EMVCo SBMP Security Evaluations

Applus+ Laboratories is accredited by EMVCo to evaluate HCE-based payment solutions, as well as the components that enable the transaction and provide security to withstand known attacks.

Applus+ Laboratories is accredited by EMVCo to evaluate HCE-based payment solutions, as well as the components that enable the transaction and provide security to withstand known attacks.

The introduction of Host Card Emulation (HCE) revolutionized mobile payment, enabling the implementation of software-based secure payment solutions. Nowadays, most payment brands have their own certification scheme for HCE-based mobile apps and wallets.

In order to facilitate the development of those payment applications, EMVCo launched its own certification for software-based mobile payment (SBMP). This new certification scheme is aimed not only at the payment app and the SDK itself, but also at software elements and tools that enable the transaction and provide security features to the mobile payment solution. Vendors of products such as TEE, biometrics or software protection tools can evaluate their solution under this EMVCo specification in an accredited laboratory. By using already-evaluated elements to develop a mobile app or an SDK, vendors can reduce the scope of the security evaluation, saving time and costs in their future composite evaluation process.

EMVCo SMBP Evaluation Product Families

Applus+ Laboratories is accredited and has extensive knowledge to evaluate the security of all the product families in the EMVCo SMBP scheme:

- **CDCVM (Consumer Device Card-holder Verification Methods):** The adoption of biometrics - fingerprints, iris recognition or facial recognition – by the main Mobile OEM, has turned those authentication methods in to a mainstream alternative to PIN for mobile payment apps. By certifying their solution, biometric vendors can offer a competitive advantage to their clients, easing the certifications process for all the payment apps that will run on that mobile handset.
- **TEE (Trusted Execution Environment):** Mobile Payment apps can also rely on TEE to ensure that transactions take place in an isolated environment that manages and protects sensitive assets. Similar to biometric solutions, TEE vendors can now certify their TEE, facilitating future payment app security evaluations.
- **Software Protection Tools:** EMVCo SBMP also allows evaluating tools that protect mobile payment apps against static and dynamic attacks. Payment vendors can include in their products those evaluated protection tools that offer protection mechanisms such as Cryptographic libraries, like White Box Crypto, Fuzzing, techniques providing Obfuscation, Anti-tampering, Environment checks, and others, and reduce future composite evaluation times.
- **Others:** Device-binding mechanisms, Drivers, Secure Remote Management mechanisms and Attestation mechanisms.
- **SDK and Wallets/Payment Apps:** This EMVCo SBMP scheme also allows to evaluate both SDK and payment apps, and its methodology is commonly accepted by leading payment schemes.

EMVCo SBMP Evaluation steps

- Documentation Review
- Source Code Review
- Vulnerability Analysis
- Penetration Testing

Payment Schemes Certification Options

Most payment brands have their specific compliance program for software-based mobile payments. Applus+ Laboratories is accredited to conduct security evaluations required to comply with Visa, Amex, Discover, and Mastercard security requirements.