所有支付应用程序密码在传输期间不可读。	**3.3.1.a** 检查供应商文档和应用程序配置，确认已使用强效加密法使所有支付应用程序密码在传输期间始终不可读。	

PA-DSS 要求	测试程序	指南
	3.3.1.b 对于所有类型的应用程序密码，检查密码传输（例如，通过从另一个系统登录应用程序，以及向其他系统验证应用程序），以确认已使用强效加密法使所有支付应用程序密码在传输期间始终不可读。	
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。 ***注：****输入变量不需要不可预测或加密*	**3.3.2.a** 检查供应商文档和应用程序配置，确认： • 使用强效单向加密算法，基于许可标准使存储的密码不可读。 • 在应用加密算法之前，每个密码都与唯一的输入变量组合。	
	3.3.2.b 针对所有类型的应用程序密码，确认应用程序可能将密码存储在的所有位置（包括应用程序、底层系统、日志文件、注册表设置等位置中）。针对所有位置和密码类型，检查存储的密码文件，确认在使用强效单向加密算法时密码显示为不可读，并且在存储时始终带有唯一的输入变量。	
3.4 支付应用程序必须限制对所需功能/资源的访问，并对内置帐户实行最小权限： • 默认情况下，所有应用程序/服务帐户仅具有其原本所需功能/资源的访问权限。 • 默认情况下，所有应用程序/服务帐户对其所需的每项功能/资源仅分配到最低级别的权限。 ***符合 PCI DSS 要求 7***	**3.4.a** 根据*《PA-DSS 实施指南》*的要求安装支付应用程序，并在安装过程完成之后检查内置帐户的设置，以确认： • 所有应用程序/服务帐户仅具有其原本所需功能/资源的访问权限。 • 所有应用程序/服务帐户对其所需的每项功能/资源仅分配到最低级别的权限。	为了将对持卡人数据和敏感功能的访问限制在仅需要此类访问的帐户，必须为每个内置帐户定义访问需求和所需的权限级别，以便这些帐户可以执行指定的功能，但不会获得其他不必要的访问或权限。 分配最小权限可帮助预防对应用程序不甚了解的用户错误地或意外地更改应用程序配置或修改其安全设置。执行最小权限还能在非授权人员访问用户 ID 时最大限度地缩小损失范围。
	3.4.b 测试导致更改内置帐户的所有应用程序功能（包括导致用户帐户恢复默认设置、更改现有帐户配置、生成新帐户以及重新创建现有帐户的应用程序功能）。 对于已经执行的所有类型的更改，请检查内置帐户设置并测试应用程序功能，以确认在更改完成之后： • 所有应用程序/服务帐户仅具有其原本所需功能/资源的访问权限。 • 所有应用程序/服务帐户对其所需的每项功能/资源仅分配到最低级别的权限。	

要求 4：　　记录支付应用程序活动

PA-DSS 要求	测试程序	指南
4.1 安装过程完成时，支付应用程序的“开箱即用”式默认安装必须记录所有用户访问，并能将所有活动链接到单个用户。 ***符合 PCI DSS 要求 10.1***	**4.1.a** 安装支付应用程序。测试应用程序，确认支付应用程序检查记录在安装时自动启用。	支付应用程序具备下述流程或机制非常重要：可将用户关联到访问过的应用程序资源、生成检查日志并提供追溯可疑活动到特定用户的功能。事故后取证团队非常依赖这些日志以便发起调查。
	4.1.b 检查由供应商编制的*《PA-DSS 实施指南》*，确认其中包括以下说明： • 如何安装应用程序，以便在安装过程完成之后能够以默认方式配置和启用日志。 • 如何根据下面的 PA-DSS 要求 4.2、4.3 和 4.4 为安装后客户可配置的日志选项设置符合 PCI DSS 的日志设置。 • 日志不能禁用，如果禁用将导致不符合 PCI DSS。 • 对于支付应用程序包含或所需的第三方软件组件，如何为安装后客户可配置的日志选项配置符合 PCI DSS 的日志设置。	
4.2 支付应用程序必须提供自动检查记录以便重建以下事件： ***符合 PCI DSS 要求 10.2***	**4.2** 通过检查支付应用程序检查日志设置和检查日志输出，测试支付应用程序并执行以下操作：	记录 4.2.1 – 4.2.7 中的事件可使组织能够识别并跟踪潜在的恶意活动。
4.2.1 所有单个用户通过应用程序对持卡人数据进行访问	**4.2.1** 确认所有单个用户通过支付应用程序对持卡人数据进行的访问均已记录。	恶意个人可以获取通过应用程序访问持卡人数据的用户帐户信息，或者新建未经授权的帐户来访问持卡人数据。通过记录对持卡人数据的所有个人访问，可识别受到威胁或误用的帐户。
4.2.2 应用程序中分配有管理权限的任何个人所做的所有操作	**4.2.2** 确认对支付应用程序持有管理权限的任何个人所做的所有操作均已记录。	具有更高权限的帐户（例如“管理员”帐户）可能会对应用程序的安全性或操作功能产生极大影响。若不记录所执行的活动，则组织无法追踪到特定操作和个人产生的因管理员错误或权限误用导致的任何问题。
4.2.3 对由应用程序管理或其内部的应用程序检查记录的访问	**4.2.3** 确认对由应用程序管理或其内部的应用程序检查记录的访问均已记录。	恶意用户经常尝试修改检查日志以掩盖其操作，组织可通过访问记录跟踪单个帐户的任何不一致或可能被篡改的记录。

PA-DSS 要求	测试程序	指南
4.2.4 无效的逻辑访问尝试	**4.2.4** 确认无效的逻辑访问尝试均已记录。	恶意个人经常会对目标系统执行多次访问尝试。多次无效的登录尝试可说明非授权用户尝试“强制获得”或猜测密码。
4.2.5 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	**4.2.5** 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）进行的使用和更改，以及对应用程序帐户进行的任何更改、增加、删除均已记录。	如果不知道发生事故时登录的用户，就无法确定所使用的帐户。另外，恶意用户会尝试操纵验证控制来绕过控制或模仿有效帐户。包括但不限于创建新帐户、提升权限或更改访问权限之类的活动表明系统的验证机制可能遭到未经授权的使用。
4.2.6 初始化、停止或暂停应用程序检查日志	**4.2.6** 确认已记录以下内容： • 初始化应用程序检查日志 • 停止或暂停应用程序检查日志。	在执行非法活动之前关闭（或暂停）检查日志是恶意用户避免检测的常用方法。检查日志的初始化说明用户通过禁用日志功能来掩盖其操作。
4.2.7 创建和删除应用程序内的系统级对象，或者通过应用程序创建和删除系统级对象	**4.2.7** 确认创建和删除应用程序内的系统级对象，或者通过应用程序创建和删除系统级对象的操作均已记录。	恶意用户通常会在目标系统上创建或替换系统级对象以便控制特定的功能或该系统上的操作。通过在创建或删除系统级对象（例如数据库表或所存储的程序）时进行记录，可以更轻松地确定修改是否获得授权。
4.3 支付应用程序必须至少为每个事件记录以下检查记录条目： ***符合 PCI DSS 要求 10.3***	**4.3** 通过检查支付应用程序对每个可检查事件（来自 4.2）的检查日志设置和检查日志输出，测试支付应用程序并执行以下操作：	通过为 4.2 中可检查事件记录 4.3.1 – 4.3.6 中的详细信息，可以快速识别潜在的安全隐患，并且能够获得谁在何时何地以何种方式做过何种操作的详细信息。
4.3.1 用户识别	**4.3.1** 确认日志条目中包含用户识别。	
4.3.2 事件类型	**4.3.2** 确认日志条目中包含事件类型。	
4.3.3 日期和时间	**4.3.3** 确认日志条目中包含日期和时间戳。	
4.3.4 成功或失败指示	**4.3.4** 确认日志条目中包含成功或失败指示。	
4.3.5 事件的起因	**4.3.5** 确认日志条目中包含事件的起因。	
4.3.6 受影响的数据、系统组件或资源的特性或名称	**4.3.6** 确认日志条目中包含受影响的数据、系统组件或资源的特性或名称。	

PA-DSS 要求	测试程序	指南
4.4. 支付应用程序必须方便集中式记录。 ***注：****该功能可能包括，但不限于：* • 通过行业标准日志文件机制记录，例如通用日志文件系统 (CLFS)、Syslog、分隔文本等。 • 提供功能和文档将应用程序专有的日志格式转换为适合快速、集中式记录的行业标准日志格式。 ***符合 PCI DSS 要求 10.5.3***	**4.4.**a 检查由供应商编制的*《PA-DSS 实施指南》*，确认向客户和集成商/经销商提供： • 所支持的集中式记录机制的描述 • 将支付应用程序日志合并到集中式记录环境的说明和程序。 **4.4.b** 根据*《PA-DSS 实施指南》*的要求安装和配置支付应用程序，以确认提供了准确的说明，并且提供方便客户将日志归纳到集中式日志服务器的功能。	如果未对检查日志提供充分的保护，则无法保证其完整性和准确性，且检查日志会在遭受威胁后成为无用的调查工具。包括集中式记录系统中的支付应用程序日志可使客户集成和关联其日志，并在其环境中保证日志一致性。

要求 5：　　开发安全支付应用程序

PA-DSS 要求	测试程序	指南
5.1 软件供应商已经定义并实现支付应用程序安全开发的正式流程，其中包括： • 支付应用程序根据 PCI DSS 和 PA-DSS（例如安全验证和记录）开发。 • 开发过程基于行业标准和/或最优方法。 • 信息安全并入整个软件开发生命周期。 • 在应用程序发布或更新之前执行安全审核。 ***符合 PCI DSS 要求 6.3***	**5.1.a** 检查书面软件开发流程并确认流程基于行业标准和/或最优方法。	如果未在软件开发的要求定义、设计、分析和测试阶段纳入安全考虑，安全漏洞则会被无意或恶意地引入应用程序代码。
	5.1.b 确认书面软件开发流程包括以下程序： • 信息安全并入整个软件开发生命周期。 • 按照 PCI DSS 和 PA-DSS 要求开发支付应用程序。	
	5.1.c 确认书面软件开发流程包括： • 在应用程序发布或更新之前执行定义的安全审核。 • 执行安全审核程序以确保满足 PCI DSS 和 PA-DSS 的安全目标。	
	5.1.d 访问软件开发人员以确认遵守书面流程，例如： • 信息安全并入整个软件开发生命周期。 • 按照 PCI DSS 和 PA-DSS 要求开发支付应用程序。 • 在应用程序发布前执行安全审核，以确保实现安全目标，包括 PCI DSS 和 PA-DSS 要求。	
5.1.1 在测试或开发过程中不使用真实的 PAN。 ***符合 PCI DSS 要求 6.4.3***	**5.1.1.a** 审核软件开发流程，确认其中包括用于确保不将真实的 PAN 用于测试或开发过程的程序。	如果在应用程序发布之前需要使用真实的 PAN 来测试应用程序功能，支付卡品牌和众多收单机构能够提供适合测试的账号。
	5.1.1.b 观察测试流程并访问工作人员，确认没有将真实的 PAN 用于测试或开发过程。	
	5.1.1.c 检查部分测试数据，确认真实的 PAN 未用于测试或开发过程。	
5.1.2 在向客户发布之前，删除测试数据和帐户。 ***符合 PCI DSS 要求 6.4.4***	**5.1.2.a** 审核软件开发流程，确认其中包括用于确保在向客户发布支付应用程序之前删除测试数据和帐户的程序。	测试数据和帐户应该在应用程序发布给客户之前删除，因为包含这些项目可能会泄漏应用程序内部的关键构造信息。
	5.1.2.b 观察测试流程并访问工作人员，确认测试数据和帐户在向客户发布之前已删除。	
	5.1.2.c 检查最终支付应用程序产品，确认测试数据和帐户在向客户发布之前已删除。	

PA-DSS 要求	测试程序	指南
5.1.3 在向客户发布支付应用程序之前，删除自定义支付应用程序帐户、用户 ID 和密码 ***符合 PCI DSS 要求 6.3.1***	**5.1.3.a** 审核软件开发流程，确认其中包括用于确保在向客户发布支付应用程序之前已删除自定义支付应用程序帐户、用户 ID 和密码的程序。	预发布的自定义帐户、用户 ID 和密码可能会被开发人员或其他对该帐户非常了解的个人用作后门以获得对应用程序的访问权，并且会为破坏应用程序及相关持卡人数据提供可乘之机。
	5.1.3.b 观察测试流程并访问工作人员，确认自定义支付应用程序帐户、用户 ID 和密码在支付应用程序发布给客户之前已删除。	
	5.1.3.c 检查最终支付应用程序产品，确认自定义支付应用程序帐户、用户 ID 和密码在支付应用程序发布给客户之前已删除。	
5.1.4 在任何重大变更后，支付应用程序代码会在发布给客户之前进行审核，以便识别任何潜在的编码漏洞（使用手动或自动流程），其中至少包括： • 代码变更由代码原作者以外人员以及熟悉代码审核方法和安全编码实践的人员进行审核。 • 执行代码审查以确保代码按照安全编码指南进行开发。（参见 PA-DSS 要求 5.2。） • 发布前已进行适当修正。 • 代码审查结果在发布前已由管理人员审核并批准。 • 代码审核结果文档包括管理者审批、代码作者和代码审核者，以及发布前实施的修正。 ***注：****这项代码审核要求适用于所有支付应用程序组件（包括内部和面向公众的 web 应用程序），并作为系统开发生命周期的一部分。代码审核可由经验丰富的内部人员或第三方执行。* ***符合 PCI DSS 要求 6.3.2***	**5.1.4.a** 检查书面软件开发程序并访问责任工作人员，确认供应商对所有重大应用程序代码变更执行代码审核（使用手动或自动流程），具体如下： • 代码变更由代码原作者以外人员以及熟悉代码审核方法和安全编码实践的人员进行审核。 • 执行代码审查以确保代码按照安全编码指南进行开发。（参见 PA-DSS 要求 5.2。） • 发布前已进行适当修正。 • 代码审查结果在发布前已由管理人员审核并批准。 • 代码审核结果记录包括管理者审批、代码作者和代码审核者，以及发布前实施的修正。	恶意个人通常会利用应用程序代码中的安全漏洞来获取对网络的访问权并攻击持卡人数据。为防止此类攻击，应采用适当的代码审核技术。 代码审核技术应确认在整个开发过程中均采用安全编码最优方法。应用程序供应商应在适用时将相关安全编码实践并入所使用的特定技术。 应由熟悉该技术且在代码审核技术方面经验丰富的人员执行审核，以便识别出潜在的编码问题。指定代码开发人员以外的其他人员执行代码审核，以实现独立、客观的审核。 在代码发布之前纠正编码错误可防止错误代码将客户环境暴露给潜在的攻击者。而且错误代码在部署之后将更难纠正且代价更高。管理人员在发布前进行正式审核并签字有助于确保代码通过审批，并已按政策与程序进行开发。
	5.1.4.b 针对部分更改的代码，检查代码审核结果，以确认： • 代码审核由代码作者以外的经验丰富的人员执行。 • 代码审核按照安全编码指南制定。 • 在发布前已实施适当的修正。 • 代码审核结果在发布之前已由管理人员审核和批准。	

PA-DSS 要求	测试程序	指南
5.1.5 实行安全源控制实践以确认开发过程中源代码的完整性。	**5.1.5.a** 检查书面软件开发程序并访问责任工作人员，确认供应商维持安全源控制实践以确定开发过程中源代码的完整性。 **5.1.5.b** 检查机制并观察确保源代码安全的程序，确认开发过程中能够保持源代码的完整性。	良好的源代码控制实践有助于确保所有代码变更都按照计划实施并得到授权，而且仅由具备更改代码正当原因的人员执行。此类实践包括具备严格访问控制的代码签入和签出程序，以及在更新代码之前立即进行比较以确认上次审批过的版本未被更改（例如，使用校验和）。
5.1.6 支付应用程序根据安全编码技术行业最优方法进行开发，包括： • 使用应用程序环境最小权限进行开发。 • 利用故障保护默认值开发（除非在最初的设计阶段有规定，否则默认拒绝所有执行）。 • 针对所有接入点综合考虑进行开发，包括应用程序的多通道输入等的输入变化。	**5.1.6.a** 检查软件开发流程，确认安全编码技术已定义并包括： • 使用应用程序环境最小权限进行开发。 • 利用故障保护默认值开发（除非在最初的设计阶段有规定，否则默认拒绝所有执行）。 • 针对所有接入点综合考虑进行开发，包括应用程序的多通道输入等的输入变化。 **5.1.6.b** 访问开发人员，确认应用程序根据安全编码技术行业最优方法进行开发，包括： • 使用应用程序环境最小权限进行开发。 • 利用故障保护默认值开发（除非在最初的设计阶段有规定，否则默认拒绝所有执行）。 • 针对所有接入点综合考虑进行开发，包括应用程序的多通道输入等的输入变化。	使用最小权限开发应用程序是确保不安全假设不被引入应用程序的最有效方式。包括故障保护默认值可防止攻击者获取有关应用程序故障的敏感信息，这些信息可用于发起后续攻击。确保安全性应用于所有访问和应用程序输入可避免输入通道可能保持打开而受到破坏的可能性。开发代码时如果没有考虑这些概念会导致不安全应用程序的发布和之后可能采取的大量补救措施。

PA-DSS 要求	测试程序	指南
5.1.6.1 编码技术包括如何在内存中处理 PAN 和/或 SAD 的文档。	**5.1.6.1.a** 检查编码技术，确认其中包括如何在内存中处理 PAN 和/或 SAD 的相关文档。	攻击者会利用恶意软件工具捕获内存中的敏感数据。最大限度地减少内存中 PAN/SAD 的暴露，有助于降低其被恶意用户捕获或被不知不觉保存到某个内存文件中的磁盘上且不受保护的可能性。 本要求旨在确保考虑内存中 PAN 和 SAD 的处理方法。 了解敏感数据在内存中出现的时间、保持的时间以及存在的格式，有助于应用程序供应商识别其应用程序中的潜在不安全因素并决定是否采取需要额外保护。 该活动是否能产生任何编码技术取决于所要开发的特定软件及所使用的技术。
	5.1.6.1.b 访问开发人员，确认他们在应用程序开发过程中考虑了如何在内存中处理 PAN/SAD。	

PA-DSS 要求	测试程序	指南
5.1.7 至少每年为应用程序开发人员提供一次安全开发实践方面的最新培训，这些培训应适用于开发人员的工作职能和所使用的技术，例如： • 安全应用程序设计 • 避免常见编码漏洞的安全编码技术（例如，供应商指南、OWASP 前十大威胁、前 25 大高危软件错误、CERT 安全编码等） • 管理内存中的敏感数据 • 代码审核 • 安全性测试（例如渗透测试技术） • 风险评估技术。 ***注：****针对应用程序开发人员的培训可由内部或第三方提供。培训的开展方式包括在职培训、讲师授课和基于计算机的培训。*	**5.1.7a** 确认书面软件开发流程要求至少每年为应用程序开发人员提供一次安全开发实践方面的最新培训，这些培训应适用于开发人员的工作职能和所使用的技术。 **5.1.7.b** 抽取部分开发人员进行面谈，确认他们熟悉适合所用技术的安全开发方法和编码技术。 **5.1.7.c** 检查培训记录，确认所有应用程序开发人员至少每年接受一次适用于他们工作职能和所用技术的培训。	确保开发人员熟悉安全开发实践将有助于最大限度减少通过不良编码实践而引入的安全漏洞数量。接受过培训的人员也更能识别应用程序设计和代码中的潜在安全问题。软件开发平台和方法经常变化，软件应用程序面临的威胁和风险也是如此。安全开发方法培训应与不断变化的最新开发方法保持一致。
5.1.7.1 根据需要更新培训来介绍所使用的新开发技术和方法。	**5.1.7.1** 检查培训材料并抽取部分开发人员进行面谈，确认根据需要更新培训来介绍所使用的新开发技术和方法。	
5.2 开发所有支付应用程序来防止软件开发流程中的常见编码漏洞。 ***注：****在本版本 PA DSS 发布时，已采用行业最优方法将 PA-DSS 要求 5.2.1 到 5.2.10 和 PCI DSS 6.5.1 到 6.5.10 中列举的漏洞保持为最新。但当有关漏洞管理的行业最优方法（例如 OWASP 前十大威胁、前 25 大高危软件错误、CERT 安全编码等）出现更新时，这些要求必须采用当下最新的最优方法。* ***符合 PCI DSS 要求 6.5***	**5.2** 通过实施手动或自动的穿透测试，确认该应用程序不易受到常见编码漏洞的攻击。所使用的穿透测试须专门尝试利用以下每项内容：	应用层是高风险层，可能成为内部和外部威胁的目标。如果没有恰当的安全措施，持卡人数据和其他公司保密信息可能会暴露。 要求 5.2.1 到 5.2.10 是应具备的最低控制要求。本列表包含本版本 PA-DSS 发布时最常见的编码漏洞。当行业认可的常见编码漏洞改变时，供应商编码实践也应相应更新。
注：*下文的要求 5.2.1 到 5.2.6 适用于所有支付应用程序（内部或外部）：*		

PA-DSS 要求	测试程序	指南
5.2.1 注入攻击，特别是 SQL 注入。同时还须考虑 OS 命令注入、LDAP、XPath 等其他注入攻击。	**5.2.1** 注入攻击（特别是 SQL 注入）可通过以下编码技术解决： • 验证输入，以确认用户数据无法修改命令和查询的意思 • 利用参数化查询。	注入攻击，特别是 SQL 注入，是破坏应用程序的一种常用方法。当用户提供的数据作为命令或查询的一部分被发送到解释器时，就发生了注入。攻击者的恶意数据会诱导解释器执行非计划的命令或修改数据，从而使应用程序内的组件遭受缓冲区溢出等攻击。 所有输入数据在处理前均应经过应用程序验证 — 例如，通过检查所有字母字符、字母与数字混合字符等
5.2.2 缓冲区溢出	**5.2.2** 缓冲区溢出可通过以下编码技术解决： • 验证缓冲区边界 • 截取输入字符串。	当应用程序在其缓冲区空间上没有适当的检查范围时，则发生缓冲区溢出。这可能造成缓冲区内的信息被挤出缓冲区存储空间，而进入可执行的存储空间。当发生这种情形时，攻击者能在缓冲区的末端插入恶意代码，并通过促使缓冲区溢出将该恶意代码推入可执行的存储空间。随后，攻击者将执行该恶意代码并经常借机远程访问该应用程序和/或被感染的系统。
5.2.3 非安全加密存储	**5.2.3** 非安全加密存储可通过以下编码技术解决： • 防止密码攻击 • 采用强效加密算法和密钥。	未适当利用强效加密功能存储数据的应用程序受到威胁、泄露验证凭证和/或持卡人数据的风险会增大。
5.2.4 非安全通信	**5.2.4** 非安全通信可通过正确验证和加密所有敏感通信的编码技术来解决。	未采用强效加密法对敏感网络流量进行充分加密的应用程序受到威胁和泄露持卡人数据的风险会增加。

PA-DSS 要求	测试程序	指南
5.2.5 不正确的错误处理	**5.2.5** 不正确的错误处理可采用不会通过错误消息泄露信息的编码技术解决（例如通过返回一般而非具体的错误详情）。	泄露关于其配置和内部工作方式的信息、或通过不正确的错误处理方法泄露专用信息的应用程序会面临威胁风险。攻击者会利用这一漏洞窃取敏感数据，或威胁整个系统。如果恶意个人能够创建应用程序未正确处理的错误，他们便能获得详细的系统信息、创建拒绝服务中断、引起安全故障，或导致应用程序或系统崩溃。例如，“提供的密码不正确”这一消息就在告诉攻击者其提供的用户 ID 是正确的，他们应该只关注攻击密码。使用较通用的错误消息，例如“数据无法验证”。
5.2.6 PA-DSS 要求 7.1 的漏洞识别流程中确认的所有“高风险”漏洞	**5.2.6** 编码技术可解决任何可能影响应用程序的“高风险”漏洞，具体规定请参阅 PA-DSS 要求 7.1。	所有通过供应商漏洞风险分级流程（具体规定请参阅 PA-DSS 要求 7.1）确定为“高风险”的漏洞以及可能影响应用程序的漏洞均应在应用程序开发期间找到并解决。
注：*下文的要求 5.2.7 到 5.2.10 适用于基于 web 的应用程序和应用程序接口（内部或外部）：*		Web 应用程序因其架构特性具有独特的安全风险，较易受到威胁。
5.2.7 跨站点脚本 (XSS)	**5.2.7** 跨站点脚本 (XSS) 可通过以下编码技术解决： • 所有参数在应用前均进行验证 • 利用上下文相关的转义。	只要应用程序接收用户提供的数据并在未首先验证或编译内容的情况下将其发送到一个 web 浏览器，则发生 XSS 攻击。攻击者可通过 XSS 在受害人的浏览器中执行脚本，从而劫持用户会话、破坏网站外观、引入蠕虫等。

PA-DSS 要求	测试程序	指南
5.2.8 不正确的访问控制（例如不安全的直接对象引用、未能限制 URL 访问和目录遍历）	**5.2.8** 不正确的访问控制（例如不安全的直接对象引用、未能限制 URL 访问和目录遍历）可通过以下编码技术解决： • 正确的用户验证 • 净化输入 • 不向用户暴露内部对象引用 • 不允许访问未授权功能的用户界面。	当开发人员将引用作为 URL 或形式参数暴露给内部执行对象（例如文件、目录、数据库记录或密钥）时，则发生直接对象引用。攻击者可利用这些引用在未授权的情况下访问其他对象。 能列举并导航一个网站的目录结构（目录遍历）的攻击者可获得未授权信息的访问权限并进一步洞悉网站的运行方式，以供以后利用。 允许访问未授权功能的用户界面可能导致未经授权的个人获得专用凭证或持卡人数据的访问权限。限制数据资源的访问权有助于防止向未授权资源显示持卡人数据。
5.2.9 跨站请求伪造 (CSRF)	**5.2.9** 跨站点请求伪造 (CSRF) 可通过确保应用程序不信任由浏览器自动提交的授权凭证和令牌的编码技术来解决。	CSRF 攻击会迫使已登录的受害者浏览器向一个存在漏洞的 web 应用程序发送预先验证的请求，随后攻击者便能执行受害人获准执行的任何状态变更操作（例如更新帐户明细、买入，甚至验证该应用程序）。
5.2.10 失效的验证与会话管理	**5.2.10** 通常，失效的验证与会话管理可通过以下编码技术解决： • 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。	安全验证和会话管理可防止未授权个人破坏合法的帐户凭证、密钥或会话令牌，如若不然，入侵者可能会占用授权用户的身份。
5.3 软件供应商在对所有应用程序进行变更时必须遵循变更控制程序。变更控制程序必须遵循与新版本相同的软件开发流程（具体规定请参阅 PA-DSS 要求 5.1）并包括以下内容： ***符合 PCI DSS 要求 6.4.5***	**5.3.a** 检查供应商进行软件修改的变更控制程序，并： • 确认程序遵循要求 5.1 中规定的书面软件开发流程 • 确认程序需要下文的 5.3.1 – 5.3.4 项。	如果管理不当，软件更新和安全补丁的效果可能得不到完全实现，并且可能造成无法预料的后果。
	5.3.b 与开发人员面谈，确定支付应用程序的最新变更。检查支付应用程序的最新变更情况，查询与变更相关的变更控制文件资料。对于每次检查过的变更情况，确认已按照变更控制程序对以下内容作了记录：	

PA-DSS 要求	测试程序	指南
5.3.1 影响记录	**5.3.1** 确认每次变更情况的变更控制文件已包含对客户影响的记录。	应记录变更影响，以便所有相关方能针对任何处理中的变更制定相应计划。
5.3.2 相关被授权方的变更审批记录	**5.3.2** 确认每次变更都有相关被授权方的审批记录。	获被授权方批准表明该变更是管理层认可的经批准的合法变更。
5.3.3 功能测试，以确认该变更未对系统安全性造成不利影响	**5.3.3.a** 确认已执行功能测试，以确认该变更未对系统安全性造成不利影响。 **5.3.3.b** 确认所有变更（包括补丁）在发布之前均经过测试证实符合 5.2。	通过执行全面的测试，确认支付应用程序的安全性未因实施变更而降低。应通过测试确认在应用程序发生任何变更后，所有现行安全控制措施仍然有效、为同样有力的控制措施取代或得到加强。
5.3.4 取消或产品卸载程序	**5.3.4** 确认已为每次变更准备好了取消或产品卸载程序。	每次变更都应有取消程序，如果变更失败或对应用程序的安全产生不利影响，即可将应用程序恢复到之前的状态。
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。该方法必须遵循*《PA-DSS 计划指南》*中的支付应用程序变更程序并至少包含以下内容：	**5.4** 检查书面软件开发流程，确认其包括软件供应商的版本控制方法且要求该版本控制方法符合《PA-DSS 计划指南》。 确认要求支付应用程序（包括支付应用程序的所有变更）遵循书面版本控制方法。	如果没有全面定义的版本控制方法，可能无法准确识别应用程序变更，客户和集成商/经销商也可能无法理解应用程序版本变更带来的影响。
5.4.1 版本控制方法必须定义所使用的特定版本元素，包括： • 详细说明如何使版本方案的元素符合*《PA-DSS 计划指南》*中指定的要求。 • 版本方案的格式，包括元素数量、分隔符、字符集等（包含字母、数字和/或字母数字字符）。 • 定义版本方案中每个元素表示的含义（例如，变更类型、重要、次要或维护版本、通配符等） • 定义表示通配符使用的元素。	**5.4.1.a** 检查书面版本控制方法，确认其包含以下内容： • 详细说明如何使版本编号方案的元素符合*《PA-DSS 计划指南》中指定的要求。* • 指定了版本编号方案的格式，其中包括元素数量、分隔符、字符集等（以 1.1.1.N 为例，包含字母、数字和/或字母数字字符）的详情。 • 定义版本编号方案中每个元素表示的含义（例如，变更类型、重要、次要或维护版本、通配符等） • 定义表示通配符使用的元素。 **5.4.1.b** 确认版本方案的元素符合《PA-DSS 计划指南》中指定的变更类型。	支付应用程序供应商版本控制方法应包含指定的版本方案，该方案详细说明特定支付应用程序所使用的元素、版本格式、不同版本元素的层次结构等。 版本方案应明确指定在版本号中使用各个元素的方法。 版本方案可用多种方法表示，例如，N.NN.NNA，其中“N”表示数字元素，“A”表示字母元素。版本控制方案应说明版本中的每个元素可使用的字符集 （例如，0-9、A-Z 等）。

PA-DSS 要求	测试程序	指南
注：*通配符只能由表示不影响安全的变更的版本号元素替换。请参见 5.4.3，了解通配符使用的更多要求。*	**5.4.1.c** 选取部分最近所做的支付应用程序变更、所分配的版本号以及规定应用程序变更类型的变更控制文件资料，并确认版本号中的元素符合书面版本控制方法定义的相应变更和参数。	如果没有正确定义的版本方案，版本号格式可能无法准确表示对应用程序所做的变更。
	5.4.1.d 抽取部分开发人员进行面谈，确认他们熟悉版本方案，包括通配符在版本号中的恰当使用。	
5.4.2 版本控制方法必须根据*《PA-DSS 计划指南》*说明所有应用程序变更的类型和影响，包括： • 说明所有应用程序变更的类型和影响。 • 以下变更的详细识别方法和定义： - 不影响应用程序或其依赖项的功能的变更 - 影响应用程序功能但不影响 PA-DSS 要求的安全性的变更 - 影响任何安全功能或 PA-DSS 要求的变更。 • 如何将每种类型的变更与特定的版本号相关联。	**5.4.2.a** 检查软件供应商的书面版本控制方法，确认版本控制方法包括： • 应用程序变更的所有类型和影响的说明（例如对应用程序没有影响、有少量影响或有重要影响的变更） • 以下变更的详细识别方法和定义： - 不影响应用程序或其依赖项的功能的变更 - 影响应用程序功能但不影响 PA-DSS 要求的安全性的变更 - 影响任何安全功能或 PA-DSS 要求的变更。 • 如何将每种类型的变更与特定的版本号相关联。	
	5.4.2.b 确认版本控制方法符合*《PA-DSS 计划指南》*的要求。	
	5.4.2.c 与人员面谈并查看每种变更的流程，确认所有类型的变更均遵循书面方法。	
	5.4.2.d 选择支付应用程序的部分最新变更并审查规定应用程序变更类型的变更控制文件资料，从而根据书面方法确认分配给变更的版本符合变更类型。	

PA-DSS 要求	测试程序	指南
5.4.3 版本控制方法必须明确说明是否使用通配符，如果是，还需说明其使用方法。它必须包含以下内容： • 通配符在版本控制方法中的具体使用方法。 • 不得将通配符用于对安全性或任何 PA-DSS 要求有影响的任何变更。 • 用来表示不影响安全的变更的任何版本号元素（包括通配符元素）绝不能用来表示影响安全的变更。 • 通配符元素不得位于可表示影响安全的变更的版本元素之前。位于通配符元素之后的任何版本元素均不能用来表示影响安全的变更。 ***注：****通配符的使用必须符合《PA-DSS 计划指南》的要求。*	**5.4.3.a** 检查软件供应商的书面版本控制方法，确认其包含通配符的详细使用方法，包括： • 通配符在版本控制方法中的具体使用方法。 • 不得将通配符用于对安全性或任何 PA-DSS 要求有影响的任何变更。 • 用来表示不影响安全的变更的任何版本号元素（包括通配符元素）绝不能用来表示影响安全的变更。 • 位于通配符右侧的任何元素均不得用于影响安全的变更。体现影响安全的变更的版本元素须显示在第一个通配符元素的“左侧”。	PA-DSS“通配符”元素可用于在版本方案中表示多个不影响安全的变更。 通配符是供应商版本方案的唯一可变元素，用来说明用通配符元素表示的每个版本之间只有不影响安全的次要变更。例如，版本号 1.1.x 可涵盖特定版本 1.1.2 和 1.1.3 等，使客户了解除了外观变化或其他次要类型的变更，它们之间的基本代码实际未变。 通配符的任何使用都必须在供应商的版本控制方法中预定义，且必须符合*《PA-DSS 计划指南》*的要求。 ***注：****通配符的使用为可选，没有强制要求。*
	5.4.3.b 确认任何通配符的使用均符合*《PA-DSS 计划指南》*的要求。例如，显示在通配符元素后面的元素不可用于影响安全的变更。	
	5.4.3.c 与人员面谈并查看每种变更的流程以确认： • 不得将通配符用于对安全性或任何 PA-DSS 要求有影响的任何变更。 • 用来表示不影响安全的变更的版本号元素（包括通配符元素）从没有用于表示影响安全的变更。	
	5.4.3.d 选择支付应用程序的部分最新变更并审查规定应用程序变更类型的变更控制文件资料。确认： • 通配符没有用于对安全性或任何 PA-DSS 要求有影响的任何变更。 • 用来表示不影响安全的变更的版本号元素（包括通配符元素）没有用于表示影响安全的变更。	

PA-DSS 要求	测试程序	指南
5.4.4 供应商的已发布版本控制方法必须传达给客户和集成商/经销商。	**5.4.4** 确认*《PA-DSS 实施指南》*包含针对客户和集成商/经销商的供应商已发布版本控制方法的说明，并包含以下详情： • 版本控制方案详情，包括版本方案的格式（元素数量、分隔符、字符集等）。 • 版本方案如何表示影响安全的变更的相关详情。 • 其他类型的变更如何影响版本的相关详情。 • 所使用的任何通配符元素的详情，包括确认其绝不会用于表示影响安全的变更。	确保包含在*《PA-DSS 实施指南》*中的供应商版本控制方法会为客户和集成商/经销商提供理解其所使用的支付应用程序版本所需的信息，以及他们对每个支付应用程序版本所进行的变更的类型。
5.4.5 如果使用内部版本到已发布版本控制方案的映射，则版本控制方法必须包含内部版本到外部版本的映射。	**5.4.5.a** 检查书面版本控制方法，确认其包含内部版本到已发布外部版本的映射。	部分支付应用程序供应商有供内部使用或参考的版本控制方法，它们不同于用于外部（或公共）发布的版本控制方法。在这种情况下，对两种版本控制方法进行完善的定义和记录并全面记录它们之间的关系很重要。
	5.4.5.b 检查最新变更情况，确认映射到已发布版本控制方案的内部版本符合书面方法中定义的变更类型。	
5.4.6 软件供应商必须具备相关流程，以在发布应用程序更新前审查其是否符合版本控制方法。	**5.4.6.a** 检查书面软件开发流程和版本控制方法，确认具备相关流程，以在发布应用程序更新前审查其是否符合版本控制方法。	支付应用程序供应商具备相关流程来确保产品更新符合计划发布的目的和范围并且这些变更准确传达给客户至关重要。否则，可在客户不知情的情况下对应用程序进行有不良安全影响的变更。
	5.4.6.b 与软件开发人员面谈并查看流程，确认在发布应用程序更新前审查其是否符合版本控制方法。	

PA-DSS 要求	测试程序	指南
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缺陷和漏洞。风险评估流程包括以下内容： • 涵盖支付应用程序的所有功能，包括但不限于影响安全的功能和跨信任边界的功能。 • 应用程序决策点、流程、数据流、数据存储和信任边界的评估。 • 支付应用程序中与 PAN 和/或 SAD 或持卡人数据环境 (CDE) 交互的所有区域，以及可能导致持卡人数据泄露的流程导向结果的识别。 • 来自持卡人数据流分析的潜在威胁和漏洞列表，且每一项都分配有风险等级（例如，高、中或低优先级）。 • 在开发流程中实施恰当的更正和对策。 • 记录风险评估结果，供管理层审核和批准。	**5.5** 检查书面软件开发程序并与责任工作人员面谈，确认供应商在软件开发流程中使用风险评估技术，且该流程包括： • 涵盖支付应用程序的所有功能，包括但不限于影响安全的功能和跨信任边界的功能。 • 应用程序决策点、流程、数据流、数据存储和信任边界的评估。 • 支付应用程序中与 PAN 和/或 SAD 或持卡人数据环境 (CDE) 交互的所有区域，以及可能导致持卡人数据泄露的流程导向结果的识别。 • 来自持卡人数据流分析的潜在威胁和漏洞列表，且每一项都分配有风险等级（例如，高、中或低优先级）。 • 在开发流程中实施恰当的更正和对策。 • 记录风险评估结果，供管理层审核和批准。	为了维护支付应用程序的质量和安全，应用程序供应商应在软件开发流程中采用风险评估技术。 威胁建模是一种风险评估方法，可用来分析应用程序的构成和数据流，了解将保密信息暴露给未授权的应用程序用户的可能性。这些流程允许软件开发人员和架构师在开发流程的早期识别并解决潜在的安全问题，从而提高应用程序安全性并最大程度地降低开发成本。
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。记录包括： • 正式批准应用程序或应用程序更新发布的授权方签字 • 供应商遵循安全开发流程的确认书。	**5.6.a** 检查书面流程，确认应用程序和任何应用程序更新的最终发布必须经过正式批准和记录，包括正式批准发布的授权方签字以及遵循所有 SDLC 流程的确认书。 **5.6.b** 抽取部分最新发布的应用程序和应用程序更新，审查批准文件来确认其包含： • 授权方的正式批准和签名 • 遵循所有安全开发流程的确认书。	支付应用程序供应商机构内部应该有人负责审查并确保已执行安全开发流程的所有方面（具体规定请参阅要求 5.1 到 5.5）。如果没有责任方的正式审核和确认，可能会遗漏或缺失关键的安全流程，导致应用程序产生故障或不够安全。

要求 6：　　保护无线传输

PA-DSS 要求	测试程序	指南
6.1 对于使用无线技术的支付应用程序，变更无线供应商默认值，包括但不限于默认的无线密钥、密码和 SNMP 社区字符串。无线技术必须安全实施。 ***符合 PCI DSS 要求 1.2.3 和 2.1.1***	**6.1** 对于使用无线技术的支付应用程序，以及与支付应用程序捆绑的所有无线应用程序，确认无线应用程序未使用供应商的默认设置，详情如下：	无线技术的利用是恶意个人访问网络和持卡人数据的常用方法。若无线网络未实施足够的安全配置（包括变更默认设置），则无线嗅探器可窃听流量、轻松捕获数据和密码并轻易进入并攻击网络。为此，支付应用程序不得使用默认值或非安全的无线设置。 如果防火墙不限制无线网络对 CDE 的访问，则非授权访问无线网络的恶意个人可轻松连接到 CDE 并威胁帐户信息的安全性。
	6.1.a 检查由供应商编制的*《PA-DSS 实施指南》*，确认其包含针对客户和集成商/经销商的如下说明： • 支付应用程序在安装受其控制的所有无线组件时对默认密钥、密码和 SNMP 社区字符串进行了强制性变更。 • 知道密钥/密码的人离开公司或调动职位时，无线密钥和密码（包括 SNMP 字符串）的变更程序。 • 随支付应用程序一起提供但不受其控制的任意无线组件的默认密钥、密码和 SNMP 社区字符串的变更说明。 • 在任意无线网络和存储持卡人数据的系统之间安装防火墙的说明。 • 支付应用程序的无线功能使用的任何无线流量的详情（包括详细的端口信息）。 • 配置防火墙来拒绝或（若出于业务需要需使用这些流量）仅允许无线环境和持卡人数据环境间的授权流量的说明。	
	6.1.b 对于受支付应用程序管理的所有无线功能，根据*《PA-DSS 实施指南》*安装应用程序并测试应用程序和无线设置来确认以下内容： • 密钥默认值在安装时已更改。 • 无线设备的默认 SNMP 社区字符串在安装时已更改。 • 接入点的默认密码/口令在安装时已更改。 • 已更新无线设备的固件来支持通过无线网络进行的验证和传输的强效加密。 • 其他与安全有关的无线供应商默认值已更改（若适用）。	
	6.1.c 对于支付应用程序管理的所有无线功能，请遵循*《PA-DSS 实施指南》*中变更无线密钥、密码/口令和 SNMP 字符串的说明。确认*《PA-DSS 实施指南》*中的说明准确且能确保变更无线密钥、密码和 SNMP 字符串。	

PA-DSS 要求	测试程序	指南
	6.1.d 对于随支付应用程序一起提供但不受其控制的所有无线组件，遵循*《PA-DSS 实施指南》*中变更默认密钥、密钥/口令和 SNMP 社区字符串的说明。确认*《PA-DSS 实施指南》*中的说明准确且能确保变更无线密钥、密码和 SNMP 字符串。	
	6.1.e 安装应用程序并测试无线功能，确认应用程序使用的无线流量和端口符合*《PA-DSS 实施指南》*的要求。	
6.2 使用无线技术的支付应用程序必须便于使用行业最优方法（例如，IEEE 802.11i）来实施验证和传输的强效加密。 ***注：****禁止将 WEP 用作安全控制。* ***符合 PCI DSS 要求 4.1.1***	**6.2.a** 对于使用无线技术的支付应用程序，测试所有无线功能以确认应用程序使用行业最优方法（例如，IEEE 802.11.i）来为验证和传输提供强效加密。	恶意用户使用可轻松获取的免费工具来窃听无线通信。使用强效加密法可限制无线网络中敏感信息的泄漏。 对于持卡人数据的验证和传输，必须使用强效加密术来防止恶意用户访问无线网络中的数据或利用无线网络来访问其他系统或数据。
	6.2.b 对于与支付应用程序捆绑的所有无线应用程序，测试无线功能以确认应用程序使用行业最优方法（例如，IEEE 802.11.i）来为验证和传输提供强效加密。	
	6.2.c 检查供应商编制的*《PA-DSS 实施指南》*，确认其包含针对客户和集成商/经销商的如下说明： • 配置应用程序以使用行业最优方法（例如，IEEE 802.11.i）来为验证和传输提供强效加密的方法，和/或 • 如何配置所有与支付应用程序捆绑在一起的无线应用程序，以使用行业最优方法对验证和传输实施强效加密。	
6.3 为客户提供安全使用无线技术的说明， ***注：****此要求适用于所有支付应用程序，无论该应用程序是否为配合无线技术使用而研发。* ***符合 PCI DSS 要求 1.2.3、2.1.1 和 4.1.1***	**6.3** 检查由供应商编制的*《PA-DSS 实施指南》*，确认为客户和集成商/经销商提供有关符合 PCI DSS 的无线设置的如下指导： • 关于在安装时更改所有无线默认密钥、密码和 SNMP 社区字符串的说明。 • 关于知道密钥的任何人离职或更换岗位时即更改无线密钥、密码和 SNMP 字符串的说明。 • 关于在所有无线网络和持卡人数据系统间安装防火墙，并配置防火墙以拒绝流量或（如果出于业务需要需使用流量）仅允许无线环境和持卡人数据环境间的授权流量的说明。 • 关于使用行业最优方法（例如，IEEE 802.11.i）对验证和传输实施强效加密的说明。	支付应用程序供应商应向客户提供配置该应用程序以支持使用无线技术的指导说明，即使该应用程序并非明确设计配合无线环境使用。无线网络十分普遍，客户应了解应该实施哪些常见无线安全设置，才能确保支付应用程序的安全。

要求 7：　　针对漏洞测试支付应用程序并实时更新支付应用程序

PA-DSS 要求	测试程序	指南
7.1 软件供应商必须制定发现和管理漏洞的流程，具体如下： ***注：****该流程必须包括与支付应用程序一起提供或其要求使用的底层软件或系统（例如：网络服务器、第三方库文件与程序）。* ***符合 PCI DSS 要求 6.1***	**7.1.a** 检查漏洞管理流程文档，确认将程序定义为： • 使用可信外源识别新安全漏洞，获取安全漏洞信息 • 为所有已识别的漏洞指定风险等级 • 发布前，对支付应用程序进行测试和更新，了解有无漏洞存在。 **7.1.b** 确认用于确定新安全漏洞与纠正支付应用程序的流程可以适用于与支付应用程序一起提供或其要求使用的所有软件（例如：网络服务器、第三方库文件与程序）。	供应商需及时更新可能影响其应用程序的新漏洞，包括底层组件中的漏洞或该应用程序打包或要求使用的软件。 支付应用程序供应商知道其应用程序或底层组件存在漏洞后，应能在发布前解决这些漏洞，或实施其他机制，从而降低该漏洞在第三方安全补丁无法立即使用的情况下被利用的风险。
7.1.1 使用可信外源识别新安全漏洞，获取安全漏洞信息。	**7.1.1** 与负责人员面谈并查看流程，确认新安全漏洞已被识别： • 位于支付应用程序和与支付应用程序一起提供或其要求使用的底层软件或系统中 • 使用可信来源（如软件/系统供应商网站、国家标准与技术研究所的国家漏洞数据库、MITRE 的常见漏洞和暴露清单及美国国土安全部的 US-CERT 网站）。	可信外源应用于获取漏洞信息和/或第三方软件组件中的补丁。漏洞信息来源应当可信，并且通常包含供应商网站、行业新闻组、邮件列表或 RSS 反馈。行业来源的示例包括：国家标准与技术研究所 (NIST) 的国家漏洞数据库、MITRE 的常见漏洞和暴露清单及美国国土安全部的 US-CERT 网站。
7.1.2 为所有已识别的漏洞指定风险等级，包括与支付应用程序一起提供或其要求使用底层软件或系统中出现的漏洞。 ***注：****风险等级应以行业最优方法和潜在影响考虑为依据。例如，漏洞分级标准可能包括对 CVSS 基础得分的考虑及/或供应商的分类及/或对应用程序功能的影响。* *风险等级至少应标识出所有被视为对应用程序具有“高风险”的漏洞。除风险等级外，如果安全漏洞将造成威胁、影响关键系统组件，或如果不解决可能会造成潜在危害，则可被视为“重要”。*	**7.1.2** 与负责人员面谈并查看流程，确认已为新的安全漏洞指定风险等级，包括与支付应用程序一起提供或其要求使用底层软件或系统中出现的漏洞。	当供应商发现可能影响其应用程序的漏洞后，必须评估该漏洞产生的风险并确定风险等级。这需要制定积极监控漏洞信息行业来源的流程。 供应商能够通过风险分类（例如“高”、“中”或“低”）识别和优先解决风险最高的项目（如：更快地发布高优先级的补丁），降低对客户环境风险最大的漏洞被利用的可能性。

PA-DSS 要求	测试程序	指南
7.1.3 发布前，对支付应用程序进行测试并更新暴露的漏洞	**7.1.3** 与责任工作人员面谈并查看流程，确认支付应用程序在发布前已接受漏洞测试。	支付应用程序供应商的漏洞管理流程中应包含足够的测试，确保已识别的漏洞在发布前得到相应的解决。 *测试方法示例包括用来识别潜在漏洞的穿透测试和/或模糊测试技术，例如：通过输入不良数据或非预期数据，或修改数据的位大小。*
7.2 软件供应商必须制定用以及时研发和部署安全补丁及更新的相应流程。	**7.2** 检查研发和发布安全补丁和更新的流程文件资料，以验证该流程包含从第 7.2.1 至 7.2.2 所规定的程序：	当某危险漏洞被识别时，应立即研发用来解决该安全漏洞的软件更新并向客户发布，以最大程度缩短时间并减少漏洞被利用的可能性。
7.2.1 已通过已知信任链安全地向客户发布了补丁和更新。	**7.2.1** 与责任工作人员面谈并查看流程，确认已通过已知信任链安全地向客户发布了补丁和更新。	发布安全补丁时必须预防恶意个人在传输过程中拦截更新及修改更新，之后再将其重新发布给信任的客户。
7.2.2 向客户发布补丁和更新时应保持补丁和更新代码的完整性。	**7.2.2.a** 与责任工作人员面谈并查看流程，确认在向客户发布补丁和更新时已保持了补丁和更新代码的完整性。	安全更新应在更新过程中包含一种机制，以确认该更新代码未被替换或篡改。完整性检查示例包括但不限于：校验和为证书数字签名等。
	7.2.2.b 于责任工作人员面谈并查看应用程序更新流程，确认补丁和更新在安装前已在目标系统上接受完整性测试。	
	7.2.2.c 使用任意代码实施更新流程，确定该系统不允许更新，以确认补丁与更新代码的完整性得以保持。	
7.2.3 为客户提供安全安装补丁和更新的相关说明。	**7.2.3** 检查由供应商编制的*《PA-DSS 实施指南》*，确认该文件已为客户与集成商/经销商提供以下信息： • 供应商将如何传达新补丁和更新通知。 • 如何通过已知信任链安全地发布补丁和更新。 • 如何在保持补丁和更新代码完整性的情况下访问和安装补丁及更新。	向客户和集成商/经销商推荐安全接受和安装补丁的流程有助于保护更新流程和应用程序的完整性。

PA-DSS 要求	测试程序	指南
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。	**7.3.a** 检查发布更新的流程并与负责人员面谈，确认所有更新都包含发布说明，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。	发布说明向客户提供了软件更新的详情，包括：更改了哪些文件，修改了哪些应用程序的功能，以及哪些与安全相关的功能可能会受影响。发布说明还应注明某个具体补丁或更新如何影响与该补丁发布相关的整体版本号。
	7.3.b 检查应用程序更新示例的发布说明，确认其中已包含更新。	

要求 8：　　便于安全的网络实施

PA-DSS 要求	测试程序	指南
8.1 支付应用程序必须能够在安全的网络环境中进行实施。应用程序不能妨碍使用 PCI DSS 所要求的设备、应用程序或配置。 *例如：支付应用程序不能影响补丁的安装、反恶意软件的保护、防火墙配置或遵从 PCI DSS 所要求的任何其他设备、应用程序或配置。* ***符合 PCI DSS 第 1、3、4、5 及 6 要求***	**8.1.a** 按照*《PA-DSS 实施指南》，在符合 PA-DSS 要求的实验室环境中安装应用程序。*测试支付应用程序，以获取证据表明该应用程序能在完全符合 PCI DSS 要求的网络中运行。 **8.1.b** 测试该应用程序和底层系统，确认该支付应用程序不妨碍或影响底层系统的 PCI DSS 功能（例如：该应用程序不禁止补丁或反恶意软件更新的安装，或影响其他 PCI DSS 功能的运行）。	支付应用程序的设计和研发应确保该应用程序的安装和运行不得阻止组织实施 PCI DSS 所要求的其他控制。例如，支付应用程序必须能在运行杀毒解决方案的环境中运行（例如，无需关闭或卸载这些解决方案）。
8.2 支付应用程序仅能使用或要求使用必要且安全的服务、协议、守护进程、组件及相关软件和硬件，包括由第三方提供的执行支付应用程序的软件和硬件。 *注：SSL 和早期 TLS 不视为强效加密法。支付应用程序不得使用或支持使用 SSL 或早期 TLS。使用或支持 TLS 的应用程序不得允许退回到 SSL。* ***符合 PCI DSS 要求 2.2.3***	**8.2.a** 检查由支付应用程序启用或要求使用的系统服务、协议、守护进程、组件及相关软件和硬件。确认仅有必要且安全的服务、协议、守护进程、组件、从属软件和硬件在默认“开箱即用”的方式下启用。 **8.2.b** 安装应用程序并测试应用程序功能，确认如果该应用程序支持任何不安全的服务、守护进程、协议或组件，则确保其已在默认“开箱即用”的方式下安全配置。 **8.2.c** 确认*《PA-DSS 安装指南》*记录了执行支付应用程序功能所必需的协议、服务、组件及相关的软件和硬件，包括由第三方提供的上述项目。	业务需要（或已通过默认值启用）的很多协议常被恶意个人利用，对系统或网络造成威胁。支付应用程序不应要求使用不安全的协议、服务、守护进程等。如果应用程序支持使用不安全的服务、守护进程、协议或组件，须在默认情况下对其予以保护。
8.3 支付应用程序不得要求使用妨碍使用多因素验证技术或影响其正常运行的服务或协议。 ***注：****多因素验证要求至少使用三种验证方法（参见下文）中的两种进行验证。使用一个因素两次（例如，使用两个不同的密码）不视为多因素验证。验证方法（也称为因素）如下：* • 所知，如密码或口令等 • 所有，如令牌设备或智能卡等 • 个人特征，如生物特征 ***符合 PCI DSS 要求 8.3***	**8.3.a** 检查支付应用程序功能，确认该功能不要求使用任何妨碍使用多因素验证技术或影响其正常运行的服务或协议。 **8.3.b** 识别应用程序支持的远程访问机制，确认该机制不会阻止多因素验证。	支付应用程序的设计和开发应确保安装和运行该应用程序不得要求组织使用禁止其实施和运行安全访问所需的多因素验证解决方案的服务或协议。例如：若 RADIUS 是所支持的验证和授权技术，则应用程序不应默认使用端口 1812（通常被认为由 RFC 2865 分配给 RADIUS）。 *多因素技术的示例包括但不限于带令牌的 RADIUS、带令牌的 TACACS，或者便于进行多因素验证的其他技术。*

要求 9：　　绝不能在连接到互联网的服务器上存储持卡人数据

PA-DSS 要求	测试程序	指南
9.1 支付应用程序的开发必须满足如下要求：不要求任何网络服务器与任何持卡人数据存储组件位于同一台服务器上，也不要求数据存储组件位于带有网络服务器的相同网络区域（如 DMZ）内。 ***符合 PCI DSS 要求 1.3.7***	**9.1.a** 识别所有的支付应用程序数据存储组件（如数据库）和所有网络服务器。 在不同的服务器上安装数据存储组件和网络服务器，并在不同的服务器上测试应用程序功能，确认支付应用程序不要求任何数据存储组件（如数据库）为了执行功能而在与网络服务器相同的服务器上安装。	鉴于公共网络（互联网、公共无线等）的开放性及这些网络可能遭受的袭击数量，支付应用程序的网络服务器组件面临极高的破坏风险。 持卡人数据存储组件所要求的保护级别比面向公众的应用程序组件更高。如果持卡人数据位于 DMZ 中，则外部攻击者更容易访问此信息，这是因为要穿透的层数更少。 因此，网络服务器决不能存储在与数据存储组件相同的服务器中。如果恶意个人能够破坏网络服务器中的帐户，则其不费吹灰之力便能破坏持卡人数据。
	9.1.b 在不同的网络区域安装数据存储组件和网络服务器。在不同的网络区域测试所有应用程序功能，确认支付应用程序不要求任何数据存储组件（如数据库）为了执行功能而在与网络服务器相同的网络区域上安装。	
	9.1.c 检查由供应商编制的*《PA-DSS 实施指南》*，确认其包含针对客户和集成商/经销商的如下说明： • 关于不要在面向公众的系统上存储持卡人数据（例如，网络服务器与数据库服务器决不能在同一台服务器上）的说明。 • 关于如何配置支付应用程序来使用 DMZ 将互联网与储存持卡人数据的系统相分离（例如：在 DMZ 中安装网络服务器，而在不同的内部网络区域安装数据存储组件）的说明。 • 应用程序要在两个网络区域之间进行通信所需使用的服务/端口列表（以便客户可自行配置防火墙，以便仅打开所需的端口）。	

要求 10：　便于对支付应用程序进行安全的远程访问

PA-DSS 要求	测试程序	指南
10.1 任何来自客户环境外部对支付应用程序进行的远程访问都必须使用多因素验证。 ***注：****多因素验证要求在验证过程中至少使用三种验证方法中的两种（有关验证方法的说明，请参阅 PA-DSS 要求 3.1.4）。* ***符合 PCI DSS 要求 8.3***	**10.1.a** 检查由供应商编制的*《PA-DSS 实施指南》*，确认其包含针对客户和集成商/经销商的如下说明： • 关于所有来自客户网络外部对支付应用程序的远程访问都必须使用多因素验证以满足 PCI DSS 要求的说明。 • 关于应用程序所支持的多因素验证机制的说明。 • 关于将应用程序配置为支持多因素验证的说明（至少使用 PA DSS 要求 3.1.4 中说明的三种验证方法中的两种）。	多因素验证要求至少对来自网络外部的访问实施两种验证方法。 支付应用程序供应商需要向客户提供如何配置应用程序以支持指定的多因素验证机制的指导说明，从而确保这些机制能妥善实施并满足适用的 PCI DSS 要求。 多因素验证要求适用于可从客户环境外进行远程访问的所有工作人员。
	10.1.b 如果应用程序供应商可对来自客户环境外部的客户支付应用程序进行远程访问，则对供应商政策进行检查，确认该供应商支持客户对所有上述访问进行多因素验证的要求。	
10.2 任何对支付应用程序的远程访问必须安全执行，具体如下：	**10.2** 确认远程访问按照以下方式执行：	支付应用程序供应商和/或集成商/经销商采用的任何远程访问机制（例如，用于支持这些提供商提供的服务）应支持所有适用的 PCI DSS 要求。
10.2.1 如果支付应用程序的更新是通过对客户系统的远程访问实现的，软件供应商必须告知客户只在需要从供应商那里下载更新时才开启远程访问技术，下载完毕后须即刻关闭。 或者，如果是通过虚拟专用网络 (VPN) 或其他高速连接方式发送，软件供应商必须建议客户妥善配置防火墙或个人防火墙产品，以确保“随时保持”连接。 ***符合 PCI DSS 要求 1 和 12.3.9***	**10.2.1.a** 如果支付应用程序更新通过远程访问发送至客户系统，请检查由供应商编制的*《PA-DSS 实施指南》*，确认其包含： • 向客户与集成商/经销商提供关于安全使用远程访问技术的指导说明，明确规定远程访问技术仅能在供应商和业务合作伙伴需要时激活，并在使用后立即停用。 • 如果电脑是通过 VPN 或其他高速连接方式实现连接的，则按照 PCI DSS 第 1 要求，建议客户与集成商/经销商使用防火墙或个人防火墙产品，以确保“随时保持”连接。	
	10.2.1.b 如果供应商通过远程访问将支付应用程序和/或更新发送至客户网络，请查看供应商通过远程访问将支付应用程序和/或更新发送至客户网络所使用的方法，并确认其包含以下内容： • 仅当需要时激活远程访问技术，并在使用后立即停用。 • 如果远程访问通过 VPN 或其他高速连接实现，则请根据 PCI DSS 要求 1 获取连接。	

PA-DSS 要求	测试程序	指南
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，则必须对每个客户使用唯一的验证凭证（例如密码/口令）。 ***符合 PCI DSS 要求 8.5.1***	**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，则应检查供应商流程并与工作人员面谈，确认对每一位可访问的客户使用唯一的验证凭证（例如密码/口令）。	为防止使用单一的一组凭证对多个客户的环境造成威胁，持有对客户环境进行远程访问所需帐户的供应商应对每个客户使用不同的验证凭证。 避免使用重复的规则来生成易于猜测的密码。这些验证凭证会在一段时间后被人知晓，并被未授权人员利用，从而对供应商的客户造成威胁。
10.2.3 如果供应商、集成商/经销商或客户能对客户的支付应用程序实施远程访问，则必须安全地实施此类访问，例如： • 更改远程访问软件中的默认设置（例如，更改默认密码，并对每位用户使用唯一的密码）。 • 只允许来自特定（已知的）IP/MAC 地址的连接； • 使用强效验证和复杂密码登录（请参阅 PA-DSS 要求 3.1.1 至 3.1.11）。 • 根据 PA-DSS 要求 12.1 启用加密数据传输。 • 在尝试登录失败达到一定次数后，启用帐户锁定功能。（请参阅 PA-DSS 要求 3.1.9 至 3.1.10）。 • 在获得访问许可之前，通过防火墙建立一个 VPN 连接。 • 启用记录功能。 • 仅限集成商/经销商的授权工作人员访问客户环境。 ***符合 PCI DSS 第 2、8 和 10 要求***	**10.2.3.a** 检查由供应商编制的*《PA-DSS 实施指南》*，确认已就须安全实施对支付应用程序的所有远程访问为客户和集成商/经销商提供了指导，例如： • 更改远程访问软件中的默认设置（例如，更改默认密码，并对每位用户使用唯一的密码）。 • 只允许来自特定（已知的）IP/MAC 地址的连接； • 使用强效验证和复杂密码登录（请参阅 PA-DSS 要求 3.1.1 至 3.1.11）。 • 根据 PA-DSS 要求 12.1 启用加密数据传输。 • 在尝试登录失败达到一定次数后，启用帐户锁定功能。（请参阅 PA-DSS 要求 3.1.9 至 3.1.10）。 • 在获得访问许可之前，通过防火墙建立一个 VPN 连接。 • 启用记录功能。 • 仅限授权工作人员访问客户环境。 **10.2.3.b** 如果软件供应商可以对客户的支付应用程序进行远程访问，则查看供应商的远程访问方法并与工作人员面谈，以确认远程访问得以安全实施	支付应用程序供应商需要向客户和集成商/经销商提供如何配置应用程序以支持安全远程访问的指导说明，从而确保这些机制能妥善实施并满足 PCI DSS 要求。 这些要求适用于访问客户环境所使用所有类型的远程访问。

要求 11：　　对经由公共网络传输的敏感信息进行加密

PA-DSS 要求	测试程序	指南
11.1 如果支付应用程序能够或便于通过公共网络发送持卡人数据，则该程序必须支持使用强效加密法和安全协议，以便在通过公开、公共网络传输时保护敏感持卡人数据，至少包括： • 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 ***注：****SSL 和早期 TLS 不视为强效加密法。支付应用程序不得使用或支持使用 SSL 或早期 TLS。使用或支持 TLS 的应用程序不得允许退回到 SSL* *开放式公共网络包括但不限于：* • 互联网 • 无线技术，包括但不限于：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 ***符合 PCI DSS 要求 4.1***	**11.1.a** 如果支付应用程序能够或便于通过公共网络发送持卡人数据，则确认该应用程序提供强效加密法和安全协议，或已明确规定须使用该类方案。 **11.1.b** 检查由供应商编制的*《PA-DSS 实施指南》*，确认供应商已向客户和集成商/经销商提供关于该应用程序提供或指定使用强效加密法和安全协议的指导说明，其中包括： • 关于持卡人数据通过公共网络传输时必须使用强效加密法和安全协议的说明。 • 关于确认只接受可信密钥和/或证书的说明。 • 如何配置支付应用程序，以便仅使用安全版本和安全实施安全协议。 • 如何配置支付应用程序，以防止退回到非安全版本或配置（例如，若适用 TLS，应用程序则不得允许退回到 SSL）. • 如何配置支付应用程序，以便针对所使用的加密方法采用合适的加密强度。 **11.1.c** 如果支付应用程序提供强效加密法和安全协议，则按照*《PA-DSS 实施指南》*中的说明安装和测试该应用程序，并确认： • 实施的协议默认仅使用可信的密钥和/或证书. • 实施的协议默认仅使用安全的配置且不支持非安全版本或配置。 • 实施的协议默认不允许退队到非安全版本或配置（例如，若使用 TLS，应用程序不得允许退回到 SSL）。 • 根据所使用的加密方法实施适当的加密强度。	由于恶意个人通常会在数据传输过程中轻松拦截和/或转移数据，因此必须对通过公共网络传输的敏感信息进行加密。 要实现持卡人数据的安全传输需使用可信密钥/证书、安全传输协议以及用于持卡人数据加密的合适加密强度。 注意：有些协议的实施（例如 SSL、SSH 版本 1.0 和早期 TLS）存在攻击者可用于控制受影响系统的已知漏洞，如缓冲区溢出。无论支付应用程序使用哪项安全协议，均需确保将其默认配置为仅使用安全的配置和版本，从而防止使用非安全连接。

PA-DSS 要求	测试程序	指南
11.2 如果支付应用程序便于通过终端用户通讯技术（如：电子邮件、即时通讯和聊天）发送 PAN，则支付应用程序必须提供使该 PAN 不可读或实施强效加密法的解决方案，或指定使用强效加密法对 PAN 进行加密。 ***符合 PCI DSS 要求 4.2***	**11.2.a** 如果支付应用程序允许和/或便于通过终端用户通讯技术发送 PAN，则确认已提供使该 PAN 不可读或实施强效加密法的解决方案，或已明确规定须使用该类方案。	电子邮件、即时通讯和聊天在内部和公共网络中传送时，可通过包嗅探轻松拦截。除非支付应用程序在使用此类技术时使用强效加密法或使该 PAN 不可读，否则请勿使用此类通讯技术来发送 PAN。
	11.2.b 检查由供应商编制的*《PA-DSS 实施指南》*，确认供应商已向客户和集成商/经销商提供关于该应用程序提供或指定使用解决方案的指导说明，其中包括： • 使用能够使 PAN 不可读或使用强效加密法保障 PAN 安全的定义解决方案的程序。 • 关于当 PAN 通过终端用户通讯技术发送时，其必须时刻保持不可读或受强效加密保护的说明。	
	11.2.c 如果支付应用程序提供了解决方案，则安装并测试该应用程序，以确认该解决方案使 PAN 不可读或实施了强效加密法。	

要求 12：　保护所有非控制台管理访问

PA-DSS 要求	测试程序	指南
12.1 如果支付应用程序便于进行非控制台管理访问，则请使用强效加密法对所有此类访问进行加密。 ***注意：*** • *决不能对管理访问使用明文协议（如 Telnet 或 rlogin）。* • *SSL 和早期 TLS 不视为强效加密法。支付应用程序不得使用或支持使用 SSL 或早期 TLS。使用或支持 TLS 的应用程序不得允许退回到 SSL。* ***符合 PCI DSS 要求 2.3***	**12.1.a** 在实验室安装支付应用程序并测试非控制台管理连接，以确认在要求提供管理员密码前已调用强效加密法。	如果远程管理未采用安全验证和加密通信，敏感管理或操作级信息（例如管理员的密码）便可能泄露给窃听者。恶意个人可利用这些信息访问应用程序和/或网络，修改权限并窃取数据。
	12.1.b 检查支付应用程序配置设置，确认支付应用程序未使用明文协议（例如 Telnet 和 rlogin）来进行非控制台管理访问。	
	12.1.c 检查由供应商编制的*《PA-DSS 实施指南》*，确认其已向客户和集成商/经销商提供如何配置应用程序以使用强效加密法加密非控制台管理访问的相关指导说明。	
12.1.1 指导客户使用强效加密法加密所有非控制台管理访问，以便进行基于 Web 的管理和其他非控制台管理访问。 ***注：****决不能对管理访问使用明文协议（如 Telnet 或 rlogin）。* ***符合 PCI DSS 要求 2.3***	**12.1.1** 检查由供应商编制的*《PA-DSS 实施指南》*，确认其已向客户和集成商/经销商提供实施强效加密法以对所有非控制台管理访问进行加密的相关指导说明。	支付应用程序供应商需要向客户和集成商/经销商提供配置应用程序的指导说明，以便使用强效加密法对所有非控制台管理访问进行加密。这样做可确保安全控制得到妥善实施并满足 PCI DSS 和 PA-DSS 指南。
12.2 针对拥有非控制台管理访问权限的所有工作人员使用多因素验证。 ***注：****多因素验证要求在验证过程中至少使用三种验证方法中的两种（有关验证方法的说明，请参阅 PA-DSS 要求 3.1.4）。* ***符合 PCI DSS 要求 8.3***	**12.2.a** 确认应用程序附带多因素验证，或已指定使用多因素验证。	管理访问要求进一步保障尝试获取访问权限的个人和其声称的身份相符。 由于可在应用程序、系统或网络级别实施多因素验证，因此不要求所有应用程序均需包含多因素验证解决方案。应用程序供应商可以让其应用程序附带多因素验证，也可以为用户和集成商/供应商提供安装多因素验证以便对应用程序进行管理访问的相关说明。
	12.2.b 检查由供应商编制的*《PA-DSS 实施指南》*，确认其已为客户和集成商/经销商提供使用多因素验证的指导说明，包括： • 关于须对所有可对 CDE 进行非控制台管理访问的工作人员使用多因素验证的说明。 • 使用应用程序附带的多因素验证功能（若提供）的程序。	
	12.2.c 如果支付应用程序附带多因素验证功能，则安装并测试该应用程序，以确认在授予访问权限前已应用多因素验证。	

要求 13：　为客户、经销商和集成商维护《PA-DSS 实施指南》

PA-DSS 要求	测试程序	指南
13.1 制定、维护并散发给客户、经销商与集成商的*《PA-DSS 实施指南》*，该指南须满足以下要求：	**13.1** 检查*《PA-DSS 实施指南》*及相关的供应商流程并与工作人员面谈，确认： • *《PA-DSS 实施指南》*已分发给拥有该应用程序的所有客户、经销商和集成商。 • 供应商实施有效的机制，可在客户、经销商和集成商要求时提供*《PA-DSS 实施指南》*。	一本精心设计且详尽的*《PA-DSS 实施指南》*有助于指导客户和集成商/经销商在支付应用程序及其底层组件中实施适当的安全措施和配置，以满足保护持卡人数据的相关 PCI DSS 和 PA-DSS 指南。
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。	**13.1.1** 检查*《PA-DSS 实施指南》*并确认其： • 清楚说明了支付应用程序名称和其适用的版本。 • 提供了所有必需的应用程序依赖条件详情，以便该应用程序能以符合 PCI DSS 的方式进行配置。	
13.1.2 在所有引用*《PA-DSS 实施指南》*的地方，指出本文件中所有要求的位置所在。	**13.1.2** 检查*《PA-DSS 实施指南》*并使用附录 A 作为参考，确认*《PA-DSS 实施指南》*涵盖了本文件中的所有相关要求。	
13.1.3 至少每年均根据应用程序或 PA-DSS 要求的变更情况，进行一次审查，从而使该文件资料与所有影响到该应用程序的变更及本文件的要求保持同步。	**13.1.3.a** 检查*《PA-DSS 实施指南》*并与工作人员面谈，确认*《PA-DSS 实施指南》*已根据如下要求进行审查： • 至少每年执行一次 • 根据应用程序的变更情况进行 • 根据这些 PA-DSS 要求的变更情况进行。	当每个应用程序更新时，系统功能和关键应用程序安全机制（在某些情况下）也将修改或引入。若*《PA-DSS 实施指南》*未与支付应用程序的最新版本保持同步，则客户和集成商/经销商可能忽视或错误配置关键应用程序的安全控制，最终可能导致攻击者绕过此类安全机制并破坏敏感数据。
	13.1.3.b 确认*《PA-DSS 实施指南》*根据需要更新并与下列各项保持同步： • PA-DSS 要求的变更情况 • 应用程序或其依赖条件的变更情况。	
	13.1.3.c 检查*《PA-DSS 实施指南》*及相关的供应商流程并与工作人员面谈，确认供应商已实施有效的机制，向客户、经销商和集成商传达出现的更新并根据需要提供更新后的版本。	

要求 14：　为工作人员分配 PA-DSS 职责，并为工作人员、客户、经销商和集成商维护培训计划

PA-DSS 要求	测试程序	指南
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。	**14.1** 检查培训材料并与负责人员面谈，确认所有供应商工作人员每年至少接受一次有关 PA-DSS 和信息安全的培训。	为使支付应用程序的设计能有效符合 PA-DSS 指南，支付应用程序供应商工作人员应熟悉 PA-DSS 及与 PA-DSS 持续评估相关的职责。支付应用程序供应商应负责确保其工作人员在上述领域接受了良好的培训。
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	**14.2.a** 检查已记录在案的职责，确认以下各项职责已得到正式分配： • 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。	在每个支付应用程序供应商组织中，应向责任方（无论是个人还是团队）分配 PA-DSS 的正式职责，以确保所有 PA-DSS 要求都得到相应满足。
	14.2.b 与负责以下职责的工作人员面谈，确认其已明确和理解其角色和职责： • 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。	
14.3 为支付应用程序集成商和经销商制定并实施培训和交流计划。培训应至少包括以下内容： • 如何实施支付应用程序及相关系统和网络，才能符合 PCI DSS 要求 • 涵盖本文件（及附录 A 中）指出的适用于*《PA-DSS 实施指南》*的所有项目。	**14.3.a** 检查为集成商与经销商准备的培训材料，确认该材料包括以下内容： • 如何以符合 PCI DSS 要求的方式实施支付应用程序及相关系统和网络的相关培训 • 涵盖本文件（及附录 A 中）指出的适用于*《PA-DSS 实施指南》*的所有项目。	对应用程序的不当配置、维护或支持都可能会导致将安全漏洞引入客户的持卡人数据环境中，从而可能导致这些漏洞为攻击者所利用。应用程序供应商应当向集成商/经销商提供关于应用程序安全安装和配置的培训，以确保当其安装到客户的环境中时，应用程序

PA-DSS 要求	测试程序	指南
	14.3.b 检查供应商的交流计划及相关供应商流程，并与供应商人员面谈，以确认： • 已向集成商和经销商提供培训材料 • 供应商实行有效的机制，可在集成商和经销商要求时提供更新的材料。	能够符合 PCI DSS 要求 支付应用程序供应商有责任向集成商和经销商提供这些方面的培训。
	14.3.c 抽取部分集成商和经销商进行面谈，确认他们已接受应用程序供应商提供的培训并收到了培训材料。	
	14.3.d 检查可证实集成商和经销商已收到软件供应商所提供培训材料的相关证据。	
14.3.1 至少每年均根据应用程序或 PA-DSS 要求的变更情况，审查一次培训材料。 根据需要更新培训材料，使相关文件资料与最新的支付应用程序版本和 PA-DSS 要求的变更情况保持同步。	**14.3.1.a** 检查为集成商与经销商准备的培训材料，确认该材料： • 至少每年均已根据应用程序或 PA-DSS 要求的变更情况审查一次 • 已根据需要进行更新，使相关文件资料与最新的支付应用程序版本和 PA-DSS 要求的变更情况保持同步。	为支付应用程序供应商人员、集成商和经销商提供的培训材料应至少每年更新一次，以确保材料与最新版本的应用程序和 PA-DSS 要求保持同步。使用过时的培训材料会造成培训计划无效，从而导致应用程序自身的安全功能设计缺陷，或导致集成商和经销商对应用程序的不当配置。
	14.3.1.b 检查支付应用程序新版本的发布流程，确认已更新的文件资料与新的支付应用程序同时向集成商和经销商发布。	
	14.3.1.c 抽取部分集成商和经销商进行面谈，确认他们已收到了应用程序供应商所提供更新过的培训材料。	

附录 A：《*PA-DSS 实施指南*》的内容概要

本附录的目的在于总结与《*PA-DSS 实施指南*》主题相关的 PA-DSS 要求，说明提供给客户和集成商/经销商的《*PA-DSS 实施指南*》的内容（请参阅第 11 页的《PA-DSS 实施指南》），并明确相关控制的实施责任。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
1.1.4	删除由支付应用程序以前版本存储的敏感验证数据。	必须向客户和集成商/经销商说明以下内容： ▪ 必须移除历史数据（由支付应用程序以前版本存储的磁道数据、卡验证代码、PIN 或 PIN 数据块）、 ▪ 如何移除历史数据。 ▪ 上述移除对于 PCI DSS 遵从性来说是绝对必需的。	**软件供应商**：按照 PA-DSS 第 1.1.4 要求，向客户提供工具或程序，用于安全移除以前版本所存储的敏感验证数据。 **客户与集成商/经销商**：按照《*PA-DSS 实施指南*》与 PA-DSS 第 1.1.4 要求删除所有历史数据。
1.1.5	删除因对支付应用程序实施故障排除而收集的所有敏感验证数据（预授权）。	必须向客户和集成商/经销商说明以下内容： ▪ 仅在解决特定问题需要时才收集敏感验证数据（预授权）。 ▪ 仅在特定的、已知的、有访问限制的位置存储此类数据。 ▪ 在解决特定问题时，仅收集有限的必要数据。 ▪ 存储时，必须对敏感验证数据进行加密。 ▪ 使用后须立即安全删除此类数据。	**软件供应商**：按照 PA-DSS 第 1.1.5.a 要求，不得存储敏感验证数据，也不得对客户的问题执行任何故障排除。 **客户与集成商/经销商**：按照《*PA-DSS 实施指南*》与 PA-DSS 第 1.1.5.a 要求，不得存储敏感验证数据，也不得对任何问题实施故障排除。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
2.1	在客户自定义的保留期结束后安全删除持卡人数据。	必须向客户和集成商/经销商提供以下内容： ▪ 关于超过客户自定义保留期的持卡人数据必须安全删除的说明。 ▪ 支付应用程序存储持卡人数据的所有位置的清单，以便客户了解哪些位置存储的数据需要删除。 ▪ 关于客户需要安全删除不再是法律、监管或业务方面所必需的持卡人数据的说明。 ▪ 如何安全删除支付应用程序所存储的持卡人数据，包括存储在底层软件或系统（比如操作系统、数据库等）中的数据 ▪ 如何配置底层软件或系统（比如操作系统、数据库等） 才能防止对持卡人数据的无意捕获或保留。	**软件供应商**：指导客户必须对超过客户自定义保留期的持卡人数据进行安全删除，包括支付应用程序以及底层软件或系统存储此类数据的所有位置，以及如何安全删除支付应用程序所存储的持卡人数据。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.1 要求，安全删除超过客户自定义保留期的持卡人数据。
2.2	显示 PAN 时必须予以掩盖，以便仅限具有业务需要的工作人员查看除前六位/后四位以外的 PAN。	必须向客户和集成商/经销商提供以下内容： ▪ 显示 PAN 的所有情形的详细信息，包括但不限于 POS 设备、显示屏、日志和收据。 ▪ 确认支付应用程序默认情况下在所有显示中掩盖 PAN。 ▪ 关于如何配置支付应用程序，以便于仅限具有合理业务需求的工作人员查看除前六位/后四位以外的 PAN（包括显示完整的 PAN）的说明。	**软件供应商**：向客户提供关于掩盖 PAN 以仅限具有业务需要的工作人员查看除前六位/后四位以外的 PAN 的说明。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.2 要求，对 PAN 的显示予以掩盖，以便仅限具有业务需要的工作人员查看除前六位/后四位以外的 PAN。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
2.3	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。	必须向客户和集成商/经销商提供以下内容： ▪ 详细介绍应用程序用于使持卡人数据不可读的每种方法的所有可配置选项，并指示如何针对支付应用程序存储持卡人数据的所有位置来配置每种方法（根据 PA-DSS 要求 2.1）。 ▪ 客户可能输出持卡人数据以存储到支付应用程序外部的所有情形的清单，以及客户负责在所有此类情形中使 PAN 不可读的说明。 ▪ 如果已启用除错日志（例如，为了进行故障排除而启用），且日志包含 PAN，则须根据 PCI DSS 保护日志、在完成故障排除后尽快禁用日志，并在不再需要使用时安全删除日志的相关说明。	**软件供应商**：向客户提供关于使所有位置存储或由应用程序输出的 PAN 均不可读的说明。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.3 要求，使所有位置存储的 PAN 均不可读。
2.4	保护用于防止持卡人数据被泄露和滥用的密钥。	必须向客户和集成商/经销商说明以下内容： ▪ 限制只有极少数必需的保管人才能访问密钥。 ▪ 尽量减少密钥安全存储的位置和形式。	**软件供应商**：指导客户用于保护持卡人数据的密钥应安全存储在极少的位置，并且仅极少数必需的保管人才有密钥访问权限。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.4 要求，密钥应安全存储在极少的位置，并且仅极少数必需的保管人才有密钥访问权限。
2.5	必须对用于持卡人数据加密的密钥实施密钥管理流程与程序。	必须向客户和集成商/经销商提供以下内容： ▪ 关于如何安全生成、分发、保护、更改、存储和注销/替换密钥，以及客户或集成商/经销商在哪些领域参与了这些密钥管理活动的说明。 ▪ 密钥保管人用于确认其理解并接受密钥保管责任的“密钥保管表格”样本。	**软件供应商**：向客户提供关于访问用于持卡人数据加密的密钥以实施密钥管理流程和程序的说明。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.5 要求，对用于持卡人数据加密的密钥实施密钥管理流程与程序。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
2.5.1 – 2.5.7	实施安全的密钥管理功能。	向客户和集成商/经销商提供关于如何执行以下各项密钥管理功能的说明： ▪ 生成强效密钥。 ▪ 安全的密钥分配。 ▪ 安全的密钥存储。 ▪ 针对密钥周期结束的密钥的密钥变更。 ▪ 密钥的完整性变弱或怀疑密钥遭受威胁时，认为有必要注销或替换密钥。 ▪ 使用支付应用程序所支持的任何手动明文密钥管理操作时，必须采用分割知识和双重控制。 ▪ 防止密钥的非授权替换。	**软件供应商**：向客户提供关于实施安全密钥管理功能的说明。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.5.1 – 2.5.7 要求，实施用于密钥的安全密钥管理功能。
2.6	提供一种可使支付应用程序所存储的密钥材料或密文不可恢复的机制。	必须向客户和集成商/经销商提供以下内容： ▪ 详细介绍如何使用应用程序随附的工具或程序使加密材料不可检索的程序。 ▪ 关于按照 PCI DSS 中的密钥管理要求，当密钥不再使用时其密钥材料应不可恢复的说明。 ▪ 关于如何用新的密钥对历史数据进行重新加密的说明，包括在解密/重新加密过程中保持明文数据安全性的程序。	**软件供应商**：提供工具或程序，用于安全移除应用程序中存储的密钥材料或密文；并提供工具或程序，以便用新的密钥对历史数据进行重新加密。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 2.6 要求，删除所有的历史密钥材料。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
3.1	对管理访问与对持卡人数据的访问使用唯一的用户 ID 和安全验证。	必须向客户和集成商/经销商提供以下内容： ▪ 关于支付应用程序如何通过以下方式针对该应用程序生成或管理的验证凭证（如用户名、密码）执行强效验证方面的指导： – 根据 PA-DSS 要求 3.1.1 至 3.1.11，在安装完成前对验证凭证强制执行安全变更。 – 根据 PA-DSS 要求 3.1.1 至 3.1.11，（安装以后）针对任何后续改动强制执行安全变更。 ▪ 为了保持 PCI DSS 遵从性，在提供验证方法时需对验证配置方面的任何更改都进行确认，验证方法的严格程度应该至少与 PCI DSS 的要求相同。 ▪ 向该环境中的所有默认帐户分配安全验证 ▪ 针对不使用的任何默认帐户，分配安全验证，然后禁用或不使用这些帐户。 ▪ 对于不是由支付应用程序生成或管理的验证凭证，如何按照 PA-DSS 第 3.1.1 至 3.1.11 要求，在安装完成时或针对安装后的后续更改，为有管理权限或有权限访问持卡人数据的所有应用程序级别帐户变更和创建验证凭证。 ▪ 通过管理访问识别应用程序中的所有角色和默认帐户。	**软件供应商**：按照 PA-DSS 第 3.1.1 至 3.1.11 要求，对于由支付应用程序生成或管理的验证凭证，确保支付应用程序使客户的帐户/密码使用唯一的用户 ID 和安全验证。 对于不是由支付应用程序生成或管理的验证凭证，确保*《PA-DSS 实施指南》*可清楚明确地指导客户和集成商/经销商如何按照 PA-DSS 第 3.1.1 至 3.1.11 要求变更和创建安全验证凭证。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 3.1.1 至 3.1.11 要求，设置与维护唯一的用户 ID 与安全验证。
3.2	在访问带有支付应用程序的 PC、服务器与数据库时，使用唯一的用户 ID 与安全验证。	按照 PA-DSS 第 3.1.1 至 3.1.11 要求，指导客户和集成商/经销商在访问带有支付应用程序和/或持卡人数据的 PC、服务器与数据库时，使用唯一的用户名与安全验证。	**软件供应商**：按照 PA-DSS 第 3.1.2 至 3.1.9 要求，确保支付应用程序支持客户对供应商所设置用于访问 PC、服务器与数据库的帐户/口令使用唯一的用户 ID 与安全验证。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 3.1.1 至 3.1.11 要求，设置与维护唯一的用户 ID 与安全验证。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
4.1	实施自动的检查记录。	提供关于实施自动检查记录的指导，包括： ▪ 如何安装应用程序，以便在安装过程完成之后能够以默认方式配置和启用日志。 ▪ 如何按照 PA-DSS 要求 4.2、4.3 和 4.4，针对安装后客户可配置的任何日志选项，进行符合 PCI DSS 要求的日志设置。 ▪ 必须启用日志，禁用日志会导致对 PCI DSS 的非遵从性。 ▪ 对于与支付应用程序打包使用或其要求使用的第三方软件组件，如何针对安装后客户可配置的任何日志选项，进行符合 PCI 要求的日志设置。	**软件供应商**：按照 PA-DSS 第 4.2、4.3 和 4.4 要求，确保支付应用程序支持客户使用符合要求的日志。 **客户与集成商/经销商：**按照*《PA-DSS 实施指南》*与 PA-DSS 第 4.2、4.3 和 4.4 要求，建立并维护符合 PCI DSS 要求的日志。
4.4	支持中央日志。	提供关于所支持中央日志机制的描述，以及将支付应用程序日志整合到一个中央日志服务器的说明和程序。	**软件供应商**：按照 PA-DSS 第 4.4 要求，确保支付应用程序在客户环境中支持中央日志。 **客户与集成商/经销商：**按照*《PA-DSS 实施指南》*与 PA-DSS 第 4.4 要求，建立并维护中央日志。
5.4.4	实施并传达应用程序版本控制方法。	描述供应商发布的版本控制方法，并包括以下几方面的相关指导： ▪ 版本控制方案详情，包括版本方案的格式（元素数量、分隔符、字符集等）。 ▪ 关于版本控制方案如何标明可影响安全的变更的详细说明。 ▪ 其他类型的变更如何影响版本的相关详情。 ▪ 所使用的任何通配符元素的详情，包括确认其绝不会用于表示影响安全的变更。	**软件供应商**：记录并实施软件版本控制方法，作为系统开发周期的一部分。按照 PA-DSS 第 5.5 要求，该方法必须遵循*《PA-DSS 实施指南》*中规定的支付应用程序更改的程序。 **客户与集成商/经销商：**了解正在使用的支付应用程序版本，并确保正在使用的版本已经过验证。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
6.1	安全地实施无线技术。	如果支付应用程序开发用来与无线技术配合使用，则必须向客户和集成商/经销商： ▪ 关于在安装时，支付应用程序即会更改应用程序所控制所有无线组件的默认密钥、密码和 SNMP 社区字符串的说明。 ▪ 知道密钥/密码的人离开公司或调动职位时，无线密钥和密码（包括 SNMP 字符串）的变更程序。 ▪ 随支付应用程序一起提供但不受其控制的任意无线组件的默认密钥、密码和 SNMP 社区字符串的变更说明。 ▪ 在任意无线网络和存储持卡人数据的系统之间安装防火墙的说明。 ▪ 支付应用程序的无线功能使用的任何无线流量的详情（包括详细的端口信息）。 ▪ 配置防火墙来拒绝或（若出于业务需要需使用这些流量）仅允许无线环境和持卡人数据环境间的授权流量的说明。	**软件供应商**：告知客户和集成商/经销商，如果支付应用程序使用了无线技术，则必须按照 PA-DSS 第 6.1 要求更改无线技术供应商的默认设置。 **客户与集成商/经销商**：如果客户或集成商/经销商在支付环境中实施了无线技术，则按照 PA-DSS 第 6.1 要求更改供应商默认设置，并按照*《PA-DSS 实施指南》*与 PCI DSS 第 2.1.1 要求安装防火墙。
6.2	通过无线网络安全地传输持卡人数据	如果支付应用程序开发用来与无线技术配合使用，应说明使用行业最优方法（例如 IEEE 802.11i）以实施持卡人数据验证和传输的强效加密。其中包括： ▪ 配置应用程序以使用行业最优方法（例如，IEEE 802.11.i）来为验证和传输提供强效加密的方法，和/或 ▪ 如何配置所有与支付应用程序捆绑在一起的无线应用程序，以使用行业最优方法对验证和传输实施强效加密。	**软件供应商**：告知客户和集成商/经销商，如果支付应用程序使用了无线技术，则必须按照 PA-DSS 要求 6.2 实施安全的加密传输。 **客户与集成商/经销商**：如果客户或集成商/经销商在支付环境中实施了无线技术，则按照*《PA-DSS 实施指南》*与 PA-DSS 第 6.2 要求使用安全的加密传输。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
6.3	提供关于安全使用无线技术的说明。	提供关于符合 PCI DSS 要求的无线设置的说明，其中包括： ▪ 关于在安装时更改所有无线默认密钥、密码和 SNMP 社区字符串的说明。 ▪ 关于知道密钥的任何人离职或更换岗位时即更改无线密钥、密码和 SNMP 字符串的说明。 ▪ 关于在任何无线网络与存储持卡人数据的系统之间安装防火墙，以及将防火墙配置为拒绝或控制（如果出于业务需要需使用流量）无线环境和持卡人数据环境间的任何流量的说明。 ▪ 关于使用行业最优方法（例如，IEEE 802.11.i）对验证和传输实施强效加密的说明。	**软件供应商：**告知客户和集成商/经销商按照 PA-DSS 第 6.3 要求保障无线技术的安全。 **客户与集成商/经销商：**按照*《PA-DSS 实施指南》*与 PA-DSS 第 6.2 要求，保障无线技术的安全。
7.2.3	为客户提供安全安装补丁和更新的相关说明。	必须向客户和集成商/经销商提供以下内容： • 供应商将如何传达新补丁和更新通知。 • 如何通过已知信任链安全地发布补丁和更新。 • 如何在保持补丁和更新代码完整性的情况下访问和安装补丁及更新。	**软件供应商：**记录并实施传达、发送和安全安装补丁与更新的相关流程。 **客户与集成商/经销商：**根据*《PA-DSS 实施指南》*安全访问并安装补丁和更新。
8.2	仅使用必要且安全的服务、协议、组件及相关软件和硬件，包括第三方提供的上述项目。	记录对于支付应用程序的任何功能而言所必需的所有协议、服务、组件及相关软件和硬件。	**软件供应商：**确保支付应用程序通过以下方式，支持客户仅使用必要且安全的协议和服务等：1) 默认仅安装必要的协议和服务等，以实现“开箱即用”；2) 默认已安全地配置好那些必要的协议和服务等；以及 3) 将必要的协议和服务等记录在案，以作为客户和集成商/经销商的参考。 **客户与集成商/经销商：**按照 PA-DSS 第 5.4 要求，使用*《PA-DSS 实施指南》*中所记录的列表，来确保在系统中仅使用必要且安全的协议和服务等。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
9.1	仅在未连接至互联网的服务器上存储持卡人数据。	必须向客户和集成商/经销商提供以下内容： ▪ 关于不要在面向公众的系统上存储持卡人数据（例如，网络服务器与数据库服务器决不能在同一台服务器上）的说明。 ▪ 关于如何配置支付应用程序，以使用 DMZ 将互联网和存储持卡人数据的系统分隔开来的说明。 ▪ 应用程序要在两个网络区域之间进行通信所需使用的服务/端口列表（以便客户可自行配置防火墙，以便仅打开所需的端口）。	**软件供应商**：按照 PA-DSS 第 9 要求，确保支付应用程序不需要将持卡人数据存储在 DMZ 或接入互联网的系统上，并且允许使用 DMZ。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 9 要求，设置与维护支付应用程序，不要将持卡人数据存储在接入互联网的系统上
10.1	对来自客户环境外部的支付应用程序的所有远程访问实施多因素验证。	向客户和集成商/经销商提供以下内容： ▪ 关于所有来自客户网络外部对支付应用程序的远程访问都必须使用多因素验证以满足 PCI DSS 要求的说明。 ▪ 关于应用程序所支持的多因素验证机制的说明。 ▪ 关于如何将应用程序配置为支持多因素验证的说明（至少使用 PA DSS 要求 3.1.4 中说明的三种验证方法中的两种）。	**软件供应商**：根据 PA-DSS 要求 10.2，确保支付应用程序支持客户对来自客户环境外部的支付应用程序的所有远程访问使用多因素验证。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 10.2 要求，为源自客户环境外的支付应用程序的所有远程访问建立并维持多因素验证。
10.2.1	安全地发送支付应用程序的远程更新。	如果支付应用程序的更新是通过对客户系统的远程访问发送的，请提供以下内容： ▪ 关于根据 PCI DSS 要求 12.3.9，仅当下载需要时才激活用于支付应用程序更新的远程访问技术，并在下载完成后立即关闭访问的说明。 ▪ 说明按照 PCI DSS 第 1 要求，如果电脑是通过 VPN 或其他高速连接方式实现连接的，则经由安全配置的防火墙或个人防火墙接收支付应用程序的远程更新。	**软件供应商**：按照 PA-DSS 第 10.3 要求，安全地发送支付应用程序的远程更新 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*、PA-DSS 第 10.3 要求与 PCI DSS 第 1 要求，安全地接收来自供应商的支付应用程序的远程更新。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
10.2.3	安全地实施远程访问软件。	包括关于必须安全实施对支付应用程序的所有远程访问的说明，例如： ▪ 更改远程访问软件中的默认设置（例如，更改默认密码，并对每位用户使用唯一的密码）。 ▪ 只允许来自特定（已知的）IP/MAC 地址的连接； ▪ 使用强效验证和复杂密码登录（请参阅 PA-DSS 要求 3.1.1 至 3.1.11）。 ▪ 根据 PA-DSS 要求 12.1 启用加密数据传输。 ▪ 在尝试登录失败达到一定次数后，启用帐户锁定功能（请参阅 PA-DSS 要求 3.1.9 至 3.1.10）。 ▪ 在获得访问许可之前，必须建立一个通过防火墙的虚拟专用网络（“VPN”）的连接。 ▪ 启用记录功能。 ▪ 仅限集成商/经销商的授权人员可访问客户环境。	**软件供应商**：(1) 如果供应商可以远程访问客户的支付应用程序，应实施安全的远程访问，比如 PA-DSS 第 10.3.2 要求中所规定的远程访问。(2) 确保支付应用程序支持客户使用远程访问安全功能。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 10.3.2 要求，针对所有支付应用程序远程访问使用远程访问安全功能。
11.1	通过公共网络安全地传输持卡人数据。	如果支付应用程序能够或便于通过公共网络发送持卡人数据，则应包含关于实施并使用强效加密法和安全协议，以确保通过公共网络安全地传输持卡人数据的说明，包括： ▪ 当持卡人数据通过公共网络传输时，须使用强效加密法和安全协议。 ▪ 关于确认只接受可信密钥和/或证书的说明。 ▪ 如何配置支付应用程序，以便仅使用安全版本和安全实施安全协议。 ▪ 如何配置支付应用程序，以防止退回到非安全版本或配置（例如，若适用 TLS，应用程序则不得允许退回到 SSL）. ▪ 如何配置支付应用程序，以便针对所使用的加密方法采用合适的加密强度。	**软件供应商**：按照 PA-DSS 第 11.1 要求，确保支付应用程序支持客户使用强效加密法和安全协议来实现持卡人数据在公共网络上的安全传输。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 11.1 要求，建立与维护强效加密法和安全协议，以确保持卡人数据的安全传输。

PA-DSS 要求	PA-DSS 主题	所需的实施指南内容	控制的实施责任
11.2	对通过终端用户通讯技术传送的持卡人数据进行加密。	如果支付应用程序通过终端用户通讯技术支持发送 PAN，要说明应实施和使用能够使 PAN 不可读的解决方案或实施强效加密法。这些说明包括： ▪ 使用能够使 PAN 不可读或使用强效加密法保障 PAN 安全的定义解决方案的程序。 ▪ 关于当 PAN 通过终端用户通讯技术发送时，其必须时刻保持不可读或受强效加密保护的说明。	**软件供应商**：提供或指定使用能够使 PAN 不可读或实施强效加密法的解决方案，并按照 PA-DSS 第 11.2 要求，确保当支付应用程序通过终端用户通讯技术发送 PAN 时，支付应用程序支持加密 PAN 或使其不可读。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 11.2 要求，使通过终端用户通讯技术传送的所有 PAN 均不可读或采用强效加密法对其进行加密。
12.1	对所有非控制台管理访问进行加密。	如果支付应用程序支持非控制台管理访问，要说明如何配置应用程序以便使用强效加密法，对所有在持卡人数据环境中对支付应用程序或服务器进行的非控制台管理访问进行加密。	**软件供应商**：按照 PA-DSS 第 12.1 要求，如果支付应用程序支持非控制台管理访问，确保支付应用程序对非控制台管理访问实施强效加密。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 12.1 要求，对所有非控制台管理访问进行加密。
12.1.1	对所有非控制台管理访问进行加密。	要向客户和集成商/经销商说明，在对所有非控制台管理访问进行加密时应是实施强效加密法。	**软件供应商**：按照 PA-DSS 第 12.1.1 要求，确保支付应用程序支持客户对非控制台管理访问进行加密。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 12.1.1 要求，对所有非控制台管理访问进行加密。
12.2	针对拥有非控制台管理访问权限的所有工作人员使用多因素验证。	向客户和集成商/经销商提供关于使用多因素验证的说明，包括： • 关于须对所有可对 CDE 进行非控制台管理访问的工作人员使用多因素验证的说明。 • 使用应用程序附带的多因素验证功能（若提供）的程序。	**软件供应商**：按照 PA-DSS 第 12.2 要求，确保支付应用程序向所有具有非控制台管理访问权限的工作人员提供或指定使用多因素验证。 **客户与集成商/经销商**：按照*《PA-DSS 实施指南》*与 PA-DSS 第 12.2 要求，针对所有非控制台管理访问使用多因素验证。

附录 B：针对 PA-DSS 评估的测试实验室配置

对于每次实施的 PA-DSS 评估，PA-QSA 必须确认 PA-DSS 评估测试过程中所使用实验室的状态与能力。该确认书必须与填妥的*认证报告 (ROV)* 一起提交。

对于每一个实验室认证程序，PA-QSA 必须注明用来进行评估和执行这些认证程序的实验室是否为 PA-QSA 或软件供应商的实验室。PA-QSA 需要维护符合以下规定所有要求的测试实验室，并在可能的情况下尽量使用其自己的实验室来实施评估。软件供应商的实验室仅当必要（例如，PA-QSA 未配备运行支付应用程序的大型机、AS400 或 Tandem）且经过确认符合所有实验室要求时方可使用。

PA-QSA 必须确认下表中的所有项目，同时：

- **确定进行 PA-DSS 审查所使用实验室的位置和所有人**
- **描述准备用于 PA-DSS 审查的实验室测试结构与环境**
- **描述在 PA-DSS 审查中，支付应用程序的真实使用情况是如何在实验室进行模拟的**

*PA-DSS ROV 报告模板*提供了每次评估必须提供的实验室认证的详细信息。

实验室要求	实验室验证程序
1. 按照供应商的安装说明或客户所接受的培训内容安装支付应用程序。	**1.** 确认在 PA-DSS 报告中列出的用于模拟真实客户体验的所有平台上对支付应用程序产品进行默认安装时，都遵循了供应商向客户提供的安装手册或培训内容。
2. 安装并测试 PA-DSS 报告中所有的支付应用程序版本。	**2.a** 确认已安装待测支付应用程序的所有常见实施（包括特定地区/国家的版本）。
	2.b 确认已测试所有支付应用程序版本和平台，包括所有必要的系统组件和相关部分
	2.c 确认已测试每个版本支付应用程序的所有关键功能。
3. 安装并实施 PCI DSS 所要求的一切安全策略。	**3.** 确认已在测试系统上实施了 PCI DSS 所要求的一切安全策略（例如，防火墙与杀毒软件）。
4. 安装和/或配置 PCI DSS 所要求的一切安全设置。	**4.** 确认已在测试系统上针对支付应用程序所使用的操作系统、系统软件与应用程序实施了符合 PCI DSS 所有要求的系统设置、补丁等。
5. 模拟支付应用程序的真实使用情况。	**5.a** 实验室模拟支付应用程序的“真实”使用情况，包括所有实施支付应用程序的系统与应用程序。例如，支付应用程序的标准实施可能是指在带有 POS 机和后端办公或公司网络的零售店里设置的客户/服务器环境。实验室模拟完整的实施过程。
	5.b 实验室在模拟/测试中仅使用测试卡号码，不在测试中使用真实的 PAN。 ***注：****测试卡通常可由供应商或处理机构或收单机构提供。*

实验室要求	实验室验证程序
	5.c 实验室执行支付应用程序的授权和/或结算功能，并且按照以下第 6 项的内容检查所有输出。
	5.d 实验室和/或流程对所有可能情况下由支付应用程序生成的输出进行描述，包括暂时的、永久的、错误处理、除错模式、日志文件等。
	5.e 实验室和/或流程通过使用模拟的"真实"数据与无效数据，模拟和验证支付应用程序的所有功能，以包括所有产生的错误状态与日志条目。
6. 提供以下的穿透测试方法能力，并对其进行试用：	**6.a** 使用取证工具/方法：按照 PA-DSS 第 1.1.1–1.1.3 要求，使用取证工具/方法在所有已确认的输出中搜索，以寻找敏感验证数据（如商业工具、脚本等）的证据。[6]
	6.b 尝试利用应用程序漏洞：按照 PA-DSS 第 5.2 要求，利用当前的漏洞（比如 OWASP 十大安全隐患、SANS CWE 前 25 大高危软件错误、CERT 安全编码等），以尝试利用支付应用程序。
	6.c 实验室和/或流程尝试在支付应用程序更新过程中执行任意代码：按照 PA-DSS 第 7.2.2 要求，使用任意代码实施更新过程。
7. 供应商的实验室只有在经确认达到所有要求后方可使用。	如果必须使用软件供应商的实验室（例如，PA-QSA 缺乏运行支付应用程序的主机、AS400 或 Tandem），PA-QSA 可以（1）借用供应商的设备，或（2）使用供应商的实验设施，但上述情况须与测试地点一起详细记录在报告中。无论作何选择，PA-QSA 须确认供应商的设备与实验室达到以下要求：
	7.a PA-QSA 确认供应商的实验室已达到本文件中所规定的一切要求，并已将相关详情记录在报告中。
	7.b PA-QSA 必须验证远程实验室环境的洁净安装，以确保该环境真实地模拟了实际情况，并且供应商还没有以任何方式修改或干预该环境。
	7.c 所有测试均由 PA-QSA 实施（供应商不能对自己的应用程序实施测试）。

[6] 取证工具或方法：是指用于发现、分析与提出取证数据的工具或方法，它能提供一条有效的途径用于快速、彻底地验证、搜寻与再现电脑证据。当取证工具或方法由PA-QSA 使用时，这些工具或方法应能准确地找到由支付应用程序写入的任何敏感的验证数据。这类工具可以是商业性的、开源性的或是由 PA-QSA 内部开发的。

实验室要求	实验室验证程序
	7.d 所有测试 (1) 均在供应商的处所现场实施；或 (2) 经由安全方式连接的网络（例如，VPN）远程实施。
	7.e 在模拟/测试中仅使用测试卡号码，不要在测试时使用真实的 PAN。测试卡通常可由供应商或处理机构或收单机构提供。）
8. 维护有效的质量保证 (QA) 流程。	**8.a** PA-QSA 的 QA 人员确认，测试中已包含 PA-DSS 报告所确定的所有版本和平台。
	8.b PA-QSA 的 QA 人员确认，PA-DSS 的所有要求均已完成测试。
	8.c PA-QSA 的 QA 人员确认，PA-QSA 的实验室配置与流程均达到要求，并已准确记录在报告中。
	8.d PA-QSA 的 QA 人员确认，该报告准确描述了测试结果。