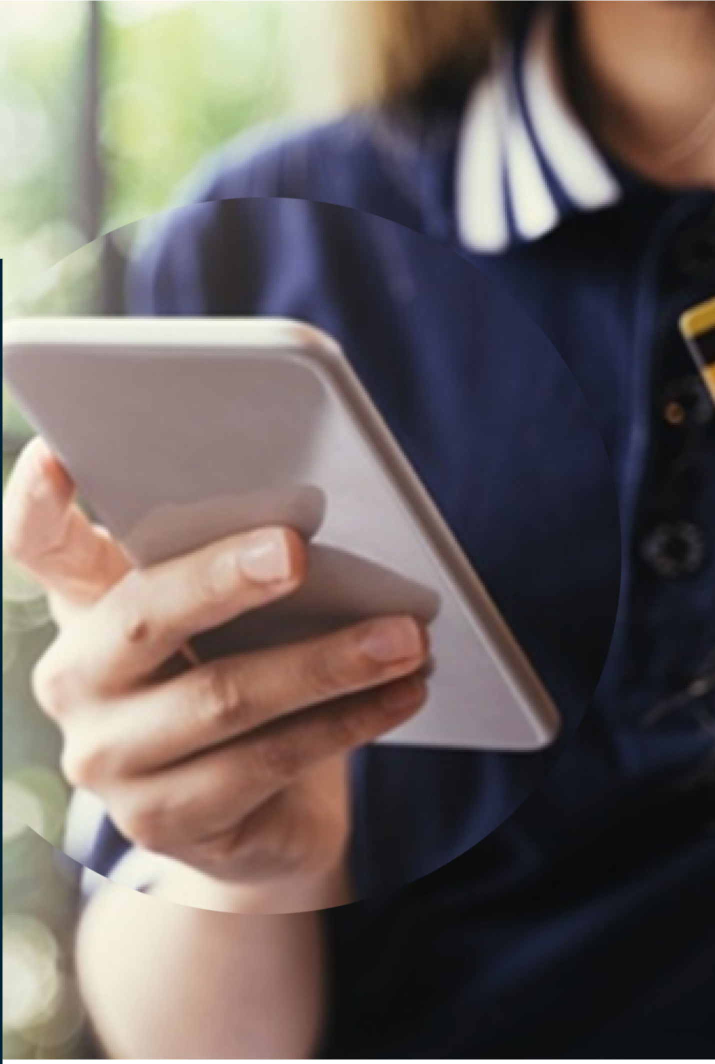
TRUSTONIC



# CPoC + PIN: achieving certification

The PCI's CPoC + PIN standard is anticipated in 2021. See how the key to achieving certification is in harnessing the combined power of the TEE and trusted user interface (TUI).

## What is CPoC + PIN?

The Payment Card Industry (PCI) Security Standards Council – the body that defines standards governing payment card security will – soon issue a new standard called CPoC™ + PIN. CPoC + PIN will revolutionize card payments by enabling PIN entry on smart mobile devices to allow higher value transactions. By offering a secure, integrated experience on a smartphone, this removes the need for expensive, specialist hardware such as card readers and traditional Point of Sale (POS) terminals.

CPoC + PIN is another step in the CPoC journey. In December 2019, the PCI issued the standard for Contactless Payments on COTS, called CPoC™. This 'tap-and-go' payment solution allows merchants to use commercial off-the-shelf devices (COTS) to accept payments from contactless cards, without the need for a separate device. Currently, CPoC can be used only for contactless payments – not PIN entry – meaning transactions must be for less than the contactless limit. With CPoC + PIN, payments above the contactless limit requiring a PIN will soon be possible using only the merchant's smartphone.

The challenge, however, is how you design a secure, future-proof solution that isolates and protects a user's PIN separately from their account details, on the same device?

## The main PCI concepts and standards

The main PCI standards include CPoC and SPoC, and a major concept is "PIN on Glass"

### PIN on Glass

PIN on Glass solutions enable merchants to accept card payments using a device such as a smartphone or tablet. The cardholder's PIN is entered on a 'glass-based capture mechanism' such as the touchscreen on a smartphone or tablet. There are 2 main types:

1. Hardware-based PIN entry and protection on point of interac tion (POI) devices built on a mobile device with hard ware-protected touch screens.

2. Software-based PIN entry and protection, on devices without hardware-protected touch screens, but with software mitigations.

### SPoC

With Software PIN on Commercial off-the-shelf devices (SPoC), PIN entry has moved from the card reader into the smartphone, although a card reader is still required. Security is based upon using separate encryption keys: card data is encrypted with one key on the card reader, while the PIN is encrypted with another key on the smartphone. Provided these keys remain separate and are stored securely, and the data is encrypted with different keys, the solution is secure.

### CPoC

CPoC is Contactless Payments on COTS (commercial off-the-shelf devices). "Regular" CPoC replaces the card reader with a mobile app – but can only be used in situations where a PIN is not required. Security is based upon the CPoC app running on the smartphone being protected, and security measures provided by the backend system.

## Designing a CPoC + PIN solution

Given the security challenges and complexities involved in protecting a user's PIN, achieving the CPoC + PIN standard will be no easy feat.
Fortunately, there's a solution: the TEE and the TUI.

The Trusted Execution Environment (TEE) is a secure operating system (OS) that runs alongside the main device OS environment such as Android. Think of the TEE as a secure vault which isolates critical code and data in a safe, hardware-isolated world, protecting it from attackers. The TEE minimizes the attack surface, preventing threats such as reverse-engineering, tampering, malware, and trojans.

Only Trusted Applications (TAs) can run in the TEE. TAs are typically the security-sensitive parts of an app, such as user authentication code or transaction signing code. TAs run in the safe environment of the TEE, rather than in Android where they are vulnerable.

TEEs are commonplace in Android devices; in some they include a Trusted User Interface (TUI). The TUI provides direct access from the TEE to the display and touchscreen, enabling the user interactions on a device's touchscreen, such as PIN entry, to be secured.

On devices with a hardware-backed TEE and hardware TUI, payment acceptance can be completely isolated from Android. Malware in the Android OS cannot capture the screen, simulate a key press, or spy on what's happening.
For devices without a hardware-backed TEE and hardware TUI, Trustonic has created a software version of both technologies, using advanced white-box cryptography and code protection measures.

## Conclusion

The TEE and TUI is the ideal environment for processing PIN entry. By combining the power of the TEE with a TUI, you can isolate and protect a user's PIN separately from their account details, on the same device. These technologies are, therefore, the key to achieving certification against the PCI's stringent CPoC + PIN standard. But how do you do this when you have no little or no control over the capabilities of the end device?

Trustonic's Application Security enables mobile app developers to implement TEE and TUI technology easily within apps.  Application Security adapts to provide the highest level of security on end user devices. On most Android smartphones, this is the hardware-backed TEE. On iOS and Android devices without this, a software TEE is used. Application Security also includes a TUI for protecting security-sensitive human interactions such as PIN entry. With its Layout Manager feature, TUI user interfaces can be created quickly and easily. And, with military-grade security at its core, Application Security will enable you achieve certification against the new CPoC + PIN standard.

For more info visit trustonic.com or email: info@trustonic.com