PROMON

How Application Shielding supports PSD2 compliance

Contents

Are you PSD2-ready?

The Payment Services Directive 2 (PSD2) legislation requires payment service providers (PSPs) to contribute to a more integrated, secure, and efficient payments ecosystem.

The most important requirements related to mobile app security are present in the Article 9 of the final Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC).

PSD2 takes effect on 14 September 2019. It will apply to all payment services within the EU and the EEA. For mobile banking apps, the security requirements set out in PSD2 point to a need for protection against known and unknown attacks against mobile apps.

Are you prepared?

PSD2 security requirements

The European Banking Authority (EBA) has developed Regulatory Technical Standards (RTS) to ensure an appropriate level of security for payment service users. These standards include two key security requirements: Monitoring mechanisms for malware, and security measures to mitigate risks for mobile users.

Malware detection and protection

Article 2 and 3 of the RTS states that payment service providers must implement transaction monitoring mechanisms to detect signs of malware infection in any sessions of the authentication procedure.

Secure execution environment

Payment service providers must have security measures in place to mitigate risks resulting from compromised devices (e.g. rooted or jailbroken). Article 9 of the RTS is of particular importance.

PSD2 security requirements: Article 9

Paragraph 2

Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device (such as mobile phone or tablet) to mitigate the risk which would result from that multi-purpose device being compromised.

Paragraph 3

For the purposes of paragraph 2, the mitigating measures shall include each of the following:

a) the use of separated secure execution environments through the software installed inside the multi-purpose device;

b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;

c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

The mobile threat landscape

Mobile security threats come in many forms, and they continue to evolve. The business impact from compromised apps typically results in one or more of the following:

- ⊗ Reputational damage
- ⊗ Substantial fines
- ⊗ Increased support and development costs

What are the biggest risks to mobile banking and payment app security today?

Compromised devices

Compromised devices are potential security threats to your mobile environment you need to address. There are two types of compromised devices: «Jailbroken» Apple iOS devices and «rooted» Android devices. These devices become compromised because users have actively altered them from their original manufacturer settings, or by mobile malware armed with rooting frameworks. Altering these devices intentionally removes integral security settings in your network, and puts your enterprise resources and data at risk.

Repackaging

Repackaging an app means that an attacker obtains a copy of the app from the distribution platform (Google Play Store or Apple App Store). The attacker then adds malicious functionality to it, and redistributes the app to users who are led to believe they are using a legitimate app.

Keylogging

Malware can track the keys struck on your keyboard, typically in a covert manner so that you don’t know that your actions are being monitored. This is usually done to collect personal information, such as credit card numbers, usernames and passwords.

Overlays and UI spoofing

Theft of user information using malware that overlays its own windows on top of another program, or scenarios where malware can condition the system to display a spoofed user interface (UI) to the user instead of the real UI from the original app. These types of malware aim to capture the user’s login credentials, such as username and PIN codes.

Code injection

Attackers can inject code to gain control of the app from within. This enables the app to be modified to log the PIN code of the user, or to manipulate the beneficiary of a financial transaction.

How Application Shielding supports PSD2 compliance

When running in a vulnerable operating system (OS), apps can be manipulated by an attacker. As a result, payment apps with high-security requirements cannot rely solely on the OS security features. Instead, they need to protect themselves with advanced obfuscation, app integrity checks and runtime protection features.

These sophisticated security features are sometimes called RASP (runtime application self-protection).

Promon has introduced the concept of Application Shielding with runtime protection as one of the first providers in the market. The implementation of Promon security solutions provides protection for your payment and authentication solutions, which then can safely be used for mobile payment or other authentication use cases.

Apps that are protected with Application Shielding can mitigate the whole range of sophisticated attacks, including:

- ✓ Malware attacks
- ✓ Vulnerabilities related to compromised devices
- ✓ Debugging
- ✓ Code or framework injection
- ✓ Application repackaging and app integrity breaches
- ✓ Malicious screen readers or untrusted keyboards
- ✓ Overlay attacks and UI spoofing
- ✓ Man-in-the-app and man-in-the-middle scenarios
- ✓ Stolen keys or other secrets embedded inside the app

Promon Shield for Mobile™ provides cost-efficient, hassle-free mobile app security

A common concern when implementing new security solutions is the complexity of integration and impact on development resources.

Promon's Application Shielding solution is an exception.

Promon Shield for Mobile™ can be integrated into a payment app automatically, without any need for programming, and with close-to-zero impact on development resources and project timeline.

Post-PSD2, mobile banking and payment apps need to run inside secure execution environments. They need to be protected against malware and alteration of their functionality. Shield for Mobile upholds the strictest international compliance requirements, including PSD2 compliance.

PROMON

About Promon

Promon leads the way in proactive mobile app security. For 19 years, we've been making the world a safer place by securing any app, on any device—in no time at all. Today, we protect over 2 billion users, secure 13 billion monthly transactions, and safeguard $2.5 trillion in market cap. Promon is headquartered in Oslo, Norway, with offices in more than 15 countries around the world.

Would you like to talk to an expert?

Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

Book a meeting »

promon.io

Promon AS
Cort Adelers Gate 30
0251 Oslo
Norway