PROMON

PCI MOBILE PAYMENT ACCEPTANCE SECURITY GUIDELINES

How In-App Protection can help you meet the PCI guidelines

Meeting industry standards

Mobile payment methods have revolutionised the way different sectors such as banking, commerce and retail can do business – and also the way consumers easily can perform transactions, purchases and payments. But with new payment methods comes new challenges and possibilities for cybercriminals to get access to very sensitive customer information.

If your mobile application accepts, processes, stores, or transmits payment card information, you will need to meet certain accepted industry standards for handling and protecting payment card information and become PCI compliant.

Meeting these standards can be achieved by following a number of objectives and guidelines for the security of payment transactions, as well as for the risk and controls in the supporting environment, found in the PCI Mobile Payment Acceptance Security Guidelines for Developers.

Below are several of the technical guidelines for applications accepting electronic payments on mobile devices found in section 4 in the PCI Mobile Payment Acceptance Security Guidelines for Developers, and a high-level overview on how Promon SHIELD™ In-App Protection can help you meet them. Also note that our solutions mentioned in this checklist can also help you meet several of the points in requirement 6 in the PCI DSS.

PCI guidelines

4.1	Prevent unauthorized logical device access
4.2	Create server-side controls and report unauthorized access
4.3	Prevent escalation of privileges
4.7	Harden the applications
4.9	Conform to secure coding, engineering and testing
4.11	Protect the mobile device from unauthorized applications
4.12	Protect the mobile device from malware
4.16	Provide an indication of secure state

4.1 Prevent unauthorized logical device access

This guideline says you should protect mobile devices from unauthorized logical access. The use of In-App Protection techniques can help prevent unauthorized logical access to a device by making it more difficult for an attacker to modify or reverse engineer the software by reducing the attack surface.

How Promon SHIELD™ facilitates meeting this guideline

Promon SHIELD™ provides code obfuscation to hide sensitive APIs and critical operations in the app and make it harder for an attacker to reverse engineer how your app works. Our feature Secure Application ROM will also help you further safeguard private certificates to protect your network and API communications. This is complemented with our state-of-the-art runtime protection that detects threats such as application debugging, code injection, privilege escalation (device rooting/jailbreak), and application tampering in real-time.

Our security software can also detect a device with developer mode enabled, detect if Android Developer Bridge is active, and detect apps that are not from a trusted source, such as Play Store etc.

4.2 Create server-side controls and report unauthorized access

This guideline says that you should develop the overall payment-acceptance solution to include capabilities for preventing and reporting unauthorized access attempts, identifying and reporting abnormal activity, and discontinuing access.

How Promon SHIELD™ facilitates meeting this guideline

Promon SHIELD™ can notify your application about a security event using a callback interface, which can be used to notify the end-user or back-end system about possible security problems. In addition, our feature, Secure Application ROM, will also help safeguard private certificates to protect your network and API communications.

4.3 Prevent escalation of privileges

This guideline suggests that controls should exist to prevent the escalation of privileges on the device. Bypassing permissions can allow untrusted security decisions to be made, thus increasing the number of possible attack vectors. The device should be monitored for activities that defeat operating-system security controls, such as jailbreaking or rooting. Hardening the app can help prevent escalation of privileges in a mobile device.

How Promon SHIELD™ facilitates meeting this guideline

Our security software provides security checks that are crucial for preventing the risk of privilege escalation. Promon SHIELD™ has several layers of root/jailbreak detection mechanisms to handle the most well-known approaches, as well as more heuristics type indicators that are looking for symptoms of a compromised device. These security checks can also be configured to notify your back-end system for analytics of usage.

4.7 Harden the applications

This guideline says that mobile payment-acceptance applications should be hardened to prevent unintended logical access or tampering with the app, such as code injection or reverse engineering.

How Promon SHIELD™ facilitates meeting this guideline

Our solution uses several methods to harden an app. Tamper detection checks will verify the integrity of the application signature when launching the app. Based on heuristic analysis of the device, Promon SHIELD™ is able to detect debuggers and emulators and prevent repackaging of the app. It also offers capabilities to detect the presence of code hooks and to block injection of malicious code into the application process. In addition, Promon SHIELD™ provides code obfuscation to make it harder for an attacker to reverse engineer your application.

4.9 Conform to secure coding, engineering and testing

This guideline suggests that developers should be trained on PCI standards and secure coding best practices. Developers should document their implementation and create a formal response plan to identify and mitigate new risk. The guideline references the Mobile OWASP Top 10 Risks, which includes the threats “M8: Code Tampering” and “M9: Reverse Engineering”, where runtime application self-protection and obfuscation is recommended as countermeasures.

How Promon SHIELD™ facilitates meeting this guideline

Promon SHIELD™ is designed to make your application self-defending and able to detect and react to all threats defined in M8 and M9, such as: jailbreaks/rooting, malware, debuggers/ emulators, and unauthorized modification of your application. Our security software also helps you prevent common coding vulnerabilities in software development processes, such as insecure cryptographic storage (outlined in M5), and ensures that local data and data stored in your application is non-copyable and properly protected.

4.11 Protect the mobile device from unauthorized applications

This guideline suggests that all authorized mobile apps should have a mechanism that permits authentication of the source and integrity of the executable file, and the system should prevent the loading and subsequent execution of applications that cannot be authenticated.

How Promon SHIELD™ facilitates meeting this guideline

Our tamper detection checks are able to verify and protect the integrity of the application to prevent unauthorized modifications, and our solution offers the possibility to detect and react when an app has been repackaged. Our features Secure Local Storage (SLS) and Secure Application ROM (SAROM), will ensure the protection of API keys, certificates and other secrets that you need for authentication on device (SLS) or in app (SAROM). In addition, our solution is able to detect if apps from untrusted sources are installed.

4.12 Protect the mobile device from malware

This guideline says it's ideal to deploy security software to protect the device from malicious software and applications. It also suggests application hardening / In-App Protection software, which can be employed to prevent and/or remove malicious software and applications.

How Promon SHIELD™ facilitates meeting this guideline

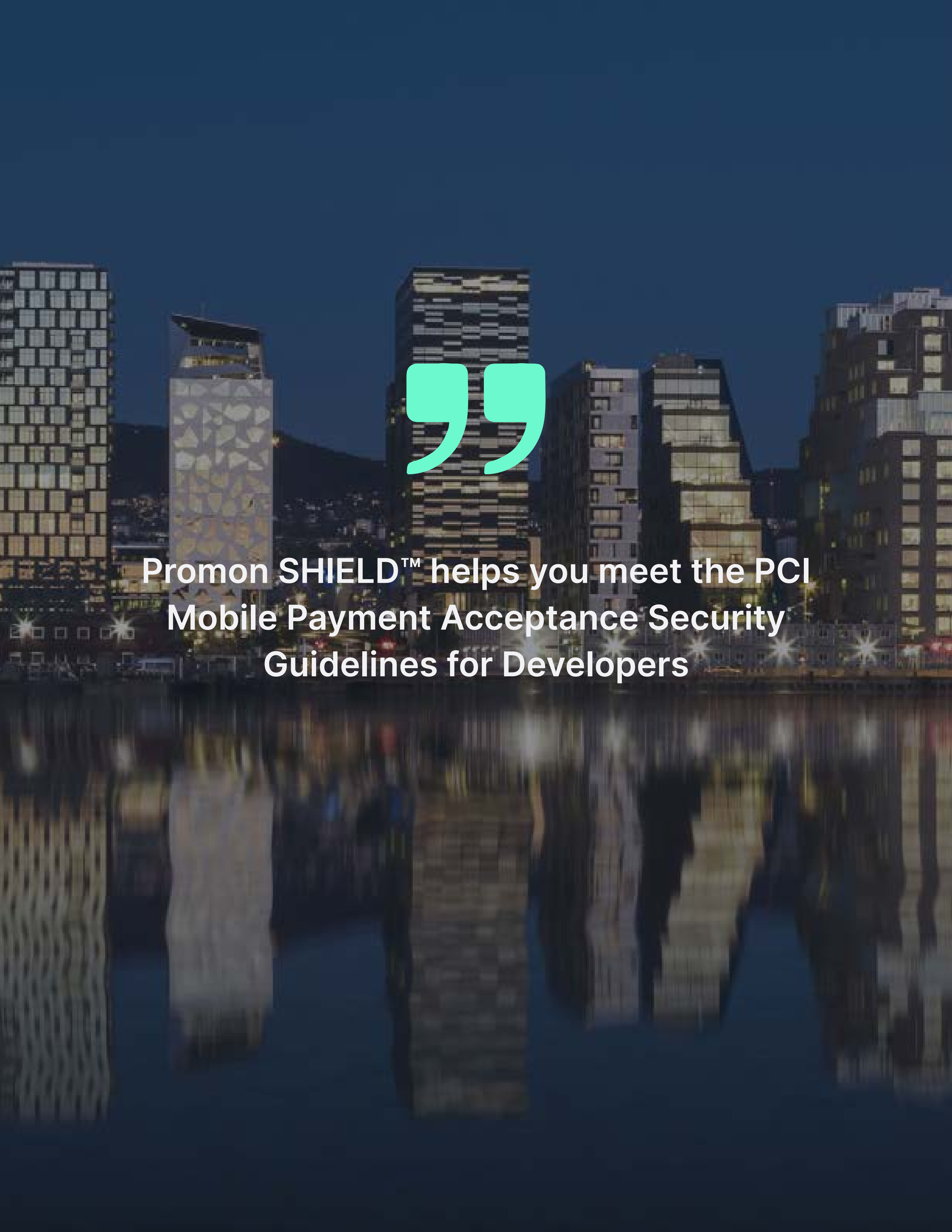
By using our security software, you will have a protected mobile app that is able to modify its behavior in real-time to interrupt potential malware attacks. Promon SHIELD™ mitigates the risks from common malware attack methods such as: Android Accessibility API abuse / UI Spoofing, overlay attacks/screenreaders, and keyloggers.

4.16 Provide an indication of secure state

This guideline states that a trusted execution environment must include mechanisms for indicating to the mobile device user that the payment-acceptance app is executing in a secure state.

How Promon SHIELD™ facilitates meeting this guideline

Promon SHIELD™ can verify the trust level of the execution environment and detect if a device is in a secure state or not before launching the app. Additional Promon features such as Trusted Execution Zone (TEZ) takes your application security to a new level by creating a dedicated trusted execution environment for the important parts of your application. In this way TEZ enables app providers to move into a trusted execution zone with ease.



Promon SHIELD™ helps you meet the PCI Mobile Payment Acceptance Security Guidelines for Developers

Promon SHIELD™

4.1	Prevent unauthorized logical device access
4.2	Create server-side controls and report unauthorized access
4.3	Prevent escalation of privileges
4.7	Harden the applications
4.9	Conform to secure coding, engineering and testing
4.11	Protect the mobile device from unauthorized applications
4.12	Protect the mobile device from malware
4.16	Provide an indication of secure state

Conclusion

Mobile applications play an increasingly large role in payment transactions, and safeguarding these apps and meeting the PCI Guidelines is vital. Our in-app protection solution Promon SHIELD™ ensures app integrity and safeguards your mobile app against reverse engineering and hacking.

Our solutions listed in this document can help you meet several points in the PCI Mobile Payment Guidelines, such as: code obfuscation to make it harder for an attacker to reverse engineer your application, tampering detection checks to verify and protect the integrity of the app, and the possibility to detect and react when your application has been repackaged.

Also note that our solutions mentioned in this checklist can also help you meet several of the points in requirement 6 in the PCI DSS.

PROMON

Get in touch

www.promon.co
info@promon.no
+47 22 02 11 30