Payment Card Industry (PCI)
Mobile Payments on COTS (MPoC)™

Technical FAQs for use with MPoC v1.0.x

Version 1.5 - November 2024

Document Changes

Date	Version	Description
March 2023	1.0	Initial release.
May 2023	1.1	Add general FAQs 4, 5, 6, 7, 8 Add 1A FAQs 3, 4, 5 Add 1C FAQ 1 Add 1F FAQ 1 Add 2A & 2B FAQ 1
August 2023	1.2	Add general FAQs 9, 10 Add 1A FAQs 6, 7
November 2023	1.3	Add general FAQs 11, 12, 13 Add 1A FAQs 8, 9 Add 1D FAQ 1 Add 2A & 2B FAQ 2 Add 3D FAQ 2 Add 5A FAQ 1
March 2024	1.4	Add general FAQs 14, 15, 16 Add 1A FAQs 10, 11 Add 1C FAQ 2 Add 1E FAQs 2, 3 Add 2A & 2B FAQ 3
November 2024	1.5	Update to align some items with MPoC v1.1 Updated title to clarify applicability to MPoC v1.0 and MPoC v1.0.1 only Delete 1A FAQs 1, 2. Update 1A FAQ 3, 6. Add 1A FAQ 12 Add 1C FAQ 3 Delete 1D FAQ 1. Add 1D FAQ 2 Delete 3D FAQ 2. Update 3D FAQ 1 Add 4A FAQ 1

Table of Contents

© 2022-2024 PCI Security Standards Council, LLC. All rights reserved.

MPoC Security Requirements: Frequently Asked Questions

These technical FAQs provide answers to questions about applying Payment Card Industry (PCI) Mobile Payments on COTS™ (MPoC™) security requirements and corresponding testing requirements as addressed in the *PCI Mobile Payments on COTS Security Requirements and Test Requirements*. These FAQs clarify the intent and assessment of the *Security Requirements and Test Requirements*. The FAQs are an integral part of those requirements and must be fully considered.

Updates: Questions newly added or modified after the initial release of this Technical FAQ document (version 1.0), are highlighted in red for clarity.

General Questions

Q 1 Are A&M Service Providers in scope of the requirements of Domain 4?

A Yes. Domain 4 applies to all and any entities which may implement the aspects covered in that domain. This includes A&M Service Providers, who must meet the requirements for Key Management Operations (requirements 4A-2.x) and Penetration Testing and Vulnerability Management (4A-3.x).

Q 2 Are 'semi-attended' systems, such as self-checkout systems, acceptable for assessment and listing under the MPoC program?

A Yes. MPoC defines 'merchant-attended' systems as including systems where "… there is a merchant or merchant agent who is able to assist with, or provide oversight of, the payment process" (from MPoC Glossary). This includes 'semi-attended' systems, such as self-checkout systems, where merchant staff are physically present to oversee multiple systems at once.

Vending machines, ticketing machines, and other systems which are not designed or intended for deployment in merchant attended environments are not suitable for assessment and listing under the MPoC program.

Q 3 Is a "Calling Application" as illustrated in Figure 3 of the MPoC Security and Test Requirements in scope for MPoC Assessment or listing?

A No. A calling application is a separate application that communicates with an MPoC Application through an API exposed by the MPoC Application. Requirements in 1A-6 forbid this API from exposing plaintext MPoC assets and the calling application. The MPoC application must be isolated using COTS platform provided memory / access space separation as described in Figure 3. A calling application is not considered for validation or listing under the MPoC Program.

Q 4 [May 2023] Must an Isolated SDK protect itself, or its memory isolation properties, from compromise during the build process during MPoC Application release?

A No. In assessing whether an SDK can be classified as Isolating, only attacks against the built MPoC Application need to be considered. Assessment of the on-going processes used to ensure the security of MPoC Application builds will be validated during the annual checkpoint process as part of the application vendors Secure SLC process.

Q 5 [May 2023] Is the execution of an MPoC SDK within a process separate to that of the MPoC Application sufficient to meet the definition of an Isolating SDK?

A Many modern operating systems allow for a single application to launch multiple processes, and provide to these processes their own virtual memory space. This new memory space can be isolated from other processes, even if those processes are owned by the same user. However, in such cases not all OS provided isolation features may be applied, and there may be shared access to keystores, files, and other resources normally restricted between different applications.

MPoC does allow for an Isolating SDK to share some assets or configurations with the integrating MPoC Application, as noted in the last paragraph of page 26:

"An Isolated SDK may share some assets or configurations with the integrating MPoC Application, such as permissions which determine access to underlying COTS Platform systems, as long as those shared assets/configurations do not expose cleartext sensitive assets".

Therefore, in cases where the MPoC Laboratory is able to validate that the COTS Platform OS's targeted by the MPoC SDK are able to provide memory isolation protection to the cleartext sensitive assets, use of separate processes may be sufficient to meet the requirements for an Isolating SDK.

© 2022-2024 PCI Security Standards Council, LLC. All rights reserved.

Q 6 [May 2023] Is a COTS device permitted to use an NFC antenna which may be removed as part of the device casing or internal sub-component such as a battery?

A Yes. MPoC requires that a COTS device is not intended for integration into another device, but use of a device which may be disassembled is acceptable if the removal of any required subcomponent renders the device inoperable or clearly in a state of disassembly (such as through the removal of an internal battery or external casing). However, MPoC does not allow for use of external or third-party NFC antenna other than through use of a listed PCI PTS SCRP. Any removable antenna must be entirely passive, MPoC does not support the use of removable NFC subsystems which contain a digitizing element.

Q 7 [May 2023] Are there any restrictions to specific form factors for COTS devices and SCRPs that can be approved or used under the PCI MPoC Program?

A No. The MPoC requirements do not dictate a specific form factor for the COTS device, the SCRP, or the combination thereof for inclusion in an approved and validated MPoC Product.

Q 8 [May 2023] What testing and reporting are expected to be performed by an MPoC Laboratory as part of an annual checkpoint?

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

- Back-end environments remain compliant with the applicable security requirements that are to be validated as part of their MPoC assessment,
- Security flaw reporting and penetration testing processes have been followed, and the COTS platform baseline has been maintained,
- Key management and change management processes have been followed, including any required key rotation processes, reseeding of DRNGs, etc,
- Security impacting changes have been processed through delta evaluations,
- The merchant communication plan has been followed,
- Any other Business As Usual (BAU) processes, such as staff training, have been ongoing.

The MPoC Laboratory may need to perform additional testing, depending on the extent to which the MPoC Product has changed. It is expected that the MPoC Laboratory will review a sample of MPoC Applications to ensure ongoing compliance to the MPoC standard.

For example, if an operating system (OS) that was included in the MPoC Solution COTS platform baseline is later determined to be no longer sufficiently secure, the MPoC Laboratory must verify that the MPoC Product vendor has updated its COTS platform baseline and is actively working with its merchants to migrate them to a version of the OS which can be validated as sufficiently secure.

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

An example of requirements which should be considered during an annual checkpoint include (but may not be limited to) the list below. The MPoC Laboratory is expected to determine the exact scope for each annual checkpoint based on the MPoC Product under review, and the changes made to that MPoC Product during the year.

Domain 1: 1A-1.1, 1A-1.2, 1A-1.3, 1A-1.4, 1B-2.4

Domain 2: 2A-1.1, 2A-1.2, 2A-1.7, 2A-1.9

Domain 3: 3A-1.1, 3B-1.2, 3B-1.3, 3B-1.4, 3C-1.1, 3C-2.3, 3D-1.1, 3D-1.2, 3D-1.3

Domain 4: 4A-1.5, 4A-2.1, 4A-2.8, 4A-3.1, 4A-3.2

Domain 5: 5A-1.3, 5A-2.2, 5A-3.1, 5A-3.3

Each annual checkpoint submission must be made by an MPoC Laboratory and include the submission of an updated MPoC Product AOV to PCI SSC after the MPoC Laboratory reviews all changes that occurred since the last full evaluation or last annual checkpoint (whichever is more recent).

Where an MPoC Product is found to not have met its BAU obligations, a passing annual checkpoint submission cannot be produced and the listed MPoC Product will go through an administrative expiry. A new full evaluation of that MPoC Product may be required before that MPoC Product can be relisted.

Q 9 [August 2023] Can individual MPoC Standard test requirements noting 'examination' be met by means other than source code review?

A Yes. Any individual test requirement may be assessed without reference to the source code. However, it is a requirement of the MPoC Program that relevant sections of source code are made available for review when the laboratory deems that necessary, and an assessment where appropriate source code was never viewed as part of the laboratory assessment would not be considered for listing.
Sufficient evidence is required to confirm any test requirement is met, and examination without source code may increase the testing and review time for an MPoC submission.

Q 10 [August 2023] Does the MPoC Standard require that payment messages are authenticated (e.g. cryptographically signed, or provided with a (H)MAC) prior to transmission from the MPoC SDK or MPoC Application?

A No. MPoC Standard does not require that payment messages are authenticated prior to transmission. However, MPoC Standard does require that the connection to the backend processing environment implement a secure channel, and this secure channel must implement controls for maintaining the confidentiality, integrity, and authenticity of the transmitted data (as validated in Security Requirement 1A-5.4).
There may be regional or acquirer specific requirements for the authentication of payment messages which are not considered by the MPoC Standard.

Q 11 [November 2023] Can an MPoC Software vendor that is validated and listed under the PCI Secure SLC program perform self-validation of PCI MPoC implementation changes?

A No. The process required for changes made to MPoC Products, including MPoC Software products, is entirely outlined within the PCI MPoC Program Guide. The MPoC program does not support different validation paths for PCI Secure SLC validated entities.

Q 12 [November 2023] Can an MPoC evaluation exclude some card-based or PIN-based payment functions of an MPoC SDK or MPoC Application?

A No. All functionality included in the MPoC SDK or MPoC Application must be considered by the MPoC Laboratory as part of the assessment, including all card-based or PIN-based payment functions.

Q 13 [November 2023] Can a 'Calling Application' interface to two or more MPoC Applications, or another MPOS application not in scope of MPoC validation?

A Yes. MPoC validation covers all functionality provided by the MPoC Product under assessment. Calling applications are separate from the MPoC Application and interface to the MPoC Application through secure inter-application APIs (see Figure 3 of the MPoC Standard). A calling application is not in scope MPoC validation, and may interface to multiple MPoC Applications, or other non-MPoC payment applications.

However, any payment processes implemented by a non-MPoC payment application are not covered by the MPoC Program and may impact any associated compliance programs.

Q 14 [March 2024] Can an MPoC evaluation exclude requirements which would normally be included in scope (such as payment acceptance methods, or connected devices)?

A No. All requirements which are brought into scope due to the functionality of the MPoC Product must be included in the assessment. Any 'N/A' finding must be justified by the MPoC Laboratory as to why that requirement does not apply. For example, the assessment of an MPoC SDK or MPoC Application which supports use of an MSR cannot exclude MSR requirements.

Q 15 [March 2024] Can an MPoC Application to be listed as part of an MPoC Solution be developed by an entity other than the MPoC Solution provider?

A Yes. The MPoC Solution provider is responsible for ensuring that any MPoC Application that is part of their listing meets all relevant MPoC requirements, including any BAU requirements. The MPoC Solution provider may act as an intermediary between the application developer and MPoC Laboratory as required.

MPoC Applications listed as part of an MPoC Software product (not an MPoC Solution) must be developed by the MPoC Software vendor, and cannot be developed by another entity.

Q 16 [March 2024] Is it required that a laboratory use more than one model/manufacturer of COTS device when evaluating a candidate MPoC Product?

A Yes. Where an MPoC Product supports Platforms that may have different implementations or configurations of operating system or hardware, more than a single model/manufacturer of COTS device must be used during testing. Use of all possible configurations of device and operating system type is not required.

MPoC Security Requirement 1A

Q 1 [November 2024 – Deleted]

Q 2 [November 2024 – Deleted]

Q 3 [November 2024 – Updated] Is it acceptable for an MPoC Application integrating an MPoC SDK to manage or implement secure channels directly, following guidance provided by the MPoC Software vendor?

A Yes. An MPoC SDK may allow for the integrating MPoC Application to implement, or provide configuration to, a secure channel to the payment processing environment. The guidance provided by the MPoC SDK vendor must detail how the secure channel is to be implemented so that it meets the requirements of 1A-5, and this guidance must be validated by the laboratory to be correct and complete during the evaluation.

The secure channel to any other systems in scope of the MPoC requirements, including the backend A&M environment and any peripheral devices such as a PCI PTS SCRP, must be implemented by the MPoC SDK. This includes implementations where the A&M environment includes the payment processing environment.
In all cases it is not permissible for the MPoC Application to disable any required secure channel, or configure the secure channel to accept insecure cipher-suites or protocol versions.

Q 4 [May 2023] Requirement 1A-4.3 states that secret or private keys embedded into MPoC SDK must be assessed against 1B-2: Software protected cryptography. For keys which are not embedded into the MPoC SDK, such as temporary or ephemeral keys, what software-protected cryptography requirements apply?

A The software protected cryptography requirements apply to all secret and/or private keys used within the COTS device except in the following cases:

- Cleartext Unique-per-transaction keys processed or temporarily stored in RAM within the rich execution environment.

- Where the cryptographic key is protected by other means, such as through protection in a TEE or by encryption with another cryptographic key.

Q 5 [May 2023] Can software protection mechanisms be used to protect private and secret keys used in the backend A&M system?

A No. Guidance from requirement 1A-4.3 notes that the embedding of secret or private cryptographic keys in aspects of the MPoC Software other than the MPoC SDK or MPoC Application is not permitted.
HSMs approved to FIPS 140-2 Level 3 or PCI HSM must be used for all cleartext key operations and storage as stated in 4A-2.2. Cryptographic keys in scope for this requirement include, but are not limited to, keys used for verifying MACs on incoming attestation data, keys used for signing attestation results and keys involved in remote key loading. Cryptographic keys used as part of a TLS secure channel and application signing keys are excluded from this requirement.

Q 6 [November 2024 - Updated] Can RSA 2048 bit be used to encrypt AES keys in MPoC Products?

A Yes, but only once per application install or if use of larger RSA keys is prevented by the COTS platform being used.
Any key provisioning process must occur over a secure channel.

Q 7 [August 2023] Can MPoC Software rely on a secure channel to meet the public key integrity and authenticity requirements of MPoC Security Requirement 1A-3.3?

A No. Public keys are sensitive assets whose integrity and authenticity must be independently assured without relying on the protections of the secure channel.

Q 8 [November 2023] Can an MPoC Laboratory accept an AOV as evidence of meeting requirement 1A-1.4?

A Yes, an AOV can be used as evidence for meeting requirement 1A-1.4 if:

- The Secure Software AOV has been produced and signed by a listed Secure Software Assessor company and assessor.
- The AOV is counter-signed by PCI SSC indicating it has passed through PCI SSC review.
- The AOV correctly details the version and vendor of the MPoC A&M software.
- The AOV indicates that the assessment occurred within the last 12 months.

Q 9 [November 2023] Can access to security-flaw-reporting programs required in 1A-1.2 and 4A-3.2 of MPoC be restricted to certain groups, such as customers?

A No. It is required that MPoC Vendors are able to receive and process security-flaw reports regardless of their origin. The process on how to deliver such security flaw reports must be publicly accessible, and clearly designated for this purpose. However, it is permissible to have more specific details of the program, such as outlines of internal processes, available to non-public groups, such as direct customers.

Q 10 [March 2024] Can the default random number generator of a COTS platform be used as the sole source of COTS-based entropy to seed a DRNG?

A As per requirement 1A-2.3 a DRNG is required when a true random number generator is not used as the source of random numbers on the COTS device. As per requirement 1A-2.5 a DRNG must use at least two sources of entropy as its seed – one sourced externally and one sourced internally. As per requirement 1A-2.4 the internal entropy seeds must be trusted.

A trusted source of entropy is one where the entropy output has been validated through testing and there is a reasonable assurance that this testing is valid for all COTS platforms in the baseline.

Where testing of the RNG is not possible or previous testing is not available, at least two sources of entropy sourced on the COTS device must be used in addition to the external source.

Q 11 [March 2024] Does the MPoC SDK / MPoC Application need to prevent the use of weak cipher suites when using TLS to meet secure channel requirements?

A Yes. An MPoC SDK / MPoC Application must ensure secure channels used to meet section 1A-5 are equal or equivalent to the cryptographic requirements outlined in Appendix C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms. Secure channels which do not meet these requirements must be rejected, or not relied upon to meet the MPoC requirements.

Q 12 [November 2024] Is validation to the PCI Secure Software Standard required for MPoC A&M backend software, as per requirement 1A-1.4?

A No. Validation of backend A&M software against the Secure Software requirements is recommended, but is no longer required.

MPoC Security Requirement 1C

Q 1 [May 2023] Is it acceptable to implement designs where an A&M message is required to enable payment processing, rather than disable payment processing?

A Yes. Some designs may be implemented such that an A&M message is required to enable payment processing, rather than disable payment processing.
MPoC Solutions where an A&M result is required to enable payment processing, rather than disable payment processing, may pass these messages through the COTS device. However, such implementations must be validated as per MPoC requirements for A&M operations and data security, including requirement 1C-4.2, and require that an acceptable 'signal-to-accept' indicator is transmitted at least every 10 transactions. During validation the MPoC Laboratory must confirm that blocking or modification of this message results in the cessation of payment acceptance.

Q 2 [March 2024] Does an A&M system require a backend component?

A Yes. An A&M system must implement a backend command and control system that collects and uses information gathered from many devices on which MPoC Applications are installed to make security decisions about any specific installed instance of the MPoC Application.

Q 3 [November 2024] Is detection of rooted or jailbroken COTS platforms always required?

A No. COTS-based MPoC Software that executes entirely outside of the REE of the COTS device, may allow for rooted and jail-broken devices to be included in the COTS platform baseline. In such cases, it must be confirmed that the COTS-based MPoC Software does not allow for sensitive assets, such as account data or cryptographic keys, to be exposed in, passed through, or obtained from the REE.

MPoC Security Requirement 1D

Q 1 [November 2024 - Deleted]

Q 2 [November 2024] Does the requirement for keys that are exposed in the REE of the COTS platform to be unique per transaction apply to secret or private keys used during the process of provisioning?

A No. This requirement does not apply to keys used only once per application install (e.g., during initial provisioning), or keys which are used to generate future keys (but cannot be used to derive historic keys).

© 2022-2024 PCI Security Standards Council, LLC. All rights reserved.

MPoC Security Requirement 1E

Q 1 Is a scrambled keypad, where the numeric digits on the keypad are moved around, necessary for validation to the MPoC requirements?

A No. The use of a scrambled keypad may assist with meeting testing requirements for PIN capture through side channel leakage, but use of such a scrambled keypad is not enforced.

Q 2 [March 2024] If a COTS device has a physical keypad, can this be used for PIN entry in an MPoC SDK / MPoC Application?

A No. An MPoC Software Product or MPoC Solution can support PIN entry only through use of the touch screen on the COTS platforms supported (in accordance with relevant MPoC requirements).

Q 3 [March 2024] Is it possible to implement per-transaction accessibility features for MPoC SDKs and/or MPoC Applications?

A Yes. Accessibility features may be made available on a per-transaction basis, and must not be the default or sole PIN entry method offered. Accessibility features must not display the individual PIN digits themselves or provide feedback (audio, visual, or haptic) that is unique to individual PIN digits. 'Zoom' features to increase the size of keypad buttons may be provided, as long as individual PIN digits cannot be uniquely identified.

Side channel testing (requirement 1E-1.3) of the accessible PIN entry mode is not required.

The MPoC Software and the A&M system must be designed to protect any unique features of the accessible PIN entry process, including monitoring and tracking the number of times accessible PIN entry is used.

When enabled, accessibility features must provide clear indication that they have been enabled and allow for the cardholder entering the PIN to disable this mode at any time. Accessibility features must exit upon completion of the payment transaction process, including error states, and require explicit enabling for each separate payment transaction.

MPoC Security Requirement 1F

Q 1 [May 2023] Requirement 1F-1.4 states that payment transactions may be accepted in offline mode for a maximum period of 48 hours. However, requirement 1F-2.4 states that the MPoC SDK must disable all payment acceptance after no more than 24 hours of no response from the A&M backend. How do these two different times relate to one another?

A The MPoC requirements separate the concept of ‘offline payment transactions’ from the concept of ‘disconnection from backend services’. For example, due to some issue with the backend payment processing environment (that does not similarly affect the A&M system), an MPoC SDK may be enabled to perform offline payment acceptance whilst still connected to the backend A&M system.

However, in all cases, if an MPoC SDK that supports offline payment processing is disconnected from the A&M backend, it will be required to cease payment processing after 24 hours. In circumstances where connection to A&M backend may be maintained (perhaps in an intermittent manner) within a 24-hour period, the MPoC SDK will be able to continue to perform offline payment processing for up to 48 hours (before connection to the payment processing backend must be re-established).

An MPoC SDK that is not enabled to support offline payment processing must suspend payment processing no more than after 60 minutes of continuous operation without a passing response from the A&M back-end component.

MPoC Security Requirement 2A & 2B

Q 1 [May 2023] When performing evaluation of an MPoC Application, is it required that the MPoC Laboratory has access to the source code of the MPoC Application? Is this required even when the MPoC Application integrates an Isolating SDK?

A Yes. As noted in the definition of ‘examination’ in the section “Testing Methods” in the MPoC standard, it is expected that source code is made available for review during an MPoC Software and MPoC Application assessment. In the case of Isolating SDKs, the MPoC Application source code is required to enable the MPoC Laboratory to validate that the MPoC SDK is integrated correctly in line with the MPoC Software security guidance, and the MPoC Application does not attempt to bypass any of the security features or sensitive asset management functions of the MPoC SDK.

Q 2 [November 2023] What testing is required of an MPoC Solution that integrates an MPoC Application which is listed as part of a listed MPoC Software Product?

A Testing of an MPoC Application to Domain 2 is not required if that MPoC Application is listed as part of an MPoC Software product, and it is not modified during integration with the MPoC Solution. An MPoC Solution that is solely using MPoC Applications which are already listed is responsible for validation of Domain 4 and Domain 5. Validation of Domain 3 is also required if the MPoC Solution is not also relying on a listed MPoC A&M Service.

Q 3 [March 2024] Can an MPoC Vendor provide tools to assist an MPoC Laboratory with the Domain 2 testing of an MPoC Application integrating that Vendor's MPoC SDK?

A Yes. An MPoC Vendor may provide tools to assist with laboratory evaluations, such as those performed under Domain 2A for MPoC Applications integrating an Isolating SDK. Such tools may include automated scanning processes to help confirm the correct and secure integration of that vendors Isolating SDK.

At all times, the MPoC Laboratory is responsible for the correctness and completeness of the testing process, and it is expected that an MPoC Laboratory will validate any such tooling prior to use.

Testing must be performed within the scope of the MPoC Laboratories validation under their MPoC Laboratory listing, including physical, logical, and procedural controls. MPoC Laboratories are not able to submit testing performed on their behalf by another entity, including the MPoC Vendor.

MPoC Security Requirement 3D

Q 1 [November 2024 – Updated] Requirements 3D-1.1 and 3D-1.2 outline the need for the security assessment of the A&M backend environment. Are these requirements the only options, and if so when do they apply?

A A&M backend environments must be assessed to either Appendix A or to PCI DSS. One of either 3D-1.1 or 3D-1.2 must be assessed as part of a compliant report. Assessment to Appendix A is only suitable if the A&M systems are sufficiently isolated from the payment processing systems and Cardholder Data Environment. For details on what may be considered 'sufficient isolation' refer to the PCI DSS, and associated information supplements and FAQs. In all other cases, where sufficient isolation is not provided, the A&M environment must be compliant to the requirements of the PCI

DSS. Assessment to the requirements in Appendix A3: Designated Entities Supplemental Validation (DESV) is no longer required.

Q 2 [November 2024 - Deleted]

MPoC Security Requirement 4A

Q 1 [November 2023] Can HSMs validated to FIPS140-2/3 Level 2 be used in an MPoC implementation?

A Yes. HSMs validated to FIPS 140-2/3 Level 2 may be used for the storage and operation of keys related to A&M data and non-PIN account data, when operated within a 'Controlled Environment' as defined in ISO13491.

MPoC Security Requirement 5A

Q 1 [November 2023] Can an MPoC Solution be implemented by an entity that is not the owner of the merchant account relationship?

A Yes. The MPoC Standard requires that merchants are securely onboarded and kept up to date with relevant information in a timely manner (requirement 5A-1.x). This communication must be documented and demonstrably in use, as validated under 5A-1.3, but may occur through channels other than those maintained by the direct owner of the merchant relationship (e.g., the merchant's bank).

Examples may include communication through the MPoC Application directly, or through out of band communication methods established during merchant onboarding.

Validation that merchant communications is occurring as needed will be performed during annual checkpoints and any full revalidation processes.

© 2022-2024 PCI Security Standards Council, LLC. All rights reserved.