

Leading Mobile Payment App SDK Company Meets PCI Requirements with DexGuard and iXGuard



Protects customers' application from jailbraiking, rooting, debugging and tampering.

The Company

As a leading provider of mobile application SDKs for iOS and Android mobile payment applications, this company makes sure that paying with smartphones is safe and userfriendly. Merchants, acquirers and payment service providers rely on this company's SDKs to build secure mobile applications for consumers.

The Challenge

Mobile payment applications have a strict set of compliance requirements to follow. For example, all of the company's customers need to comply with Payment Card Industry (PCI) SDK 3DS Security Standards. As a result, the company must ensure that the SDK itself is compliant with these standards.

COMPANY DETAILS

Industry

Financial

Privately / Publicly Owned

Private

Employees

650

Challenges

- Meeting PCI compliance requirements
- Hardening SDK to prevent rooting, jailbreaking, debugging and tampering

Solutions

- DexGuard
- iXGuard



"Payments is such a sensitive industry. Nobody wants to lose money, so security was a big priority for us. Not only did we need to secure our SDK for compliance purposes, but we also wanted to offer the most secure product for our customers."

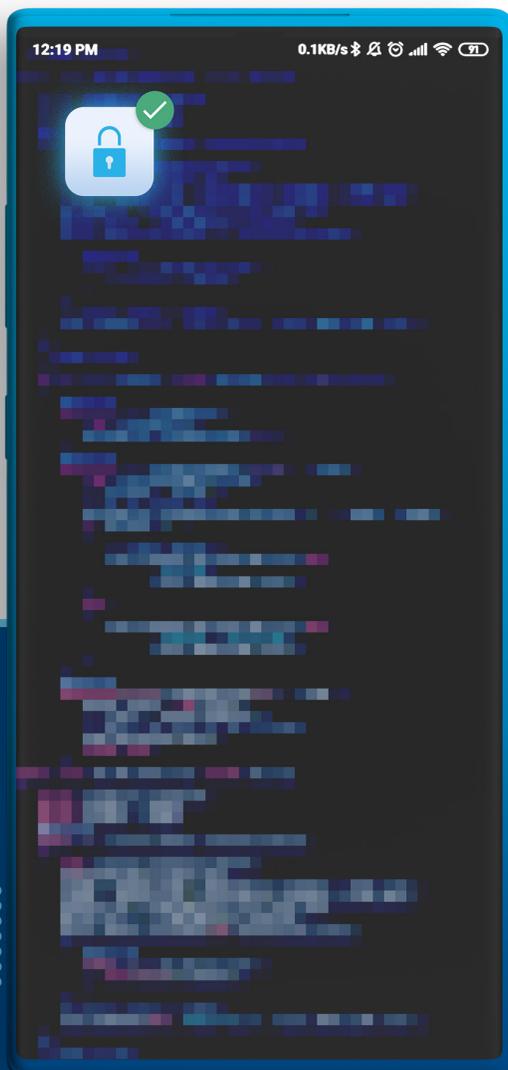
— **Product manager** at the leading mobile payment app SDK company

Working with a small security team servicing a wide variety of customers, the company turned to a solution that could help automate some of the steps toward PCI compliance. Specifically, the company needed to harden the SDK, to ensure that:

- It's not working on a rooted or jailbroken device
- There is no debugger attached
- The integrity of the SDK is not tampered with

“Guardsquare has made it harder to break or modify our software. It also gives important information to our users if there’s a security issue. Our SDK has an API that allows developers to know if the application is jailbroken, a debugger is attached, integrity is tampered with, and more. Guardsquare does all of this without affecting the performance of the software.”

— **Product Manager** at leading mobile payment app SDK Company



The Solution

After an evaluation, the security team selected Guardsquare’s DexGuard (Android) and iXGuard (iOS) tools for hardening their mobile payment SDK. The tools were deployed to make the company’s product obfuscated and encrypted, so it is harder for an attacker to break the SDK or read its code.

The Result

Guardsquare’s solutions helped the company meet its PCI mobile payment acceptance compliance requirements. As a result of implementing DexGuard and iXGuard, the SDK is hardened and provides maximum protection for customers, who are mobile payment application developers themselves.

In addition, the company’s developers have had a positive experience with Guardsquare’s support and product management teams, who have quickly resolved issues and responded to suggestions on how to improve DexGuard and iXGuard. The company looks forward to testing additional features like Protection Report and incorporating them into the product.

PROTECT

TEST

MONITOR

Curious to see how **Guardsquare** can protect your banking mobile apps against common attacks?

[Request a Demo](#)

Guardsquare offers the most complete approach to mobile application security on the market. Built on the open source **ProGuard**[®] technology, Guardsquare's software integrates seamlessly across the development cycle. From app security testing to code hardening to real-time visibility into the threat landscape, Guardsquare solutions provide enhanced mobile application security from early in the development process through publication.

More than 900 customers worldwide across all major industries rely on Guardsquare to help them identify security risks and protect their mobile applications against reverse engineering and tampering.