MineSec

PCI MPoC Standard -

All the Key Highlights

Whitepaper 2023

Table of Contents

Mobile payments has transformed the way we live. In a study conducted by Visa[1], 41% of consumers said have fully shifted, or are planning to shift to using only digital payments within the next two years. So it makes sense that what comes next is for the merchant to accept payments with their mobile phones, on the go, removing the need for dedicated POS hardware. According to Juniper Research[2], the total number of merchants deploying SoftPOS solutions will surpass 34.5 million globally by 2027; rising from 6 million in 2022.

To ensure the security of card payment transactions on the Commercial-Off-The-Shelf (COTS) devices or mobile phones, the Payment Card Industry Security Standards Council (PCI SSC) has released the Contactless-Payment-on-COTS (PCI CPoC) standard in December 2019. However, there are some limitations to the PCI CPoC standard.

Why did the PCI CPoC requirements need improvements?

First, the PCI CPoC standard does not provide requirements for a PIN solution. The requirements are defined by individual payment schemes in its SoftPOS solution with PIN pilot programs instead. If the SoftPOS solution is to be deployed in markets that do not require PIN, PCI CPoC would suffice. However, if the market requires PIN in the SoftPOS solution, the SoftPOS developer will have to develop a new application that complies with the various payment scheme-specific TTP/TOP certifications.

Second, the PCI CPoC standard is only applicable for a solution that supports online transactions which limits the use case scenarios (e.g. it will not be possible to accept payments on commercial air flights where an online connection may be limited).

Third, the PCI CPoC standard does not outline the objective of the requirements, but only the security control that needs to be implemented for compliance. This approach makes it difficult for both SoftPOS solution developers and security laboratories to evaluate whether an alternative security control can sufficiently fulfil the requirement.

Fourth, the PCI CPoC standard does not support the certification of modular solutions. This means that only a complete SoftPOS solution – comprising the payment application, attestation and monitoring server, and the payment backend, can be certified. However, the ecosystem may require multiple component providers to make up the full SoftPOS solution. Having a modular approach to certification would allow SoftPOS solution development to use already certified components to achieve greater cost effectiveness and quicker time-to-market.

[1] Visa Back to Business Global Study - 2022 Small Business Outlook.
[2] Sam Smith. Soft POS user base to grow 475% globally by 2027, as Apple's entry catalyses the market. Juniper Research, 9th August 2022

How does the new PCI MPoC standard solve these needs?

The PCI Mobile Payments on COTS (PCI MPoC) standard eliminates the above-mentioned limits.

First, the PCI MPoC standard allows mobile payment solutions to support multiple payment-acceptance channels and cardholder verification methods**.**

COTS-native contactless interface, COTS-native PIN entry, PCI PIN Transaction Security (PTS) Point of Interaction (POI) Secure Card Reader for PIN (SCRP) devices for contact and contactless, and approved Magnetic Strip Reader (MSR) devices are all supported as payment acceptance channels.

Manually entered account data, COTS-native PIN entry, No CVM and CDCVM are supported as cardholder verification methods. This means that PCI MPoC can now support PIN solutions. In fact, PCI MPoC goes beyond the SoftPOS requirements and has consolidated the market needs of all software-only solutions, as well as Software PIN on COTS (SPoC) with hardware components.

In contrast with the PCI CPoC specification, PCI MPoC allows for offline transactions which further expands the transaction use cases.

Next to this, the requirements in the PCI MPoC standard have adopted the objective-based approach**.** This change provides more flexibility for the SoftPOS solution developers in implementing security control – including any type of policy, procedure, or method to protect security-sensitive assets. Based on the objective outlined by the PCI MPoC standard, the PSP and SoftPOS developer can assess the risk to individual assets and then choose the most appropriate security controls to put in place.

Lastly, the PCI MPoC standard has outlined different types of MPoC products that can be certified by this standard. Depending on the SDK type and the implementation of the application, the applicable domain and evaluation scope will be defined. This support of modular solution allows PSP to optimise their certification strategy by leveraging previously certified modules and having the flexibility to choose which security laboratory to work with.

A MPoC solution may involve up to three types of Entities – an MPoC Solution provider, an MPoC Software developer, and an MPoC Attestation and Monitoring (A&M) service provider.

What are the MPoC solution types and MPoC security requirement domains?

The PCI MPoC standard defines three kinds of products which can be certified under the program. The derived applicable security requirements and domains depend on the

configuration of the MPoC product which is evaluated by the security laboratory. The two tables below provide the definitions of the acceptable solution types and the security domains.

MPoC Solution	A set of components and processes that supports mobile payment acceptance and protection of account data on a COTS device. At a minimum, the solution includes the MPoC Application, attestation system, and the backend systems and environments that perform attestation, monitoring, and payment processing.
MPoC Software	All software that implements the base functionality required by the MPoC Solution, including the functionality for accepting account data (optionally including the cardholder PIN) on COTS devices. The MPoC Software must implement at least one form of COTS-native account data entry, either COTS-native NFC or COTS-native PIN entry. The MPoC Software scope also includes the attestation components, backend functionality, and any APIs offered. The backend may also include the payment processing environment and functionality, but that is optional. A provider of an MPoC SDK and A&M solution will be categorised as MPoC Software.
Attestation and Monitoring Services	The operation of the attestation and monitoring functionality of a listed MPoC Software Product.

Table 1: MPoC solution types and definitions.

PCI MPoC requirements are divided into 5 domains. The first two domains cover the technical and development aspects of the MPoC product's software (the MPoC Software, or equivalent functionality in as implemented in a monolithic MPoC Solution (Domain 1)), and the MPoC Application (Domain 2).

The last three domains cover the operational aspects of the MPoC Software, Attestation and Monitoring Service, and MPoC Solution.

Domain 1	**MPoC Software Core Requirements.** The security requirements in this domain apply to the individual components and processes that make up the MPoC software (including the SDK and A&M software) or the equivalent areas of software provided by a complete MPoC solution.

Domain 2	**MPoC Application and MPoC SDK Integration.** The security requirements in this domain apply to MPoC applications that integrate, or interface to, a listed MPoC SDK or are developed as part of a monolithic solution. **Domain 2a: Secure MPoC SDK Software Integration.** This module covers the integration of a listed MPoC SDK into an MPoC application**.** **Domain 2b: MPoC Application Security.** This module covers all security mechanisms required of MPoC applications that share memory with, or have access to the memory of, the MPoC SDK they are integrating.
Domain 3	**Attestation and Monitoring (A&M) Service.** These requirements cover the operational aspects of the A&M system. If an A&M service provider wants to have its A&M service listed independently from an MPoC solution, the A&M service provider is responsible for ensuring that the requirements in this domain are met. When an MPoC solution provider is not using an A&M service provider, the MPoC solution provider is responsible for ensuring that the requirements in this domain are met.
Domain 4	**Software and Key Management.** The security requirements and test requirements in this domain cover the operational management of the software and key management aspects of the MPoC software. Domain 4 must be implemented by at least one entity in the MPoC solution, and there may be multiple entities who are required to comply with these requirements. For example, a monolithic MPoC solution would require the MPoC solution provider to be solely responsible for meeting the requirements of this domain. Alternatively, an MPoC solution may implement a separately listed A&M service provider that has been separately assessed to meet the requirements of this domain.
Domain 5	**MPoC Solution.** The security requirements and test requirements in this domain cover the operational management of the complete MPoC solution. This includes the validation of compliance for the payment processing environment, the PIN-processing environment, the MPoC attestation and monitoring environment, and any other applicable systems such as the split kernel (if applicable).

Table 2: MPoC requirement domain types and definitions.

There are 3 types of MPoC Applications:

- Monolithic MPoC Application that does not integrate any other listed MPoC products, including the MPoC SDK – All relevant Domain 1 requirements and Domain 2b of the PCI MPoC standard will be assessed.

- MPoC Application that integrates **non-Isolating** MPoC SDK (SDK that **IS NOT** validated to provide memory and cleartext asset isolation) – All requirements of Domain 2 will be assessed.
- MPoC Application that integrates **Isolating** MPoC SDK (SDK that **IS** validated to provide memory and cleartext asset isolation) – Only Domain 2a is applicable.

Additionally, if the MPoC application is certified and a PSP uses and integrates it in its merchant application using APIs exposed by the MPoC application via App-to-App (Deeplink) call, then the MPoC assessment of this merchant application is not in scope.

It is the responsibility of the MPoC solution provider to ensure that the relevant requirements for each domain are met, as well as compliance and security of the entire MPoC solution.

What is the difference between PCI MPoC, PCI CPoC and Tap-to-Phone?

First, for PCI CPoC, the entity only needs to show that their security implementation follows the requirements and that documentation for risk-management practice is in place. With the objective-based approach in PCI MPoC the developer must demonstrate how the implemented controls in the software are supported by the results of its risk-identification and risk-management practices.

Because of this new approach, the software security protections of the overall solution must reach a minimum level of robustness. The PCI MPoC standard specified an attack-costing framework to assess if a solution is robust enough at the time of the evaluation. The standard defines the robustness minimum threshold of 25 points to achieve certification. The calculation of the points is a factor of core knowledge available, the complexity of tools used and potential scalability to identify and exploit an attack to break the robustness of a solution.

Second, PCI CPoC and Tap-to-Phone require the entity to provide Secure Software Development with security requirements and guidance. PCI MPoC now requires the entity to comply with the Secure Software Life-Cycle (SLC) requirements. This can be done by undergoing evaluation as set in the new PCI MPoC standard, or submitting a Secure SLC Report Of Compliance and Attestation Of Compliance issued by an accredited Secure SLC assessor.

Third, annual penetration testing is required for SoftPOS solution under both PCI CPoC and Tap to Phone. Under the PCI MPoC program, the penetration testing requirement goes further in terms of depth of testing. There is also an added requirement to check the interfaces between the MPoC Application or MPoC SDK, and backend environments.

How do we work with PCI MPoC requirements?

MineSec designed our solutions to be in line with the new PCI MPoC modular and security approaches.

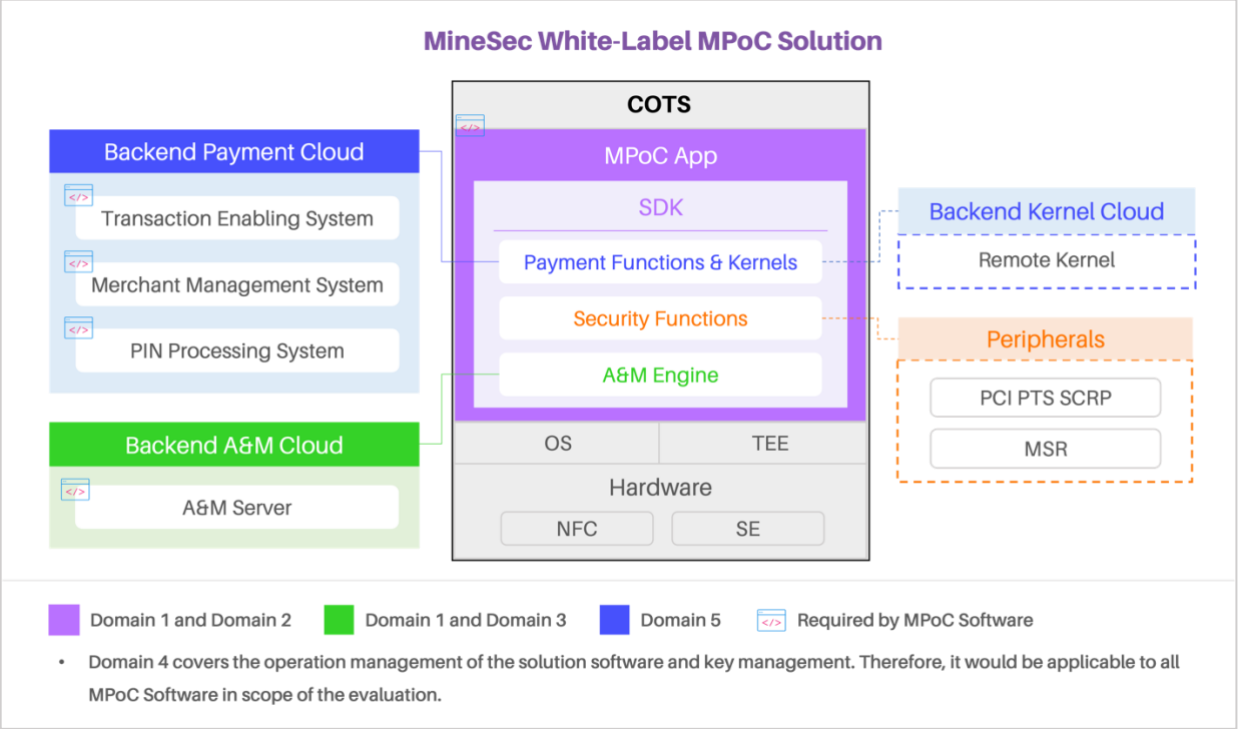
The modular design of the MineSec SoftPOS solution provides PSPs and integrators flexibility to use either our SoftPOS Technology or our White-Label SoftPOS Solution.

1. MineSec White-Label SoftPOS Technology: This comprises an SDK that integrates all the payment kernels and necessary security protection, and is connected to the AM server.
    - In this scenario, the developer of the MPoC application integrates a certified SDK.
    - The payment processing gateway connects to the A&M server. So the payment processor is the party responsible for Cardholder Data Environment (CDE) management to be PCI DSS certified and, if applicable, certified for PIN management.
    - MPoC solution integrators will be required to put their completed MPoC solution through a composite evaluation to achieve certification.
2. MineSec White-Label SoftPOS Solution: MineSec offers a total solution that includes the merchant payment application and the backend system which has a transaction-enabling platform that connects to the customer payment host, an A&M server, an operation platform for the payment service provider to manage the merchants, and a merchant platform for the merchants to access their transaction information.
    - In this solution, MineSec provides a certified MPoC application.
    - The transaction-enabling platform connects directly to the PSP payment host or gateway and is PCI DSS certified.
    - The MineSec A&M server is fully certified and integrated with the MineSec CDE.

MineSec white-label SoftPOS solution integrates all required security mechanisms and layers of protection in the SDK, payment application and A&M server to meet the robustness requirements of the PCI MPoC standard.

MineSec implements security management practices and control measures to identify and mitigate security risks. The SoftPOS solution developers leverage these management processes, and MineSec's integration and security guidelines in their solutions to fully meet the requirements of the PCI MPoC standard.

The PCI MPoC security requirements are divided into five domains and this is how it applies to the MineSec white-label solution:



PCI MPoC requires the interface between each component to be secured with a secure channel and mutual authentication.

If the kernel supports offline payment transactions which are now allowed in MPoC, then a dedicated requirement applies also to the A&M server and the attestation mechanism must support offline attestation.

The entity that provides the CDE and PIN function is responsible for PCI DSS and PIN certifications.

Summary of impact to MineSec customers

MineSec provides a modular approach to MPoC SoftPOS products. As a customer, you will have ample flexibility with MineSec to deploy a SoftPOS service best suited to your business priorities and technology capabilities.

You can come and work with us on the solution that meets your needs. Depending on the product you use, MineSec MPoC SoftPOS Solution or Software, MineSec will support you on the MPoC certification impact.

GLOSSARY – Technical Terms

Application Programming Interface (API) – A set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service.

App-to-App (Deeplink) - A type of link that send users directly to an app instead of a website or a store. They are used to send users straight to specific in-app locations, saving users the time and energy locating a particular page themselves – significantly improving the user experience.

Consumer Device Cardholder Verification Method (CDCVM) - Where a Cardholder validates the Contactless Transaction on their Mobile Device by using a passcode, pattern or Biometric ID.

Cardholder Data Environment (CDE) - The system, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

Commercial Off-the-Shelf (COTS) - A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public.

Cardholder Verification Method (CVM) - Used to evaluate whether the person presenting a payment instrument, such as a payment card, is the legitimate cardholder.

Magnetic Strip Reader (MSR) - A magnetic stripe reader, also called a magstripe reader, is a hardware device that reads the information encoded in the magnetic stripe located on the back of a plastic card.

Near-field Communication (NFC) - A short-range wireless technology that allows your phone to act as a transit pass or credit card, quickly transfer data, or instantly pair with Bluetooth devices like headphones and speakers.

PCI Contactless Payment on COTS (CPoC) – The standard released by the Payment Card Industry Security Standards Council (PCI SSC) to address mobile contactless acceptance. It provides security and test requirements for solutions that enable contactless payment acceptance on a merchant COTS device using an embedded NFC reader.

PCI Mobile Payment on COTS (MPoC) - A new, flexible mobile standard and program for payment solution development. It provides a modular, objective-based, security standard that supports various types of payment acceptance channels and consumer verification methods on COTS devices.

Personal Identification Number (PIN) - An identifying number allocated to an individual by a bank or other organization and used for validating electronic transactions.

Point of Sale (POS) - A POS system, or point-of-sale system, facilitates transactions in retail sales. An example of a well-known POS system would be a cash register. Modern POS systems are a combination of hardware and software that often includes a barcode scanner, card reader, cash drawer, and receipt printer.

Secure Card Reader for PIN (SCRP) - A mandatory item for a solution that is to be approved to the new PCI Software PIN on COTS standard, and differs from a 'normal' SCR in a number of ways; most obviously in that it is required to translate PINs sent to it from the COTS device.

Software Point of Sale (SoftPOS) - A software-based solution which transforms a regular smartphone – known as Commercial Off-The-Shelf (COTS) device – into a contactless payment terminal.

Software PIN on COTS (SPoC) - A use case where the customer PIN is entered into a commercial device like a phone, or tablet while the card is processed via small secure device.

Tap to Phone (TTP) / Tap on Phone (TOP) - A no additional hardware solution to enable your smartphone or tablet to accept contactless card present payments and become a Point of Sale terminal.

GLOSSARY – ROLES

Developer of MPoC Application – The developer of the MPoC Application that integrates a certified MPoC Software and/or develop a monolithic MPoC Application.

Integrators – The integrator of MPoC Application with a certified MPoC software.

MPoC Software / SoftPOS Developer – The developer of MPoC (or SoftPOS) software.

MPoC / SoftPOS Solution Provider – The provider of the overall, complete MPoC (or SoftPOS) solution.

MPoC Attestation & Monitoring (A&M) Service Provider - A company that provides the access and use of MPoC A&M server.

Payment Service Provider (PSP) – A third-party company that assists merchants to accept electronic payments by connecting them to consumers, card brand networks and financial institutions.

Security laboratory – An organisation that is recognised by PCI SSC to perform the security evaluations of MPoC Software and Solution using PCI security standards.