Payment Card Industry (PCI)

Contactless Payments on COTS (CPoC™)

Technical FAQs for use with CPoC 1.0

Version 1.1

July 2020

Document Changes

Date	Version	Description
December 2019	1.0	Initial release.
July 2020	1.1	Updated Q3 Added new FAQs Q4 – Q10.

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 [July 2020] 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 **[July 2020] 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.

Program Guide

Q 5 **[July 2020] 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 6 **[July 2020] 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 7 **[July 2020] 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 8 **[July 2020] 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 two CPoC solutions with similar characteristics are evaluated by the same 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 is 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 under review.

Q 9 **[July 2020] 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 10 **[July 2020] 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.”