

PCI MPoC 标准



什么是PCI MPoC标准?

PCI MPoC (现成商用移动支付) 是一种可在智能手机和平板电脑等商用移动设备上接受支付的标准。该标准整合了CPoC和SPoC标准的用例。新标准旨在支持在同一设备上输入PIN和非接触式持卡人数据，并增加了对离线交易的支持。

与**EMVCo SBMP** (基于软件的移动支付) 用于虚拟化智能卡的方式类似，PCI MPoC为安全移动支付解决方案提供了框架。

PCI MPoC 标准的组成部分

有关详细组件和要求，请参阅[PCI 安全标准](#)网站上的文档。

以下是 MPoC 文档的摘要：

已通过现有PCI SPoC或PCI CPoC计划验证的产品可提交MPoC计划进行评估。如果通过全面评估验证，这些产品可能会被PCI SSC (安全标准委员会) 接受并列为MPoC产品。

MPoC标准中列出的安全要求提供了一个框架，用于保护MPoC解决方案中捕获和处理的敏感支付信息的机密性和完整性。该框架为参与开发、部署和运营使用COTS设备的商家运营移动支付受理解决方案的实体定义了安全要求、测试要求和指南。

PCI MPoC标准的主要特点

PCI MPoC的主要特点如下：

- **模块化方法：**允许采用模块化、适应性强的方法来处理不同类型的移动支付受理渠道。PCI MPoC 提供开放的安全和测试要求，允许客户定义和定制自己的支付解决方案和使用案例。
- **集成方法：**可以使用预先认证的组件，将其集成到最终解决方案中。
- **AandM 服务：**包括认证和监控服务要求，以确保持续的安全性和合规性。

MPoC 标准的重要性

MPoC标准是几个主要支付系统实施SoftPOS解决方案的要求。在支付市场，信任是最重要的，公司必须确保其系统的安全性，以维护这种信任。那么，如何才能保证这种可靠性呢？PCI MPoC认证标准就是为此而设计的，它是证明产品值得信赖的最佳方式。该认证包括对SDK、APP AandM服务的评估。

此外，通过认证的产品将被列入PCI网站，评估人员、商户、收单机构和其他相关方可在该网站上查看COTS移动支付（MPoC）解决方案。

列入名单是进入这个快速增长的市场的好方法；同时，获得MPOC认证有助于降低风险，应对日益增长的针对商业终端的[网络攻击](#)威胁。

总之，所有打算与主要支付方案合作销售移动POS终端的利益相关者**都有义务确保其产品获得PCI认证。**

MPoC标准安全评估服务

Applus建议采取一些步骤来进行快速简便的评估：

- **预评估**是一种快速有效的方法，可识别文件证据中的遗漏信息和/或错误信息，以满足PCI MPOC的要求。

这项活动的目的是为供应商提供一份问题清单，以减少在评估过程中发现潜在问题的几率，因为潜在问题会导致项目延期和/或额外的评估迭代，这意味着额外的成本。

评估任务包括文件和代码审查。

- **评估**的目的是验证产品是否正确满足所有安全和测试要求。这取决于不同领域的要求（取决于产品功能）：
 - 领域 1: MPoC 软件核心要求
 - 领域 2: MPoC 应用集成
 - 领域 3: 认证和监控
 - 领域 4: MPoC 软件管理

- 领域 5: MPoC 解决方案
 - 评估分为五种不同的操作:
 - **审查**: 测试人员审查设计文档、源代码、配置文件、错误跟踪数据和安全测试结果等证据
 - **测试**: 测试人员使用 SAST、DAST、IAST 和 SCA 等安全工具和技术, 以及代码审查、渗透测试和内存刮擦等手动方法来评估解决方案
 - **观察**: 测试人员观察操作或测试, 记录结果, 尤其是在不同条件下的结果。
 - **访谈**: 测试人员与相关人员交谈, 了解他们的活动、对规定流程的遵守情况以及对政策和程序的了解。
 - **文档**: 测试员在评估报告中记录细节, 以满足当前或未来的测试需要。

所需的文件证明有

- **MPOC 表格**: 如前所述, 根据要评估的产品, 需要填写一些表格。
- **技术文档**: 架构和设计文档以及已实施的安全功能/配置, 包括加密方法、安全密钥管理和安全数据存储。
- **漏洞评估**: 有关公开漏洞和其他漏洞的错误跟踪数据以及保证测试的一些信息。
- **源代码**: 产品的源代码。
- **安全测试工具和技术**: 所有安全工具和功能工具之王, 使实验室能够操作或展示产品的安全稳健性。还包括测试结果。
- **第三方文档**: 任何有助于评估的第三方安全指南、产品信息或证书。

Applus+ Laboratories如何在PCI MPoC标准方面提供帮助?

[Applus+ Laboratories](#)在移动支付应用安全方面拥有丰富的经验, 从EMVCo SBMP (基于软件的移动支付) 产品到最新的PCI MPoC标准都有很高的专业技术水平。

此外, 还有[Common.SECC评估经验](#)。基于软件支付POI保护简介1.2版的详细评估。

利用我们在PCI PTS、EMVCo SBMP和Common.SECC方面的专业知识, 执行快速高效的评估。我们可以帮助您实现MPoC PCI合规性!