PCI MPoC Standard

Ensuring your mobile POS terminals are PCI accredited is essential for maintaining trust and security in the payment market. Applus+ Laboratories provides the expertise and services necessary to achieve and maintain this accreditation efficiently.

What is PCI MPoC Standard?

PCI MPoC (Mobile Payment on Commercial Off-The-Shelf) is a standard that enables payment acceptance on commercial mobile devices, such as smartphones and tablets. This standard integrates the use cases from CPoC and SPoC standards. The new standard is designed to support both PIN and contactless cardholder data entry on the same device and adds support for offline transactions.

Similar to how EMVCo SBMP (Software-based Mobile Payment) is used to virtualize smart cards, PCI MPoC provides the framework for secure mobile payment solutions.

Components of PCI MPoC Standard

For detailed components and requirements, refer to the documentation available at the PCI Security Standards website.

Hereafter a summary on the MPoC documentation is shown:

Products already validated under the already in place PCI SPoC or PCI CPoC programs can be submitted for evaluation under the MPoC Program. If validated through a full evaluation, these products may be accepted by PCI SSC (Security Standard Council) and listed as MPoC products.

The security requirements outlined in the MPoC standard provide a framework to protect the confidentiality and integrity of sensitive payment information captured and processed in MPoC solutions. This framework is defined with security requirements, test requirements, and guidance for entities involved in the development, deployment, and operation of merchant operated mobile payment acceptance solutions that use COTS devices.

Key Features of PCI MPoC Standard

The main key features of PCI MPoC are the following:

- **Modular Approach:** Allows for a modular, adaptable approach to different types of mobile payment acceptance channels. PCI MPoC offers open security and testing requirements, allowing customers to define and tailor their own payment solutions and use cases.
- **Integration Approach:** It is possible to work with pre-certified components to be integrated in the final solution.
- **AandM Services:** Includes requirements for Attestation and Monitoring services to ensure ongoing security and compliance.

Importance of MPoC Standard

The MPoC standard is required by several major payment systems to implement SoftPOS solutions. In the payment market, trust is paramount, and companies must ensure their systems remain secure to maintain this trust. So, how can they guarantee this reliability? The PCI MPoC certification standard is designed for this purpose, providing the best way to demonstrate that your product is trustworthy. This certification involves evaluating the SDK, APP, and AandM Services.

Additionally, certified products will be listed on the PCI website, where assessors, merchants, acquirers, and other interested parties can review Mobile Payments on COTS (MPoC) solutions.

Being listed is a good method to enter in this market that is growing exponentially; at the same time being MPOC accredited helps you to mitigate risks over a growing threat from cyber-attacks targeting business terminals.

In summary, all stakeholders who intend to work with the main payment schemes to sell mobile POS terminals are obliged to ensure their products are PCI accredited.

MPoC Standard security evaluation services

Applus+ Laboratories recommend some steps to perform quick and easy evaluations:

- The **pre-evaluation** is a quick and effective manner to identify missing information and/or wrong information in documentary evidence to face the requirements of PCI MPOC. The objective of this activity is to provide the vendor a list of issues that reduces the chance of potential issues found during the evaluation, which leads to project delays and/or additional evaluation iterations that imply extra cost. The tasks included are documental and code review.
- The **evaluation** is carried out to validate that the product fulfills all Security and Test Requirements correctly. This is done depending on the requirements for the different domains (depending over the product capabilities):
    - Domain 1: MPoC Software Core Requirements
    - Domain 2: MPoC Application Integration
    - Domain 3: Attestation and Monitoring
    - Domain 4: MPoC Software Management
    - Domain 5: MPoC Solution
        - The evaluation is performed in five different operations:
            - **Examination**: The tester reviews evidence such as design documents, source code, configuration files, bug tracking data, and security test results.
            - **Testing**: The tester uses security tools and techniques like SAST, DAST, IAST, and SCA, along with manual methods like code reviews, penetration testing, and memory scraping, to evaluate the solution.
            - **Observation**: The tester watches actions or tests, noting results, especially under varied conditions.
            - **Interview**: The tester talks to personnel to understand their activities, compliance with defined processes, and their knowledge of policies and procedures.
            - **Document**: The tester records details in the evaluation report for current or future testing needs.

The document proof needed are:

- **MPOC Forms**: As previously described there are some forms to be filled depending on the product to be evaluated.
- **Technical Documentation**: Architecture and Design Documentation and Security Features/configurations implemented, including encryption methods, secure key management, and secure data storage.
- **Vulnerability assessment**: Some information about bug tracking data over public and other vulnerabilities, and assurance testing.
- **Source code**: The source code of the product.
- **Security-testing tools and techniques**: All king of security tools and functional tools that allow the laboratory to operate or demonstrate the security robustness of the product. It includes testing results too.
- **Third party documentation**: Any kind of third-party security guidance, product information and or certificates that could help during the evaluation.

How can Applus+ Laboratories help with the PCI MPoC Standard?

Applus+ Laboratories offers extensive experience in mobile payment application security, from high expertise in products **EMVCo SBMP (Software-based Mobile Payment)** to the latest **PCI MPoC** standards.

Additionally, Common.SECC evaluation experience. Detailed evaluations based on the Software Payment POI Protection Profile version 1.2.

Leveraging our expertise in PCI PTS, EMVCo SBMP, and Common.SECC to perform quick and efficient evaluations. We can help you on the path to MPoC PCI compliance!