Estándar PCI MPoC

Garantizar que tus terminales móviles POS cuentan con la acreditación PCI es esencial para mantener la confianza y la seguridad en el mercado de pagos. Applus+ proporciona la experiencia y los servicios necesarios para conseguir y mantener esta acreditación de forma eficiente.

¿Qué es el Estándar PCI MPoC?

El estándar **PCI MPoC (en inglés, "Mobile Payment on Commercial Off-The-Shelf")** es una acreditación que permite aceptar pagos en dispositivos móviles de uso comercial, como smartphones y tablets. Este estándar integra los casos de uso de las normas CPoC y SPoC, y está diseñado para admitir la introducción de datos del titular de la tarjeta tanto con PIN como sin contacto en el mismo dispositivo, añadiendo compatibilidad para las transacciones sin conexión.

Similar al modo en que se usa la certificación EMVCo SBMP (Software-based Mobile Payment) para digitalizar las tarjetas inteligentes, el estándar PCI MPoC proporciona el marco para soluciones de pago móvil seguras.

Componentes del Estándar PCI MPoC

Para conocer los componentes y requisitos detallados sobre este estándar, puedes consultar la documentación disponible en la página web de PCI Security Standards.

A continuación se muestra un resumen de la documentación MPoC:

Los productos que ya han sido validados en el marco de los programas ya existentes PCI SPoC o PCI CPoC pueden presentarse para su evaluación en el marco del Programa MPoC. Si se validan mediante una evaluación completa, estos productos podrán ser aceptados por el PCI SSC (Security Standard Council) y figurar en la lista de productos MPoC.

Los requisitos de seguridad descritos en el estándar MPoC proporcionan un marco para proteger la confidencialidad e integridad de la información de pago sensible capturada y procesada en soluciones MPoC. Este marco se define con requisitos de seguridad, requisitos de prueba, y una guía para aquellas entidades que participan en el desarrollo, la implantación y el funcionamiento de soluciones de aceptación de pagos móviles operadas por comerciantes que utilizan dispositivos COTS.

Características Principales del Estándar PCI MPoC

Las principales características del estándar PCI MPoC son las siguientes:

- **Enfoque modular**: Permite un enfoque modular y adaptable a diferentes tipos de canales de aceptación de pagos móviles. El PCI MPoC ofrece requisitos abiertos de seguridad y pruebas, lo que permite a los clientes definir y adaptar sus propias soluciones de pago y casos de uso.
- **Enfoque de integración**: Es posible trabajar con componentes pre-certificados para integrarlos en la solución final.
- **Servicios AandM**: Incluyen requisitos para los servicios de atestación y supervisión para garantizar la seguridad y el cumplimiento continuos.

Importancia del Estándar MPoC

El estándar MPoC es requerido por varios de los principales sistemas de pago para implantar soluciones SoftPOS. En el mercado de pagos, la confianza es primordial, y las empresas deben garantizar la seguridad de sus sistemas para mantenerla. ¿Cómo pueden garantizar esta seguridad? El estándar PCI MPoC está precisamente diseñado para este propósito, y proporciona la mejor manera de demostrar que un producto es digno de confianza. Este estándar implica la evaluación del SDK, la APP y los servicios de AandM.

Además, los productos certificados aparecerán en la página de PCI, donde asesores, comerciantes, compradores y otras partes interesadas pueden revisar pagos móviles en soluciones COTS (MPoC).

Estar en la lista es un buen método para entrar en este mercado que está creciendo exponencialmente; al mismo tiempo, tener la acreditación MPoC te ayudará a mitigar los riesgos ante la creciente amenaza de ciberataques dirigidos a los terminales de las empresas.

En resumen, todas las partes interesadas que pretendan trabajar con los principales sistemas de pago para vender terminales móviles POS, **están obligadas a garantizar que sus productos cuentan con la acreditación PCI**.

Servicios de Evaluación de la Seguridad del Estándar MPoC

Applus+ Laboratories recomienda algunos pasos para realizar evaluaciones rápidas y sencillas:

- La **preevaluación** es una forma rápida y eficaz de identificar la información que falta y/o la información errónea en las pruebas documentales para hacer frente a los requisitos del PCI MPoC. El objetivo de esta actividad es proporcionar al proveedor una lista de problemas que reduzca la posibilidad de que se encuentren potenciales problemas durante la evaluación, lo que conlleva retrasos en el proyecto y/o iteraciones de evaluación adicionales que implican un coste extra. Las tareas incluidas son la revisión de documentos y códigos.
- La **evaluación** se lleva a cabo para validar que el producto cumple con todos los Requisitos de Seguridad y Ensayos correctamente. Esto se realiza en función de los requisitos de los diferentes dominios (dependiendo de las capacidades del producto):
    - Dominio 1: Requisitos básicos del software MPoC
    - Dominio 2: Integración de aplicaciones MPoC
    - Dominio 3: Certificación y supervisión
    - Dominio 4: Gestión del Software MPoC
    - Dominio 5: Solución MPoC
        - La evaluación se realiza en 5 fases distintas:
            - **Examen**: El examinador revisa pruebas como documentos de diseño, código fuente, archivos de configuración, datos de seguimiento de errores y resultados de pruebas de seguridad.
            - **Ensayo**: El evaluador utiliza herramientas y técnicas de seguridad como SAST, DAST, IAST y SCA, junto con métodos manuales como revisiones de código, pruebas de penetración y memory scraping, para evaluar la solución.
            - **Observación**: El evaluador observa las acciones o pruebas, anotando los resultados, especialmente en condiciones variadas.
            - **Entrevista**: El evaluador habla con el personal para entender sus actividades, cómo cumplen con procesos definidos y su conocimiento de políticas y procedimientos.
            - **Documentación**: El evaluador registra los detalles en el informe de evaluación en caso de necesitar ensayos actuales o futuros.

Las pruebas documentales necesarias son:

- **Formularios MPoC**: Como se ha descrito previamente, hay algunos formularios que deberán ser cumplimentados dependiendo del producto a evaluar.

- **Documentación Técnica**: Documentación de arquitectura y diseño y de las características/configuraciones de seguridad implementadas, incluyendo métodos de encriptación, gestión segura de claves y almacenamiento seguro de datos.
- **Evaluación de vulnerabilidades**: Información sobre datos de seguimientos de fallos sobre vulnerabilidades públicas y de otro tipo, y pruebas de garantía.
- **Código fuente**: El código fuente del producto.
- **Herramientas y técnicas de ensayos de seguridad**: Todo tipo de herramientas funcionales y de seguridad que permiten al laboratorio operar o demostrar la solidez de la seguridad del producto. Incluye también los resultados de las pruebas.
- **Documentación de terceros**: Cualquier tipo de guía de seguridad de terceros, información de productos y/o certificados que puedan ayudar durante la evaluación.

¿Cómo puede ayudarte Applus+ Laboratories con el Estándar PCI MPoC?

En Applus+ Laboratories ofrecemos amplia experiencia en seguridad de aplicaciones de pago por móvil, desde altos conocimientos en productos **EMVCo SBMP (Software-based Mobile Payment)** hasta las últimas normas **PCI MPoC**.

Además, contamos con experiencia en la evaluación Common.SECC. Evaluaciones detalladas basadas en el Perfil de Protección de PDI de Pago por Software versión 1.2.

Aprovechamos nuestra experiencia en evaluaciones de seguridad PCI PTS, EMVCo SBMP y Common.SECC para realizar evaluaciones rápidas y eficaces. ¡Podemos ayudarte en el camino hacia el cumplimiento de la PCI MPoC!