3 Reasons Why Your Payment App Needs To Get EMVCo Certified And How App Shielding Can Help You Get There

Authors: Riscure and Promon
Contact Riscure: inforequest@riscure.com
Contact Promon: info@promon.no

Abstract

There are several reasons why mobile payment app providers need to get an EMVCo Software-Based Mobile Payment (SBMP) certification. The evaluation process for software-based payment solutions ensures a thorough security assessment and acceptance from several of the world's largest card brands. In addition, if a mobile payment app provider chooses to integrate with an EMVCo certified App Shielding or SDK solution, it assures them that their app can withstand real-life threats and attacks while simultaneously reducing the app's time to market.

This paper will look at the three main reasons why mobile payment apps need to get EMVCo certified and the benefits of EMVCo SBMP certified Software Protection Tool solutions.

Table of contents

Introduction

As the payment industry - and especially mobile payment solutions - continues to evolve rapidly, it is essential to consider the security impact of these developments. Although the mobile payment (Host Card Emulations (HCE)) has been around for several years, there continue to be rapid developments of mobile solutions and security technologies that support the advancement of secure mobile payment technology and solutions, while attackers also continue to improve their capabilities and tooling.

The EMVCo certification processes exist to facilitate worldwide interoperability and acceptance of secure payment solutions. EMVCo has defined security requirements, evaluation methodologies, and evaluation processes for both card and mobile payment solutions.

As a software-based mobile payment app vendor, there are several reasons why your solutions need to become EMVCo certified. In this paper, we present the three main reasons why a payment app needs to become certified and why mobile payment app providers should implement a certified App Shielding solution.

About EMVCo

EMVCo is a global technical body that facilitates the delivery of reliable, seamless, and secure payments worldwide through specifications and evaluation processes. EMVCo collaborates closely with the payments industry and is owned by some of the world's largest card brands, such as American Express, Mastercard, and VISA.

The EMV Specifications cover a wide range of technologies that support card-based payments. Their Software-Based Mobile Payment program (SBMP) is a standardized security evaluation process designed to determine if software-based mobile payment components or solutions meet a sufficient level of security to safeguard against known and novel attacks.

3 Reasons Why Your Payment App Needs To Get EMVCo SBMP Certified

1. Get Accepted By The Largest Card Brands

In order to bring a mobile payment app to market, it must receive approval from the involved payment card brands. For security certification, EMVCo SBMP is required and recognized by several of the world's largest payment card brands, such as Mastercard, VISA, American Express, Discover, and others.

The SBMP program provides a standardized security evaluation process, methodology, and security requirements and is supported and recognized by all major payment brands and many more. Going through the evaluation process and receiving the EMVCo SBMP certification means that the payment app provider will have a solution supported by some of the largest banks, merchants, processors, vendors, and other industry stakeholders.

EMVCo is also working closely with other industry-standard bodies to provide even more secure frameworks, such as the FIDO alliance, GlobalPlatform, and the Payment Card Industry Security Standards Council (PCI SSC). This further validates the quality of the SBMP process.

2. Ensures a Secure Solution

The EMVCo SBMP evaluation process for Software-Based Payment solutions ensures a thorough security assessment of the payment solution. Receiving the EMVCo certificate for your solution demonstrates that it has been properly evaluated according to the EMVCo SBMP process and methodology. This enables the card brands to undertake their risk assessment processes and provide final security approval for the payment solution.

The SBMP security evaluation process is an approach for evaluating software-based mobile payment components and solutions based on existing procedures. It defines and combines the industry best practices and provides an efficient offering for app providers, promoting a robust security foundation for SBMP solutions.

Passing the SBMP security evaluation proves that the payment solution can withstand both currently known threats and possible future ones due to careful product design and implementation choices,

while using state-of-the-art software protection mechanisms. Receiving the SBMP certificate for your payment app or SDK ensures that the solution has been evaluated against advanced real-life attacks.

To assure that the payment app or SDK can withstand such attacks, it's of vital importance to use state-of-the-art and EMVCo-evaluated Software Protection Tools (SPT) that have proven their quality and robustness against such attacks. The SBMP program enables app developers to gain insight into the quality and robustness of certified Software Protection Tools. This is a vital development realized by EMVCo SBMP. Without such insights, it is practically very challenging for an app developer to make a well-informed decision on which Software Protection Tool is best suited to secure their app.

3. Years of Experience With Real-Life Threats On Mobile

The SBMP evaluation process is a dedicated approach for evaluating software-based mobile payment components and solutions based on existing procedures and industry best practices. It is a standardized process resulting from years of experience in mobile security of payment brands and leading security labs with respect to this innovative technology.

The imposed security requirements for the SBMP security evaluations set by EMVCo are derived from well-defined security objectives and real-life threats and attacks targeting mobile payment applications.

The SBMP evaluation methodology guides the laboratory to evaluate the security of each implemented security function, not only from the functional side but also by malicious use of the functionality and attacking the application as a real-world attacker would.

The SBMP security requirements define and promote a layered approach to the security architecture and implementation of mobile payment apps that the developers can rely on when designing and developing payment solutions. This includes the integration of multiple security mechanisms to fight off various threats and to reduce the risk of attackers abusing the payment application or gaining access to the payment assets, which could lead to scalable fraud. The more layers the attacker needs to peel off, and the more sophisticated and robust these protection layers are, the longer it takes an attacker to get to the core assets. For an attacker, the time and effort put into getting through all the layers would have to be worth it, and with enough layers, it usually isn't.

Attackers will typically go for poorly protected apps or the "low-hanging fruits," which gives a big incentive for app providers to make sure their app has better security than other competing apps. The best way to do that is by integrating the best suited - and EMVCo certified – Software Protection Tool.

Why Choose an EMVCo Certified Software Protection Tool

The SBMP security evaluation process allows a "component" and "integration" evaluation model, making it possible for components to be evaluated independently or together in order to assess the security of the overall solution. The component evaluation model includes, among other things:

- Trusted Execution Environment
- CDCVM
- Software Development Kits of Mobile Payment Applications
- Software Protection Tools

Selecting an evaluated and EMVCo certified Software Protection Tool ensures that the mobile payment app can withstand real-life threats and attacks. At the same time, it can also speed up the certification process for the SBMP application while reducing the risks of ending up with an insecure Mobile payment SDK or Mobile wallet.

Guarantees a Secure App

The most important reason for a mobile payment app provider to utilize an EMVCo certified Software Protection Tool to help protect the payment application is that when the right Application Shielding tool is selected and applied correctly, it will help ensure that the app is protected against real-life threats and sophisticated attacks.

In practice, payment solutions can be insecure as a result of various reasons, including unsuitable or ill configured software protection tools, insecure solution design, implementation errors, and a lack of layered security mechanisms.

The SBMP security evaluation addresses all these aspects and includes the same attack techniques that a real-life attacker would use. The solution design and the app shielding solution's security features are tested against state-of-the-art attack methods by experts.

The attack techniques include both static and dynamic analysis, such as: decompilation, de-obfuscation, exploiting the app functionality to bypass security mechanisms and inject malicious code through instrumentation and app emulation, and exploiting debugging features and advanced key extraction attacks through logical side-channel and fault injection attacks.

The SBMP standard guarantees a consistent security evaluation and certification process, assuring that the security is properly assessed. An evaluated and certified App Shielding solution is proof that it has been evaluated according to the SBMP and to what extent it can protect against expert-level attacks.

The key benefit is that it provides app developers with the necessary insights about the sophistication and robustness of different App Shielding solutions and the individual security mechanisms. As a result, it offers developers the information they need to select the App Shielding solution that best meets their needs.

Reduces The Overall Certification Process

Implementing a certified App Shielding solution can help to reduce the timeline of the payment app's certification process and by reducing the risks of significant vulnerabilities also improve the app's time to market.

When selecting the right EMVCo certified Software Protection Tool solution, the payment app or component developer can reduce the risk of failing the security evaluation significantly. Selecting a Software Protection Tool to help protect and shield the payment application that is sufficiently mature and robust will help ensure that the final solution is sufficiently secure and hence reduce the risk of necessary changes or mitigations in the solution.

In short, this will not only reduce the timeline of the app's certification process, but can also reduce the app's time to market and help the vendor grow revenue faster.

A Layered Approach

The Software-based Mobile Payment Applications operate in the vulnerable environment of the consumer device. Therefore, the SBMP applications often need to apply a layered security approach, incorporating different device and software components to defend against various (potential) threats. However, integrating multiple components can add complexities during the security evaluation and approval process.

An enterprise-grade App Shielding solution will provide a multi-layered approach to application protection to safeguard against a number of expert-level attacks. Each layer is intrinsically connected, providing a synergistic approach to cybersecurity-based attack vectors. When implemented in such a way, a subversive defence is implemented where-by the same vector of attack does not necessarily cause the same response within the application. With effective application shielding, it simply should not be possible to remove each security control one by one. Each of the defences in a well-designed application shield will react through the multi-layered connections within that system, reacting in ways that do not form a consistent pattern and ultimately avoiding a single attack point. For this reason, attackers will move their focus to easier targets where application shielding is not implemented well.

A sophisticated App Shielding Solution should protect against both static and dynamic attacks in a comprehensive manner. When it comes to, for example, debuggers, an App Shielding solution should include countermeasures for both high-level (for example, Java debuggers) and native debuggers, while at the same time taking into consideration indirect debugging through, for instance, emulated or virtual environments. In cases where serious security issues are encountered, for example, an active debugger, the app should exit in a strictly controlled manner in which no useful information is provided to the potential attacker.

As many real-life trojans are attacking the UI components of the app through, for example, screen readers or by exploiting Strandhogg-like vulnerabilities, it is also essential that the App Shielding solution contains a number of security mechanisms and a solid mixture of countermeasures in that area.

Wherever possible, the App Shielding solution should have security checks that are strongly bound to the rest of the app. If the security checks are entirely removed or deactivated, the app should not

be functional anymore. Such security checks should have no, or very limited, dependencies on system resources and API's and should be highly self-contained.

In a robust App Shielding solution, self-integrity checks should definitely be included not only for the security code itself but also for the rest of the app.

The Evaluation Process

The EMVCo SBMP security evaluation process is conducted by accredited expert laboratories that thoroughly test the security robustness of a product. In this process, the laboratory follows a set of security guidelines maintained by EMVCo that both support the laboratories in their evaluations but also support product, component, and solution providers in developing their products.

The security evaluation of an SBMP solution is performed according to the EMVCo SBMP evaluation methodology and requirements. Such an evaluation entails both a vulnerability analysis and penetration testing phase. During the vulnerability analysis, a security review of the solution design and implementation is performed in order to identify potential security vulnerabilities considering known and possible new attacks.

The impact and exploitability of these vulnerabilities are determined during the penetration testing phase, where specific attacks are performed in order to determine the robustness of the implemented security mechanisms and protection of the core payment assets (e.g., cryptographic material, tokens, card data).

An attack consists of two parts, a static and dynamic part. First static analysis is used to identify payment and security-related flows and assets in the decompiled application. Secondly, dynamic analysis and tools are used to obtain the sensitive assets identified and circumvent the identified security mechanisms.

A layered approach and redundancy are required in order to protect against both static and dynamic analysis and payment solutions. From experience, we know that applying advanced, robust, and properly configured software protection tools, in combination with a proper solution design, will help to ensure that the payment solution is robust enough to withstand expert attackers while simultaneously reducing the time to market and the risk of fraud throughout its lifetime.

Receiving EMVCo Certification

Once the solution or component has successfully completed the laboratory's thorough security evaluation, the evaluation report is sent to the relevant payment brands and EMVCo secretariat. Once finalized, the solution or component will receive the EMVCo SBMP Certification and can be listed on the EMVCo website as a certified solution. This is proof that the product has been evaluated according to the EMVCo SBMP process and methodology.

EMVCO's SBMP security evaluation process will ensure a solid security foundation for the software-based mobile payment apps and grant a security evaluation certificate for their components or solutions.

Conclusion

Certifying your mobile payment solution against EMVCo SBMP brings several advantages for component and app developers.

Not only is it required to gain approval by some of the world's largest card brands, more importantly, but it also ensures that the payment solution is secure and protected against state-of-the-art attacks.

The EMVCo SBMP security evaluation process is derived from well-defined security objectives and real-life threats targeting payment applications and guarantees a thorough security evaluation and consistent certification process that confirms that the level of security is determined accurately.

Selecting a Certified EMVCo SBMP Software Protection Tools can help payment app developers to prevent the majority of these risks and subsequently significantly reduce the risk of a vulnerable payment app, and therefore also the risk for fraud and reputation damage while shortening the time it takes for the app to complete the overall certification process and reduce the app's time to market.

About Riscure

Founded in 2001, Riscure is a leading global advisor on the security of connected and IoT devices, as well as a recognized vendor of advanced security testing tools and security training. Riscure helps customers around the world to build robust hardware and software solutions and to speed up the process of secure development and certification.

Since 2007, Riscure has pioneered in assessing the security of mobile solutions and mobile security technology with a current extensive track record of 200+ security evaluations of Mobile Payment and Mobile POS solutions, 25+ OEM Pays with multiple smartphone vendors (OEMs), 25+ Mobile Trusted Execution Environment (TEE) and 50+ Mobile Software Security Solutions including obfuscation, white-box cryptography, and biometric solutions.

Riscure's expertise is well recognized by the industry and has many accreditations, among which are Visa, MasterCard, Discover, American Express, EMVco, PCI, GlobalPlatform, Common Criteria certification body accreditation, ARM PSA, SESIP, Nagra, Irdeto, Verimatrix, and Synamedia, to perform security assessments of a wide variety of solutions.

About Promon

Since 2006, Promon have been pioneers in app security and App Shielding. They are delivering world-leading security software to many of the largest banks around the globe and is trusted by more than 50% of the leading banks in Europe.

Promon works across a range of industries with a variety of global Tier 1 clients, counting customers in industries such as finance, health, the public sector, and more.

Promon's technology is research-based and originates from the internationally recognized research environments at SINTEF and the University of Oslo. Promon's patented deep protection technology Promon SHIELD™ is protecting apps used by hundreds of millions of users.

Promon SHIELD™ protects apps from numerous attacks at both rest and at runtime, preventing methods such as repackaging, app tampering, and different malware-style attacks.
In 2021, Promon SHIELD™ went through a thorough security assessment and got EMVCo evaluated.

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road,
Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com

Promon HQ
Stortingsgata 4, 0158 Oslo
info@promon.no
www.promon.co

Promon Asia Pacific Limited
(+852) 3915 7642
Unit 1204, Everglory Centre
1B Kimberley Street, TST Kowloon, Hong Kong S.A.R.
info@promon.no
www.promon.co