ZIMPERIUM®

Top 5 ways to build a compliant SoftPOS app

SoftPOS apps

Contactless payments were already growing before the Covid-19 pandemic, but stricter rules around surface cleanliness and the use of cash have accelerated their usage significantly.

In a global study, Mastercard found that 80% of people surveyed preferred contactless payments, and 74% intended to continue with the payment form post-pandemic. Similarly, Accenture forecasts that $7 trillion worth of transactions will have moved from cash to cards and digital payments by 2023.

One of the most potent forces driving this growth has been the pre-existing near-field communication (NFC) technology built into many smartphones and tablets. With NFC, commercial off-the-shelf (COTS) devices can be turned into payment devices known as software point of sale (SoftPOS) terminals.

The benefits of SoftPOS for both businesses and payment processors are manifold and include:

- There is no need for specialized certified hardware
- Works on a wide variety of already owned or more cheaper smart devices
- Reconciles payments over a cellular connection, allowing them to work from virtually anywhere
- Can speed up payment processes
- Widens the acceptance for digital payments in emerging markets

Today more software developers and digital payment providers are publishing SoftPOS apps to either enter or expand their presence in the field. But the security and compliance elements of their solutions will determine the success and adoption of their SoftPOS solutions.

5 tips for building a compliant SoftPOS app

1 Understand the standards

Payment Card Industry (PCI) Security Standards organization is a global body that delineates the obligations and standards expected of companies in the field. The PCI has different compliance standards for merchants and payment processors and has recently published its security standards for Contactless Payments on COTS (CPoC) and SoftPOS technology, which we explored in detail in this whitepaper.

Compliance with the PCI standards for SoftPOS includes the following requirements about data usage, cryptography, and cryptographic key management. Compliance is necessary to be an accepted vendor for most major credit cards. While not federally mandated in the U.S., it is mandatory for card payment processors through legal precedent.

2 Deploy strong application protection measures

Virtually all attacks on software applications start with the attacker reverse engineering the app's code to determine the structure and logic. They then test for flaws they can exploit and proceed to tamper with the app's behavior. The PCI CPoC Standard clearly calls out the importance of deploying tamper-resistance—section 2.1 outlines eight different measures that apps must comply with. These include rooting and jailbreak detection, and other forms of application tampering, when detected, need to result in the non-acceptance of payment data.

3 Get the testing right

SoftPOS applications must be periodically and rigorously penetration tested to achieve and maintain compliance. It's critical to engage an accredited testing lab versed in PCI compliance that can help guide you through the certification process. Using a mobile application security testing (MAST) tool to continuously scan and test your application can help to identify compliance and security issues early in the software development life cycle and prevent delays further down the process.

New threats constantly emerge, needing to ensure that your app's security mechanisms are sufficient. Moreover, the PCI CPoC Standard requires software-based key protection mechanisms to be evaluated, at least annually, against current attack scenarios and vectors.

4 Use a white-box cryptography solution that facilitates certification

The PCI standards for SoftPOS prioritize the protection of consumer data, payment information, and funds. Strong cryptography and encryption key security are necessary to ensure security throughout the entire lifecycle of a SoftPOS transaction. Usually, this is achieved using hardware support, such as a trusted execution environment (TEE) and Secure Enclave, but not all COTS devices come with these built-in. So relying on these hardware-based security mechanisms results in security gaps when running on non-compliant hardware. Especially considering that the vendor has no control over the hardware eventually used.

Compliant SoftPOS apps must employ either software-based or hybrid security mechanisms to account for the fragmentation in COTS hardware. PCI CPoC Standard lays out the requirements for using software-only white-box security. Opting for a white-box-only approach can significantly improve time-to-market as it inherently works across all devices. White-box cryptography solutions geared explicitly toward PCI CPoC requirements will further accelerate development and certification timelines. For example, look for support for Derived Unique Key Per Transaction (DUKPT) and TR-31 key blocks so that you do not need to develop these types of controls internally.

5 Keep on top of evolving regulations

As the usage of SoftPOS applications grows and the technology evolves, the standards governing contactless transactions will also continue to mature. The next update will most likely include major additions for PCI, such as the requirements governing PIN protection on SoftPOS. Going by the working title of "Mobile Payments on COTS", the update is expected to be published in the first half of 2022.

The merging of requirements for PIN and card details to be protected through separate encryption will add a new layer to the security implementations on SoftPOS apps, most likely requiring discrete white-box deployments for each. These changes and others will be the norm, so it is essential for app vendors in the SoftPOS sphere to have a security team or third-party vendor who can keep their product in compliance.

Choose the right partners for SoftPOS success

The growth of SoftPOS usage is excellent news for mobile solution providers in the field. However, risk reduction and trust between merchants, payment providers, and individual customers are paramount for adoption, success, and revenue security. These can be achieved by implementing robust security technology that keeps data and your customers safe and helps you comply with global industry regulations while preserving a frictionless payment experience.

Zimperium's application shielding and white-box cryptography solutions meet and exceed the highest payment app security and compliance standards.

With Zimperium's Cryptographic Key Protection, you get white-box cryptography technology built for PCI certification, including out-of-the-box support for specifications such as changing the white-box implementation and cryptographic keys monthly, DUKPT key management, TR-31 key blocks, the separation of payment card and PIN cryptographic modules, and other key protection requirements.

Zimperium's Application Shielding solution embeds advanced anti-reverse engineering and anti-tampering protections into your SoftPOS app that go well beyond regulatory requirements.

Zimperium's Mobile Application Security Testing (MAST) solution helps mobile app developers identify reputation and financial risks by automatically identifying privacy, security and compliance risks in the development process before apps are released to the public.

Zimperium helps enterprises build secure and compliant payment applications and SDKs for mobile and connected devices. Click here to talk to someone on our team.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244