Evaluaciones de seguridad EMVCo SBMP

Applus+ Laboratories está acreditado por EMVCo para evaluar soluciones de pago basadas en la tecnología HCE, así como los componentes del móvil que habilitan la transacción y proporcionan seguridad ante los principales ataques conocidos.

La introducción de la tecnología Host Card Emulation (HCE) revolucionó los pagos por móvil, al permitir soluciones de software seguras para pago. Hoy en día la mayoría de esquemas de pago tienen su propio esquema de certificación para aplicaciones móviles y wallets HCE.

Con el objetivo de facilitar el desarrollo de este tipo de soluciones de pago, EMVCo ha lanzado su propia certificación, EMVCo SBMP (Software-Based Mobile Payment). Este nuevo esquema de certificación no se dirige solamente a la aplicación de pago o el SDK, sino que también sirve para certificar los elementos software y las herramientas que permiten la transacción y que proporcionan las funcionalidades de seguridad en una solución de pago por móvil.

Los desarrolladores de este tipo de productos como TEE, biometría o herramientas de protección de software pueden evaluar sus soluciones bajo esta especificación EMVCo en un laboratorio acreditado. Los desarrolladores de aplicaciones de pago podrán usar estos elementos ya evaluados al desarrollar sus aplicaciones o su SDK para reducir el alcance de la evaluación de seguridad del composite, ahorrando tiempo y reduciendo los costes de evaluación.

Familias de productos evaluables bajo EMVCo SBMP

Applus+ Laboratories está acreditado y cuenta con amplia experiencia para evaluar los diferentes tipos de familias incluidas en el esquema EMVCo SBMP.

- **CDCVM (Consumer Device Card-holder Verification Methods):** La adopción de la biometría por los principales OEM de móviles – huellas digitales, reconocimiento facial o de iris ocular – han convertido este método de autentificación en la principal alternativa frente al clásico PIN, en las aplicaciones de pago móvil. Al certificar su solución biométrica, los desarrolladores pueden ofrecer una ventaja competitiva a sus clientes, facilitando el futuro proceso de certificación de las aplicaciones de pago que funcionaran en ese dispositivo móvil.
- **TEE (Trusted Execution Environment):** Las aplicaciones de pago también pueden utilizar un TEE para asegurar que las transacciones tienen lugar en un entorno aislado que gestiona y protege los activos sensibles. Del mismo modo que en la biometría, al certificar su TEE los desarrolladores facilitan cualquier posterior evaluación de una aplicación de pago en ese móvil.
- **Herramientas de protección de Software:** El esquema EMVCo SBMP también permite evaluar las herramientas que protegen las aplicaciones de pago frente a ataques estáticos y dinámicos. Los desarrolladores de aplicaciones de pago pueden incluir en sus composite herramientas ya certificadas, como librerías criptográficas, White Box crypto, Fuzzing, técnicas que proporcionan ofuscación, anti-tampering, environmental checks u otras, reduciendo de este modo la futura evaluación del producto final.
- **Otros:** Device-binding mechanisms, Drivers, Secure Remote Management mechanisms o Attestation mechanisms.
- **SDK y Wallets/Aplicaciones de pago:** Este esquema de EMVCo también sirve para evaluar el SDK o la aplicación de pago y su metodología es comúnmente aceptada por los principales esquemas de pago.

Pasos de una evaluación EMVCo SBMP

- Revisión de la documentación
- Revisión del código fuente
- Evaluación de vulnerabilidades
- Ataques de penetración

Opciones de certificación para Esquemas de Pago

La mayoría de los esquemas tienen su propio programa de conformidad para soluciones de pago móvil basadas en software. Applus+ Laboratories está acreditado para realizar las evaluaciones de seguridad necesarias para cumplir con los requisitos de seguridad de Visa, Amex, Discover, y Mastercard (que ahora acepta la certificación EMVCo SBMP como prueba de cumplimiento).