Payment Card Industry (PCI)

Mobile Payments on COTS (MPoC)

Summary of Changes from Version 1.0.1 to 1.1

December 2024

Introduction

This document provides a summary of changes from the PCI MPoC requirements v1.0.1 to the version v1.1 release. Table 1 provides an overview of the types of changes included in update of the MPoC Standard to Version 1.1. Table 2 provides a summary of material changes found in the update of the MPoC Standard to Version 1.1.

Document Abbreviations Used

Abbreviation	Description
POI	A Point of Interaction device validated to the PCI PTS POI requirements.
SCRP	Secure Card Reader PIN. An approval class as defined in the PTS POI Device Testing and Approval Guide.
SDK	The subset of MPoC Software, that implements required functionality for the payment acceptance and attestation on the COTS device, and secure communication with the back-end systems.
COTS device	The platform on which an MPoC Application executes. Defined in the MPoC standard.
HSM	Hardware Security Module

Table 1: Change Types

Change Type	Definition
Clarification or guidance	Updates to wording, explanation, definition, additional guidance, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Evolving requirement	Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
Structure or format	Reorganization of content, including combining, separating, and renumbering of requirements to align content.

***Note:** The changes above do not include those that are corrections of grammar or typographical errors or other rephrasing of existing statements.*

Table 2: Summary of Changes

Requirements Reference	Change	Type
General	Changed the Attestation and Monitoring Service MPoC Product to a more generic “MPoC Service” Product.	Structure or format
General	Changed references to PCI PTS POI SCRP approval class to a more generic PCI PTS POI. Some changes to Security Requirements throughout the document to accommodate this change.	Structure or format
General	Implemented the term ‘COTS-based MPoC Software’ throughout to reference instances where there is applicability to either an MPoC SDK or an MPoC Application.	Structure or format
General	Introduced the ability for an MPoC SDK to integrate (up to one) other MPoC SDK.	Evolving requirement
General	Removed references to PCI DSS DESV. Some changes to Security Requirements throughout the document to accommodate this change.	Evolving requirement
General	Modified the definition of COTS devices, as well as aspects of the initial pre-amble of the document.	Evolving requirement
General	Updated the matrix of applicability to reflect associated changes in the MPoC standard and program.	Structure or format
General	Changed all Security Requirement wording to remove ‘must’ and instead make statements of each requirement.	Structure or format
General	Updated guidance throughout document as required.	Clarification or guidance
SR 1A-1.3	Updated wording of requirement and guidance to allow for different types of vulnerability assessments.	Evolving requirement
SR 1A-1.4	Removed the requirement for Secure Software validation of the A&M backend software. Replaced by previous requirement 1A-1.5.	Evolving requirement
SR 1A-1.5	Added new requirement to validate that the MPoC SDK does not pass sensitive assets to another MPoC SDK or MPoC Application.	Evolving requirement

Requirements Reference	Change	Type
SR 1A-1.6	Added new requirement to cover validation of situations where an MPoC SDK is integrating another MPoC SDK.	Evolving requirement
SR 1A-1.7	Added new requirement to validate that all card-based payment functionality has been included in the scope of the MPoC assessment.	Evolving requirement
SR 1A-1.8	Added new requirement to ensure that an MPoC SDK provides a mechanism to validate its version number.	Evolving requirement
SR 1A-2.3	Changed wording to clarify applicability when use of a true RNG cannot be assured.	Clarification or guidance
SR 1A-2.5	Changed wording to clarify that at least one trusted source of entropy is required from the COTS device. Updated guidance from existing MPoC FAQ.	Clarification or guidance
SR 1A-2.6	Changed wording to clarify the intent to ensure sufficient entropy. Added guidance.	Clarification or guidance
SR 1A-3.2	Added guidance noting that RSA 2048 bit may be used to load AES keys if the COTS platform prevents the use of larger RSA keys.	Evolving requirement
SR 1A-3.3	Changed wording to clarify applicability is prior to certificate being relied upon for security services.	Clarification or guidance
SR 1A-4.6	Changed wording to allow for use of some backend keys outside of a HSM. Added new test steps and guidance.	Evolving requirement
SR 1A-4.8	Added clarification regarding use of RSA2048 bit, aligned with changes to SR 1A-3.2. Additionally added guidance noting that a KEK of lesser strength may be used as long as the weakest key used provides at least 128 bits of effective strength.	Requirement Change
SRs 1A-4.9 – 1A-412	Moved these requirements to here from 1D-1.3 – 1D-1.6 in PCI MPoC v1.0.1.	Structure or format
SR 1A-4.11	Added note to clarify that keys used only once per install, such as keys used during initial provisioning, are not in scope of this requirement.	Evolving requirement

Requirements Reference	Change	Type
1A-5 Preamble	Clarified that MPoC Applications that integrate an MPoC SDK may configure or implement aspects of Secure Channels.	Evolving requirement
SR 1A-5.2 SR 1A-5.5	Changed wording requiring secure channel on connections between different logical elements.	Evolving requirement
SR 1A-5.6	Changed wording to clarify applicability to Secure Channels supported by the MPoC Software.	Evolving requirement
SR 1A-5.7	Added clarification that this requirement does not apply to platform-based attestation.	Evolving requirement
1B-1 Preamble	Clarified applicability to MPoC code executing on COTS devices, not on backend systems or code.	Clarification or guidance
SR 1B-1.4	Clarified that this requirement does not apply to areas of memory or COTS subsystems that the COTS-based MPoC Software does not have access to (such as a COTS keystore).	Clarification or guidance
SR 1B-1.5	Clarified scope to also include any sensitive assets managed by the MPoC SDK, as well as noting any features not provided must be considered in the attack costing calculation.	Evolving requirement
SR 1B-1.7	Changed wording to clarify the intent is to prevent use of compromised platforms which may impact the security of sensitive assets.	Clarification or guidance
SR 1B-1.11	Added test requirement to confirm that any parts of the COTS-based MPoC Software which are executed outside of the REE are authenticated prior to execution.	Evolving requirement
SR 1B-1.12	Added new requirement to capture testing to determine if an MPoC SDK is isolating or non-isolating.	Evolving requirement
SR 1B-1.13	Added new requirement to ensure payment transaction data is securely deleted from the COTS device once the data has been transmitted to the payment backend.	Evolving requirement
1B-2 Preamble	Added clarification that this section is not intended for backend systems.	Clarification or guidance

Requirements Reference	Change	Type
SR 1B-2.4	Changed wording to clarify this requirement applies when software protected cryptography is used for the protection of secret or private keys embedded into the COTS-based MPoC Software.	Clarification or guidance
SR 1B-2.5	Changed wording to clarify that secure key generation is only required if key generation is implemented.	Clarification or guidance
SR 1C-2.3	Changed wording to clarify intent is to ensure freshness and authenticity of A&M data.	Clarification or guidance
SR 1C-3.6	Changed wording to clarify intent is to prevent manipulation of payment cessation messages.	Clarification or guidance
SR 1C-4.2	Removed previous requirement as considered redundant with requirement 1A-5.7. Intent of requirement remains.	Structure or format
1D-1 Preamble	Added note to clarify that PAN truncated to relevant PCI DSS FAQs is not considered in scope for these requirements.	Clarification or guidance
SR 1D-1.2 SR 1D-1.3	Split 1D-1.2 into two requirements. Added guidance on how a PCI PTS POI that is not an SCRP device may be validated to ensure all account data is encrypted.	Evolving requirement
SRs 1D-1.3 – 1D-1.6	Moved the requirements in PCI MPoC v1.0.1 to Section 1A-4.x in the updated document as previously noted.	Structure or format
SR 1D-1.5	Added guidance to clarify that some PCI PTS POI devices may output cleartext account data, and the MPoC Software should be able to detect and respond if this occurs.	Clarification or guidance
SR 1D-1.6	Clarified that deletion of account data is required only after completion of current transaction process.	Clarification or guidance
SR 1D-2.1	Changed wording to clarify that the security guidance document must include details on all external readers supported by the MPoC Software.	Evolving requirement
SR 1D-2.2	Changed wording in test step to clarify that the POI devices supported must be validated to support chip acceptance if they are used for chip acceptance.	Evolving requirement
SR 1D-2.3	Changed wording to support PCI PTS POI devices that are not an SCRP. Includes new test item to validate that the data output from the PCI PTS POI device is encrypted.	Evolving requirement

Requirements Reference	Change	Type
SR 1D-2.4	Removed requirement for use of enablement tokens.	Evolving requirement
SR 1D-2.4	Added new requirement for use of whitelisting from an external POI device.	Evolving requirement
SR 1D-3.1	Changed wording to clarify that the security guidance document must include details on all external readers supported by the MPoC Software.	Clarification or guidance
SR 1D-3.3	Clarified that the validation of attached MSR devices includes the firmware and hardware versions only where these values are applicable.	Clarification or guidance
SR 1D-4.3	Clarified that this requirement applies only when presentment of the card may be captured on the COTS camera.	Clarification or guidance
SR 1D-4.4	Removed requirement for validation of contactless kernel functional approval.	Evolving requirement
SR 1D-4.4	Renumbered requirement from 1D-4.5 in PCI MPoC v1.0.1. Changed wording to clarify scope includes validation of relevant sections of Domain 4 and Domain 5.	Structure or format
1D-5 Preamble	Added note to clarify that PAN truncated to relevant PCI DSS FAQs is not considered in scope for these requirements.	Clarification or guidance
SR 1D-5.4	Changed wording to clarify intent is when there is an event that potentially impacts the security of the manual entry process.	Clarification or guidance
1E Preamble	Added clarification items regarding use of external POIs for PIN entry, and implementation of accessibility features during PIN entry.	Clarification or guidance
SR 1E-1.1	Added test step to confirm that any accessible PIN entry features are documented.	Evolving requirement
SR 1E-1.3	Added clarification in guidance that use of a scrambled keypad is not necessary (but may assist in meeting the requirement).	Clarification or guidance
SR 1E-1.4	Added test step to confirm that if an external keypad is used for PIN entry, it is part of a validated PCI PTS POI device.	Evolving requirement

Requirements Reference	Change	Type
SR 1E-1.5	Changed wording to clarify the intent that the PIN is encrypted into a format 4 PIN block prior to export from the COTS device.	Clarification or guidance
SR 1E-1.5	Added guidance to note that PCI PTS POI devices which are not part of the SCRP approval class may not be used for PIN translation functions.	Clarification or guidance
SR 1E-1.7	Changed wording to clarify intent is when there is an event that potentially impacts the security of the PIN entry process and that potential overlay attacks must be communicated to the back-end A&M system.	Clarification or guidance
SR 1E-1.9	Changed wording to allow for support of PCI PTS POI devices that are not an SCRP, and to clarify that the device must be validated as supporting offline PIN entry.	Evolving requirement
SR 1E-1.10	Added new requirement for testing accessible PIN entry functions.	Evolving requirement
SR 1E-1.11	Added new requirement for testing PIN entry implemented through an attached PCI PTS POI.	Evolving requirement
SR 1E-1.12	Added new requirement for testing PAN tokens, where implemented.	Evolving requirement
SR 1F-1.2 SR 1F-1.3	Removed requirements.	Structure or format
SR 1F-1.3	Added guidance to clarify that this requirement does not prohibit the transmission of encrypted offline transaction data through other 'calling' applications.	Clarification or guidance
SR 1F-1.3 SR 1F-2.3	Added guidance to clarify the scope and interpretation of these requirements.	Clarification or guidance
Module 1G	Changed title to "MPoC Software Security Guidance and Integration" to accommodate for new requirement allowing for vendor SDK testing. Added guidance to note that different levels of guidance may be provided to different entities in an overall MPoC Solution.	Structure or format
SR 1G-1.1	Changed wording to require that the security guidance document is available to potential integrators and assessment laboratories.	Evolving requirement

Requirements Reference	Change	Type
SR 1G-1.7	Changed requirement wording to confirm guidance is sufficient for secure integration of an MPoC SDK into other COTS-based MPoC Software.	Evolving requirement
SR 1G-1.8	Added new requirement to cover validation of guidance for implementations where the MPoC SDK allows for the other COTS-based MPoC Software to manage or implement secure channels.	Evolving requirement
SR 1G-1.9	Changed wording to include external readers into scope.	Evolving requirement
SR 1G-1.12	New requirement to allow for MPoC Software vendors to perform vendor verification of other COTS-based MPoC Software that integrate their the isolating SDK(s) of the MPoC SDK vendor.	Evolving requirement
Module 2A Preamble	Added guidance to clarify scope of this module.	Clarification or guidance
SR 2A-1.3	Changed wording to clarify that all card-based payment functions must be provided by the MPoC SDK(s).	Clarification or guidance
SR 2A-1.11	Added requirement to cover testing of COTS-based MPoC Software that implements or manages its own secure channels.	Evolving requirement
Section 3B-1	Moved the majority of these requirements in PCI MPoC v1.0.1 from this module to Domain 4.	Structure or format
SR 3B-1.4	Requirement moved from Section 3B-1 in PCI MPoC v1.0.1, which was moved as noted above.	Structure or format
SR 3D-1.1	Removed requirement for PCI DSS DESV validation. Requirement for validation to PCI DSS remains as requirement 4A-4.1.	Evolving requirement
SR 3C-1.1	Changed wording to clarify applicability.	Clarification or guidance
SR 4A-1.5	Changed wording to clarify that the distribution method may be relied upon to provided authenticity to the MPoC Application.	Evolving requirement

Requirements Reference	Change	Type
SR 4A-2.2	Changed wording to algin with changed requirement 1A-4.6, and to clarify that PIN related cryptographic keys must never appear outside a HSM in cleartext, and to allow for use FIPS140-2/3 Level 2 HSMs if used in a Controlled Environment (as per the definition in ISO13491).	Evolving requirement
4A-3 Title and Objective	Changed to reflect new items moved from Domain 3.	Structure or format
SR 4A-3.3 – 4A-3.4	Requirements moved from Section 3B in v1.0.1.	Structure or format
Section 4A-4	Requirements moved from Domain 5 in v1.0.1.	Structure or format
SR 5A-1.3	Added clarification that this requirement may apply to entities managing merchant systems on behalf of merchants.	Evolving requirement
Appendix B ‘Scalability’	Fixed errata showing ‘instance specific’ as 18 points instead of the correct value of 12 points	Structure or format