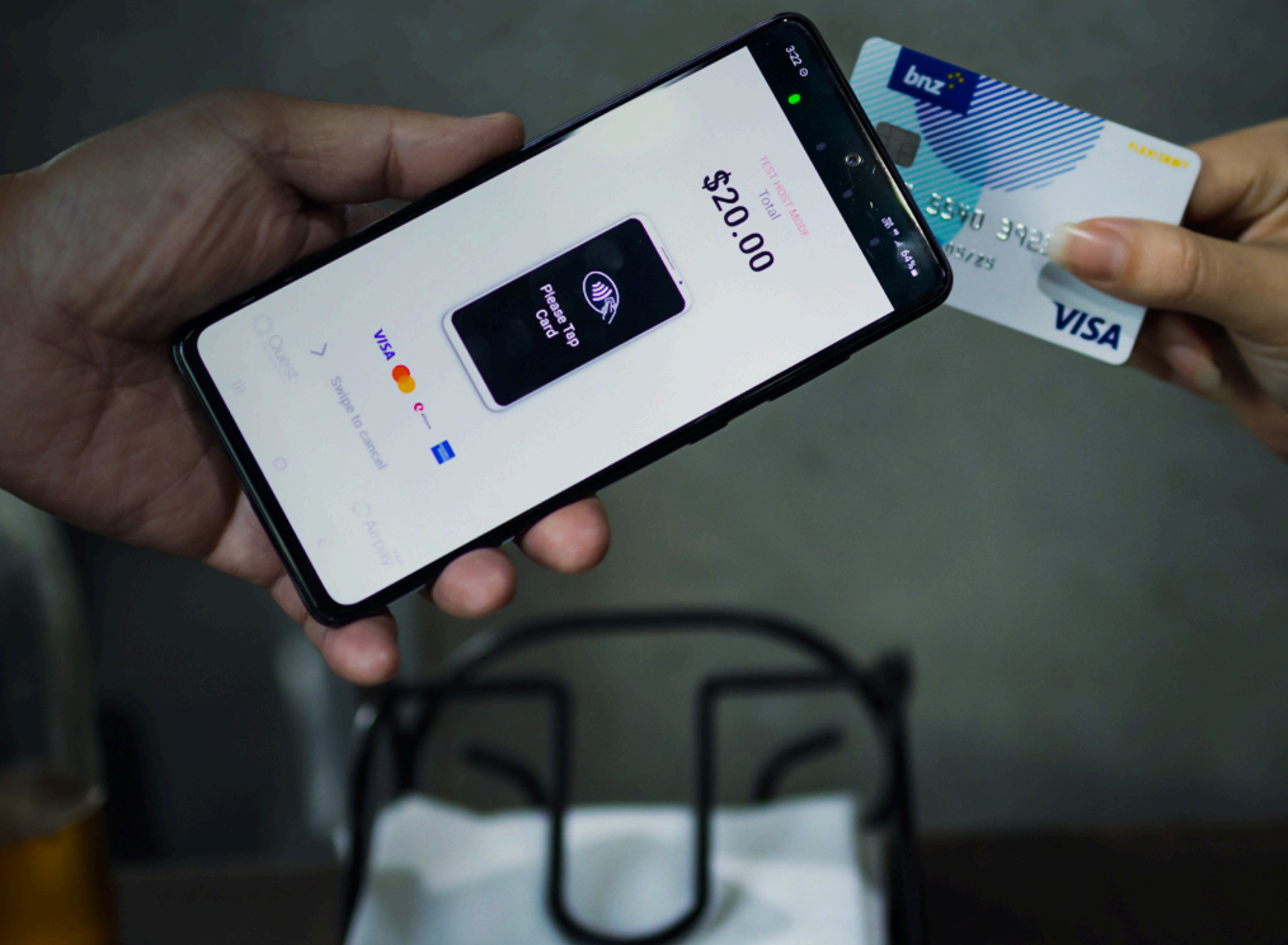
ZIMPERIUM®

Secure PIN-entry on COTS Devices using Zimperium Secure PIN



The Payment Card Industry's (PCI) Mobile Payments on COTS (MPoC) provides an industry-wide standard for software-based point-of-sale (SoftPOS) solutions. These SoftPOS solutions enable merchants to receive payments from NFC-enabled devices like Android or iOS smartphones and tablets.

The upcoming MPoC standard replaces the existing PCI SPoC and PCI CPoC standards. It introduces a modular standard that offers different certification options and supports offline transactions and software-based PIN entry. MPoC enables software-based PIN entry on the same COTS device that interacts with the NFC-enabled consumer payment method, including debit and credit cards, wearable devices, and mobile wallets. As a result, this standard represents a significant breakthrough within the payment card industry. However, to employ this standard, organizations must address significant security requirements to safeguard the PIN data.

The MPoC standard is expected to accelerate merchants' global adoption of SoftPOS solutions. However, in order to gain PCI certification, solution developers must ensure their SoftPOS solutions comply with the MPoC's robust security requirements. This includes:

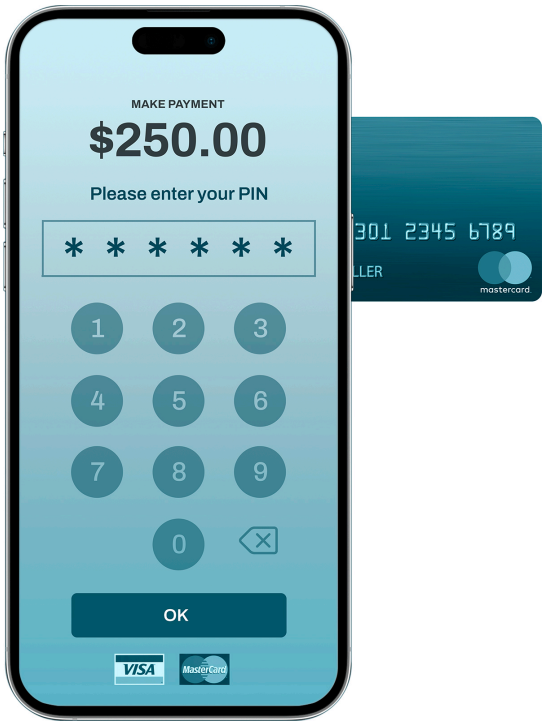
- requirements for ensuring solutions protect cryptographic keys and are resistant to advanced reverse engineering and tampering with the SoftPOS mobile applications
- visibility into threats and compromise of the COTS platform as part of the attestation and monitoring system
- prevention of the disclosure or manipulation of assets such as the cardholder's primary account number (PAN) and PIN data

The Need for Secure PIN entry

Software-based PIN entry on COTS mobile devices introduces significant security risks. That's because traditional graphical user interfaces (GUIs) are built using components provided by the operating system. These user-interface components are vulnerable to several attack techniques that enable malicious actors and malware to intercept or retrieve PIN data.

Here are a few common techniques that attackers can use to steal sensitive information, including PINs:

- Screen recording
- Activity hijacking
- Clickjacking / Tapjacking



The above attacks are typically deployed by first tricking the merchant into installing a malicious app. This malicious app then begins monitoring the activities of the SoftPOS app and attempts to intercept sensitive information.

If a malicious actor acquires elevated device privileges, an even stronger class of attacks is possible (a technique generally referred to as "rooting" in Android devices or "jailbreaking" in iOS devices). This level of access gives the attacker additional power, enabling them to monitor, record, and analyze all memory and execution processes on the mobile device. These access methods can even enable side-channel attacks in which threat actors use device peripherals, such as the gyroscope or accelerometer, to capture the PIN. All these threats have to be considered and mitigated.

To combat these threats, solution providers must ensure that:

1. the PIN entry component thwarts as many attacks as possible, and
2. keeps the PIN data and its encryption keys secret even if the attacks cannot be prevented

Introducing Zimperium Secure PIN

Zimperium's zKeyBox solution provides a set of tools that enable SoftPOS developers to implement a secure GUI-based PIN entry mechanism in Android applications. Combined, these tools form an add-on feature called **Secure PIN**. This highly configurable add-on is designed to help SoftPOS developers meet the relevant MPoC standard's requirements for securing PIN entry.[1]

Modern and high-end Android smartphones typically secure 'generic' PIN entry (for user authentication) through Trusted User Input (TUI) functionality as part of the device's Trusted Execution Environment (TEE). However, this functionality has not been a viable option for SoftPOS solution developers for several reasons:

1. The TUI functionality, as part of the device TEE, requires adaptations to be useful for SoftPOS solutions. However, as smartphone manufacturers restrict access to the TEE and its TUI functionality, this is not a viable option for SoftPOS solution developers.
2. The TUI functionality is platform specific, which introduces significant technical fragmentation and associated complexity for SoftPOS developers.
3. Given it is implemented within a TEE, the security of TUI depends on how secure the TEE is. TEEs are frequently subject to attacks, which can result in threat actors gaining complete access and control over the TEE. As the patching cycles for TEEs are typically long, often spanning multiple months, this would result in an unacceptably long time frame in which the solutions would be vulnerable.

Secure PIN secures PIN entry for SoftPOS solutions. This security is independent of the underlying COTS platform, meaning PIN data will remain secure even when the Android platform:

- Is offline
- Is outdated or not receiving security patches
- Is not Google GMS (Google Mobile Service) certified, such as in the case of Android AOSP

Some of the main requirements fulfilled by Secure PIN are:

- PIN digits and PIN encryption keys are never revealed in clear text
- PIN entry is aborted in the case of potential threats, such as a modified application, the PIN entry pad losing focus, or the detection of a debugger
- PIN entry does not use the system's keyboard or GUI elements
- full support for advanced key management schemes including TR-31 and DUKPT

Build Versus Buy

It is possible to build capabilities for securing PIN entry in-house. While this may be an appealing option at first glance, the reality is that this requires considerable development effort and is typically too time-consuming and cost-prohibitive for most developers. The main reason to avoid building it yourself is that creating a secure solution requires ongoing expertise in several areas:

1. cryptographic design and protection of cryptographic keys
2. advanced attack techniques being employed against mobile applications and platforms
3. Android platform security and mobile application security capabilities
4. regulatory compliance standards
5. resources to be and stay current on evolving threats and protection capabilities indefinitely

MPoC COTS-Native PIN Entry Compliance

The MPOC standard defines security requirements, test requirements, and guidance for entities involved in the development, deployment, and operation of merchant-operated mobile payment acceptance solutions that allow the entry of cardholder PINs on COTS devices.

The table below demonstrates how Zimperium's solution measures up to these requirements.

Security Requirements	Is Zimperium Compliant?
1A-4.2 All cryptographic processes, including *hash* functions, used to provide security to the solution must adhere to *Appendix C Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.*	Yes
1A-4.4 Each key must have a single unique purpose, and no keys may be used for multiple purposes.	Yes[2]
1A-5.5 Cryptographic keys must be established using a process that ensures the entropy and confidentiality of the key.	Yes[3]
1A-5.6 The *MPoC Software* must support the use of HSMs for storage and operation of secret and private cryptographic keys in the back-end *environments*.	Yes
1E-1.1 Information must exist that describes the secure capture and processing of the cardholder PIN.	Yes
1E-1.2 The *MPoC SDK* must not leak complete or partial PIN digits. The *MPoC SDK* must protect against side channels that use sensors present in the *COTS device* (e.g., accelerometers and gyroscopes) and screen capture.	Yes[4]
1E-1.3 The *MPoC SDK* must not provide feedback to the user (e.g., visually, auditory) that can be used to identify individual PIN digits.	Yes
1E-1.4 The PIN must be encrypted into an ISO format 4-PIN block as soon as it is captured.	Yes[5]
1E-1.5 *Attestation* functions detecting indications of potential compromise must be executed prior to each PIN entry process.	Yes
1E-1.6 The *MPoC SDK* must detect when another application overlays the *MPoC SDK* during PIN capture. In case of positive detection, the *MPoC SDK* must cancel any transaction in progress.	Yes
1E-1.7 PIN-related data (PIN, PIN related values such as touch locations, PIN block, PIN key) must not be stored on the *COTS device*-persistent storage and must be erased once no longer required.	Yes[6]
1E-1.8 Offline PIN verification is supported only through the use of an *SCRP*.	Not Applicable[7]
1E-1.9 PIN entry is not supported for non chip-based transactions.	Integrator Responsibility[8]

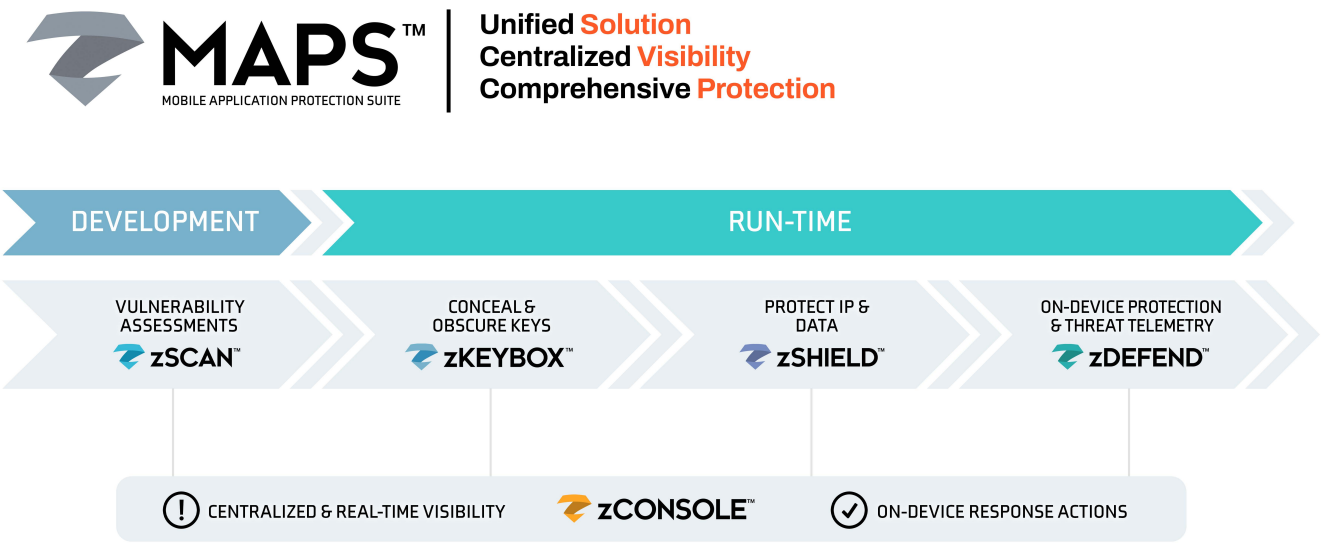
Why Zimperium's Mobile Application Protection Suite (MAPS)?

With security being a key aspect of SoftPOS solutions and PCI MPoC certification, it's important to use proven mobile application security tools from solutions providers that are committed to the space. Zimperium's Mobile Application Protection Suite (MAPS), enables mobile payment solution developers worldwide to quickly and efficiently develop secure and compliant mobile applications.

MAPS offers comprehensive capabilities, addressing all the security needs of a mobile application developer. MAPS enables SoftPOS developers to meet PCI MPoC requirements. This suite features these leading mobile application security solutions:

- **zScan:** With this solution, you can scan your app binary for security, privacy, and regulatory vulnerabilities that can be exploited by an attacker.
- **zKeyBox**: zKeyBox offers state-of-the-art, white-box cryptography that protects your encryption keys and secrets, while obscuring cryptographic algorithms so an app's execution logic is not visible to attackers, even if they gain control over the device. **Secure PIN** is a key capability within the zKeyBox solution. Throughout the PIN entry and encryption process, the PIN encryption key, the PIN, and individual PIN digits are always protected and never appear in the clear in device memory.
- **zShield:** This solution offers advanced protection for an app's source code, intellectual property (IP), and data. zShield safeguards code from a range of potential attacks, including reverse engineering and code tampering.
- **zDefend:** zDefend is a machine learning-based device attestation tool. The tool offers runtime awareness through RASP. It delivers a vast amount of telemetry and analytics from the on-device machine learning engine to address PCI MPoC monitoring and attestation needs. zDefend protects against zero-day attacks and can be updated over the air, without requiring the app itself to be rebuilt or redistributed.

While the large-scale global adoption of contactless SoftPOS is just around the corner, Zimperium has actively worked with SoftPOS developers for several years. Since 2017, we've helped dozens of SoftPOS developers achieve their security certification with payment brands and PCI.



About Zimperium

Zimperium is a global leader in mobile device and app security. The Zimperium Mobile Application Protection Suite (MAPS) helps mobile application developers build secure and robust mobile apps resistant to expert attacks. These tools are widely used in the financial industry to secure mobile banking, mobile payment, and SoftPOS applications.

MAPS is the only unified platform that combines comprehensive in-app protection with centralized threat visibility. The platform provides app shielding, cryptographic key protection, binary app scanning, and runtime protection and attestation capabilities.

To learn more, please contact us: https://www.zimperium.com/contact-us/

Sources

1. Zimperium Inc. is a Participating Organization within PCI and active participant in the Mobile Task Force which is tasked with defining the MPoC standard
2. Deriving a PIN encryption key is the responsibility of the application integrating Secure PIN. The DUKPT component of the zKeyBox is a suitable option and, if used correctly, will satisfy this requirement.
3. The Secure PIN component does not establish (by generating or key agreement) any keys. The only key it uses, gets passed to it from the incorporating application in a protected white-box format.
4. Secure PIN offers protection against side channels through COTS sensors such as accelerometers and gyroscopes by moving the PIN pad around after every key press to randomize locations where on the screen each button appears. Screen capturing is prevented while PIN entry is active.
5. The Secure PIN component encrypts the PIN to the "Intermediate Block A" format. Combining that with the PAN data to obtain the full ISO format 4 block is the responsibility of the integrating application.
6. Secure PIN assures that PIN-related data is never present in the clear in device memory and removed directly when no longer required. The integrating application is responsible for discarding the protected PIN encryption key and deleting the PIN block when no longer needed.
7. Secure PIN does not provide PIN verification functionality. It's the integrator's responsibility to assure the SCRP is used for offline PIN verification.
8. Secure PIN is not aware of the type of transaction that is being performed. It's the integrator's responsibility to prevent PIN entry for non chip-based transactions.

ZIMPERIUM®

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

Zimperium, Inc
4055 Valley View, Dallas, TX 75244