Payment Card Industry (PCI)

Contactless Payments on COTS (CPoC™)

Technical FAQs for use with CPoC 1.0

Version 1.4

July 2024

Document Changes

Date	Version	Description
December 2019	1.0	Initial release.
July 2020	1.1	Updated Q3 Added new FAQs Q4 – Q10.
December 2021	1.2	Added Q4 to update the “tamper-detection” definition. Added Q6-Q14 to clarify numerous cryptography related requirements. Added Q15 to clarify the expected logical and physical testing of COTS devices. Added Q16 to clarify a use-case where back-end attestation and monitoring systems are hosted in multiple environments or hosted by multiple entities. Added Q17 to clarify the onsite assessment requirements. Added Q24 to provide reporting guidance for CPoC labs evaluating a solution that supports multiple versions of COTS device operating systems. Added Q25 to describe the process to delay CPoC solution listing.
July 2022	1.3	Added Q26 to clarify the requirements for unsupported operating systems. Added Q27 to clarify the validation methods required for payment back-ends.
July 2024	1.4	Added Q18 to allow for support of MDM solutions

Table of Contents

CpoC Standard: Frequently Asked Questions

The following technical FAQs provide answers to questions regarding the application of Security Requirements and Test Requirements, as addressed in Payment Card Industry (PCI) Contactless Payments on COTS (CPoC™) Standard. These FAQs are an integral part of those requirements and must be considered fully.

Updates: New or questions modified for clarity are in red.

General Questions

Q 1 Is the CPoC Standard intended to support the deployment of CPoC Applications in attended environments?

A Yes. The security requirements are intended specifically to address risks associated with attended environments. Other implementations may render environments vulnerable to additional attacks that have not been considered in the security requirements and which may not be mitigated by the underlying controls established in the CpoC Standard.

Q 2 Is it possible for both CPoC and SPoC solution-listed applications to be available on a merchant's *COTS device*?

A Technically, the ability for solution-listed applications associated with both SPoC and CPoC to be available and run on the same merchant's COTS device is feasible. Although a merchant may have a legitimate business context for doing so, this may introduce an additional risk, such as making PIN and PAN available in the rich execution environment. To determine whether there are any compliance or business-related implications that must be considered, merchants should seek guidance from the payment brands for any specific rules related to POS terminals within the context of their use case.

Q 3 Can a CPoC solution provider compose a CPoC solution from third-party elements?

A The CPoC Standard does not prohibit using a third-party service provider or elements developed by a third-party as long as the CPoC solution in its entirety and *as a whole* solution is evaluated by the CPoC laboratory. Regardless of whether the CPoC solution, including CpoC application, has been developed in-house or by a third-party, each CPoC solution provider is ultimately responsible for ensuring that all requirements are met and continue to be met throughout the solution's lifecycle.

Security and Test Requirements

Q 4 [December 2021] What is the definition of “tamper-detection”?

A A characteristic that allows for the determination that an attempt has been made to compromise security.

Q 5 Module 5 references a contactless EMV kernel (singular) for card acceptance. If the CPoC solution involves more than one contactless EMV kernel, do all Module 5 requirements apply to each kernel?

A Yes. CPoC solutions generally include multiple contactless EMV kernels, and the Module 5 requirements apply to all kernels in the solution. Any kernels that are added to an approved solution are required to be evaluated, either a full or delta change evaluation, *as* determined by the CPoC lab, where all Module 5 security requirements and test requirements must be considered.

Q 6 [December 2021] What is an assessed or validated RNG, and what is expected from a CPoC lab when evaluating a CPoC solution?

A There are two types of RNGs: Deterministic Random Number Generator (DRNG) and Non-deterministic Random Number Generator (NRNG). Typically, DRNG uses an initial seed value from an NRNG to generate deterministic random values.

The entropy used for an NRNG must meet the requirements in *NIST SP 800-90B* or *§8 of ISO/IEC 18031 Information technology — Security techniques — Random bit generation*.

Many COTS platforms implement their own RNG functions, however not all meet the security requirements as noted in CPoC standard. The implementation of DRNG for security services must meet the following criteria:

- Implements a well-known standard, such as those specified in *NIST SP800-90a or §9 of ISO/IEC 18031 Information technology — Security techniques — Random bit generation*.
- Properly seeded (per CPoC security requirement 1.2.2), and
- Implementation is tested for fitness of purpose using industry-recognized test suites, such as NIST SP800-22 or AIS 31.

The CPoC laboratory is expected to perform a review of all sensitive services (such as source code review) to confirm that the RNG functions used by the solution are assessed RNGs, and that the RNG functions are used as intended. The CPoC lab must provide testing methodology and applicable testing evidence to justify their conclusions.

Q 7 [December 2021] Can an EMV Unpredictable Number (UN) be used for security services?

A No. An EMV UN used in contactless kernels on COTS acceptance device provides dynamic data for a contactless transaction. However, an EMV UN is not sufficient to provide a seed/entropy for RNG functions used by CPoC solution security services.

Q 8 [December 2021] Can secret or private cryptographic keys be used for multiple purposes?

A No. With exception of software-based protection mechanisms (e.g., white-box cryptography), all secret cryptographic keys and private cryptographic keys used in the solution must be unique per device, per application, and per purpose. For example, the same cryptographic key used to protect attestation messages cannot be used to encrypt account data. Nor can the same cryptographic key be used to protect attestation messages on different devices.

Keys used in the software-based protection mechanisms are required to be unique per purpose, but can be common across multiple devices and application instances.

Q 9 [December 2021] Do public keys have to be signed to be used in the CPoC solution?

A No. There are many ways to verify the authenticity of a public key, such as digital signatures, message authentication codes, and certificate pinning.

Q 10 [December 2021] Can self-signed certificates be used in the CPoC solution?

No. Self-signed certificates cannot be used for security services anywhere in the CPoC solution. While the integrity and authenticity of self-signed certificates can be verified (for example, by using a certificate pinning technique), there are a number of security challenges with their use. The only exceptions are self-signed certificates that exist as part of the base COTS platform or root Certificate Authority (CA) certificates that are part of PKI (such as, when Root CA is implemented internally).

Q 11 [December 2021] Must only secret cryptographic keys and private cryptographic keys that are used to encrypt account data be protected?

A No. All secret cryptographic keys and private cryptographic keys that are used for security services in the CPoC solution must be protected. This includes persistent storage of all secret cryptographic keys and private cryptographic keys in one of the approved forms defined in CPoC Security Requirement 1.4.4.

Q 12 [December 2021] What SCD(s) can be used to protect secret cryptographic keys and private cryptographic keys?

A Any SCD that protects cryptographic material used for security purposes (such as, cryptographic keys used to encrypt account data or cryptographic material used to sign CPoC application executables and scripts) must comply with industry-standard security requirements, such as *FIPS 140-2* Level 3 (or equivalent in *FIPS 140-3*), *Common Criteria*, or *PCI HSM*.

Q 13 [December 2021] Is an HSM the only acceptable method to store cryptographic material used in signing CPoC application executables and scripts?

A No. Secret cryptographic keys and private cryptographic keys can be stored in one of the approved forms defined in CPoC Security Requirement 1.4.4.

Q 14 [December 2021] How can a CPoC application protect cryptographic keys used to encrypt account data?

When stored, cryptographic keys used to encrypt account data must be maintained in one of the approved forms defined in CPoC Security Requirement 1.4.4.

Cryptographic keys used to encrypt the account data are expected to be accessible and useable only by the CPoC application. While it is encouraged that CPoC solutions utilize hardware-based security mechanisms, if supported by the COTS platform, it is acceptable for a CPoC application to rely on software-based cryptography.

For example, to protect cryptographic keys and processes used to encrypt account data, a solution could use software-based protection mechanisms (such as white-box) so that the cryptographic process does not expose cleartext cryptographic material in the COTS device runtime memory during the cryptographic operation.

The CPoC lab is expected to attempt to access cryptographic keys in the COTS device runtime memory during the cryptographic operations to confirm that the keys do not exist in cleartext, and/or that the attempt is detected by the attestation components.

Q 15 [December 2021] What is expected from CPoC labs regarding physical and logical testing of the COTS devices?

A While there is no expectation to perform physical or logical testing of a COTS device itself, CPoC labs must confirm whether COTS platforms included in the COTS system baseline have known characteristics, such as physical test, debug, or in-circuit emulation features. For example, some Android mobile devices have an NFC logging service, which is intended to be used for debugging purposes. Other COTS devices may produce unique responses based on the COTS platform chipset when used with Android Debug Bridge (ADB), which can be exploited when physically connected to the mobile device.

The CPoC lab is expected to have the expertise and knowledge of such features. Depending on the COTS platforms that the CPoC solution supports, the CPoC lab should use its expertise and knowledge to consider what attack methods should be performed when evaluating the solution, and how their features affect attack costing.

Q 16 [December 2021] Can back-end attestation and monitoring systems be hosted in multiple environments by more than one entity?

A Yes. For each environment that is hosting attestation and monitoring systems, the CPoC solution provider expected to do either: 1) Provide an Attestation of Compliance (AOC) that has been completed and signed within the previous 12 months demonstrating that the environment complies with the *PCI DSS*, including the additional controls outlined in *PCI DSS* Appendix A3 DESV, or; 2) Demonstrate compliance with the logical and physical security requirements defined in *CPoC Security Requirements*, Appendix A Monitoring and Attestation Environment Basic Protections.

Q 17 [December 2021] Does assessment of back-end systems require a physical onsite presence of the lab personnel?

A CPoC solution back-end environments include back-end monitoring and attestation environment, and back-end payment processing environment. The back-end payment processing environment must be compliant with PCI Data Security Standard, and whether remote assessment methods are acceptable is defined by the compliance-accepting entities.

When the back-end attestation and monitoring environment is included in scope of the PCI DSS assessment, it must comply with additional requirements outlined in *PCI DSS Appendix A3 DESV*, and whether physical onsite presence is required continues to be determined by the compliance-accepting entities.

In cases where the back-end attestation and monitoring environment is not subject to PCI DSS, it must be assessed and validated to the security requirements outlined in *CPoC Appendix A*. The requirements in *CPoC Appendix A* are intended to provide comparable security controls to *PCI DSS Appendix A3 DESV*, therefore it is expected that the PCI-recognized lab personnel are physically onsite for each assessment of the environment. While the intent is that assessments of physical environments are performed onsite, the use of remote assessment methods may be a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. PCI SSC has developed and published a framework of remote assessment methods that may be used when an onsite assessment cannot be performed. The PCI SSC Remote Assessment Guidelines and Procedures document can be found in the PCI SSC Document Library.

Q 18 [July 2024] Can a Mobile Device Management (MDM) solution be used as an 'OS-store' for the distribution of a CPoC application? Is additional testing required in such a case?

A Yes. An MDM system may be used for the distribution of a CPoC application, instead of the official OS store, if the requirements of 2.6.x of the PCI CPoC standard have been validated as part of the Solution listing.

Program Guide

Q 19 Can APIs (i.e., software libraries allowing third parties to interface with the CPoC solution) be validated and listed as part of a CPoC solution?

A Yes. In cases where the CPoC solution provider offers software libraries or APIs to allow third parties to interface to the solution, evaluation and validation by a CPoC lab is required as part of each CPoC solution in which such APIs are provided in order to validate that usage of the API can be done without violating or negatively impacting functionality or compliance with the *CPoC Standard.* Details regarding development, validation and listing of optional third-party APIs are specified throughout the *CPoC Program Guide*, particularly in Appendix D “CPoC Vendor-provided Libraries or APIs.”

Q 20 What is expected from a CPoC lab when evaluating a CPoC solution that offers APIs or software libraries to allow third-party developers to interface with the solution?

A The evaluation and validation of the APIs (together with the CPoC user guidance document described and defined in the CPoC Program Guide) by a CPoC lab are required as part of each CPoC Solution in which such libraries or APIs are provided. The CPoC lab must validate that third-party usage of the libraries or APIs cannot negatively impact the functionality, security, or compliance with the *CPoC Standard*.

The CPoC lab must evaluate the CPoC user guidance, provided by the CPoC solution provider, which describes how the APIs are used to interface the CPoC solution.

While reporting on the APIs’ validation, the CPoC lab must follow the same process used for the reporting of CPoC applications. Whereas the CPoC user guidance is produced and distributed under the responsibility of the CPoC solution provider, the CPoC lab must ensure that it contains the terms and conditions that address the secure usage of the APIs.

Q 21 Can a CPoC Lab reference an approval from another PCI SSC standard, such as PCI Software-Based PIN Entry on COTS (SPoC)™, to meet objectives in the CPoC standard without performing the required testing?

A No. With the exception of references to the PCI DSS AOC for back-end environments, each CPoC evaluation report must demonstrate that the CPoC solution under review was evaluated and meets the security and the test requirements of the *CPoC Standard*.

Q 22 Can testing results be reused from one evaluation to another of the same vendor?

A Yes. Testing from one CPoC evaluation can be reused in another CPoC evaluation from the same vendor. This situation occurs commonly when more than one CPoC solution with similar characteristics are evaluated by the same CPoC laboratory in parallel or in close succession. The reused data must be current (less than 12 months old) and must have been completed under the same major version of the *CPoC Standard*. The tester shall:

- Justify how the two solutions are similar. The tester must confirm that the differences in COTS device hardware, CPoC solution software, and configuration do not impact the testing results.
- Clearly indicate that the test includes reused data and meets the applicable test requirements.
- Provide evidence of testing, and that the testing is valid for the CPoC solution and the test requirement(s) under review.

Q 23 Can a CPoC lab rely on testing performed by a different CPoC lab without further testing or validation?

A If any element of a CPoC solution was evaluated by an entity other than the CPoC lab performing the evaluation under review, the evaluating CPoC lab must have access to all associated reports and supporting evidence. If those reports are not available for any reason, the evaluating CPoC lab must determine the additional work required to properly evaluate and attest to the solution's compliance with the CPoC security and test requirements.

If the evaluating CPoC lab is unable to rely on the information, whether available or not, and the CPoC lab is unable to perform the additional work required to achieve such reliance, PCI SSC will not accept the report.

In all cases, PCI SSC may reject the evaluation report if it does not contain adequate information to substantiate the conclusions or compliance with the *CPoC Standard*.

Q 24 What testing and reporting are expected to be performed by CPoC lab as part of an annual checkpoint?

A The annual checkpoint confirms that the CPoC solution continues to meet the security and test requirements of the *CPoC Standard*. The amount of testing that is required will vary. At a minimum, however, the CPoC lab must confirm that:

- Back-end environments remain compliant with PCI DSS or CPoC Appendix A, and,
- All operating processes (risk assessment, vulnerability management, change management, and so on) are being followed.

The CPoC lab may need to perform additional testing, depending on the extent to which the CPoC solution has changed. For example, if an operating system (OS) vendor no longer supports an OS that was included in the CPoC solution system baseline, the CPoC lab must verify that the CPoC solution provider has updated its system baseline and is actively working with its merchants to migrate them to a supported version of the OS.

Moreover, as part of the annual checkpoint, the CPoC lab must consider new risks, vulnerabilities/CVE, and attack techniques (such as new rooting or jailbreaking) and attempt to apply those techniques to ensure that CPoC solution attestation and monitoring systems are able to detect and respond to those attacks.

Each annual checkpoint submission must be made by a CPoC lab and include the submission of an updated *CPoC solution AOV* to PCI SSC after the lab reviews all changes that occurred since the last full evaluation or last annual checkpoint (whichever is more recent). The CPoC lab must also consider any applicable changes that occurred during the previous 12-month period. In addition, the CPoC lab must determine the level of testing needed to ensure that the solution remains compliant with all applicable CPoC security and test requirements. For more information, see the *CPoC Program Guide v1.0*, section 5.1 "Annual Checkpoints."

Q 25 [December 2021] Can a lab submit a single report for multiple versions of COTS device operating systems?

A Yes. Support for different major versions of COTS device operating systems (9.x, 10.x, and so on) is permitted in a single CPoC Solution Evaluation and listing on the Website. However, support for different COTS platforms (such as Android and iOS) are considered separate CPoC Solutions, and therefore require separate, full CPoC Evaluation Reports, validation, and listings on the Website.

When including multiple versions of an operating system, the CPoC lab must indicate in the report what testing was performed for each operating system.

Q 26 [December 2021] Can a CPoC Solution Listing be delayed at a vendor's request?

A Yes, solution providers may choose to delay listing a newly approved CPoC solution for up to a maximum of six calendar months. Written notification to PCI SSC must be submitted by the CPoC solution provider, through the CPoC laboratory performing the evaluation, along with the completed CPoC Evaluation Report. In addition, the CPoC lab must make a notation in the applicable field of the Lab Report Portal when submitting the evaluation report, indicating the period of time the listing should be withheld.

Delaying listing does not extend the solution's validation period; annual checkpoint and solution reevaluation dates will be based on the date of the countersigned AOV, not the date on which the solution is listed. A solution is not considered to be a validated CPoC solution until it is listed on the PCI SSC website.

Q 27 [June 2022] What is required of a CPoC Solution once an operating system is no longer supported?

A CPoC Solution Providers must start migrating merchants from platforms as soon as an operating system within the baseline is no longer supported. Plans for such migration must exist prior to the expiry of any supported OS, and may include commencement of migration prior to the deprecation of the OS.

The migration process for any operating system that is unsupported during an annual checkpoint (or full assessment) must be completed prior to the next annual assessment. Consecutive CPoC annual assessments noting inclusion of the same unsupported operating system(s) will not be accepted.

For example, if an Operating System becomes unsupported during September of one year the annual checkpoint performed in October of that year could include references to that Operating System. However, the checkpoint performed in the next year would not be accepted if it still included references to that Operating System.

Q 28 [June 2022] Is it required that the PCI DSS validation of the payment processing back-end system used in a CPoC solution is performed by a QSA?

A The method required be used to validate payment back-end systems to the PCI DSS is a function of the compliance programs managed by each of the relevant payment brands. For details on any specific case please contact the individual payment brands (see How do I contact the payment card brands?).