Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

Frequently Asked Questions (FAQs) for Validation Processes for Merchant-Managed Solutions

February 2022

Document Changes

Date	Description
January 2016	Initial Publication to align with the introduction of Merchant-managed Solutions in the P2PE v2.0 Standard.
February 2022	Updated references to be current and general updates based on the latest release of the P2PE Standard and Program Guide. *Note: The general context of Merchant-managed Solutions (MMS) has not changed since the initial publication.*

Frequently Asked Questions for Validation Processes for Merchant-Managed Solutions

In the context of PCI SSC's Point-to-Point Encryption (P2PE) Standard, the terms "merchant-as-a-solution-provider" and "merchant-managed solution" apply to merchants who choose to manage their own P2PE solutions for their retail locations or stores/shops, rather than outsourcing the solution to a third-party P2PE solution provider. The P2PE Standard defines the separation needed between encryption environments (where the encrypting payment terminals are physically located) and the merchant's account data decryption environment (and other merchant cardholder data environments) for a merchant-managed solution. Refer to the P2PE Standard for details.

Q 1 Where can I find out more information about P2PE and merchant-managed solutions (MMS)?

A *The Point-to-Point Encryption (P2PE) Standard specifies the requirements for merchant-managed solutions and the P2PE Program Guide provides an overview of the validation processes for MMS and refers readers to PCI SSC's website for all associated documents. In addition to the validation documents available on the PCI SSC website, this set of frequently asked questions (FAQs) for MMS is intended to provide the answers merchants and their assessors need for assessments and use of such solutions.*

Q 2 How can a merchant-managed solution be validated to the P2PE Standard?

A *The P2PE Standard supports validation of merchant-managed solutions (MMS). To confirm that the solution meets the requirements of the P2PE Standard, the assessment must be carried out by a P2PE Assessor.*

Merchants acting as their own solution providers have the same responsibilities of solution providers mentioned throughout the P2PE Standard in addition to specific requirements solely for MMS. In an MMS, the merchant-as-a-solution-provider is responsible for all solution provider roles as described in the P2PE Standard and the P2PE Program Guide.

Note: *As merchant-managed solutions are only used within a specific merchant's environment, these solutions are not eligible for listing on the PCI SSC website.*

For further information, please refer to the current P2PE Program Guide.

Q 3 Does a P2PE Instruction Manual need to be produced and maintained for merchant-managed solutions?

A *Yes, merchant-managed solutions (MMS) must have a P2PE Instruction Manual (PIM) for use in the merchant's encryption environments. The PIM must be assessed by the P2PE Assessor as meeting the requirements of the P2PE Standard in order for the MMS to be validated. Note that there is a mandatory PIM Template provided on the PCI SSC website that facilitates preparation of the PIM by the merchant-as-a-solution-provider.*

Q 4 Can P2PE Components and P2PE Applications listed on the PCI SSC website be used as a part of merchant-managed solutions?

A *Yes, P2PE Components and P2PE Applications listed on the PCI SSC website may be used within merchant-managed solutions (MMS). In an MMS, the merchant-as-a-solution-provider is responsible for all solution provider roles as described in the P2PE Standard and P2PE Program Guide, including management of any P2PE Components used within the solution.*

Q 5 Can a merchant-managed solution include P2PE Applications that are not listed on the PCI SSC website?

A *Yes. It is not required that P2PE Applications be listed on the PCI SSC website in order to be used as a part of merchant-managed solutions (MMS). However, the P2PE Application must undergo a full assessment according to the P2PE Standard and Program Guide. Note that merchants can also use PCI SSC listed P2PE Applications in their own MMS. Once the P2PE Application Assessor performing the assessment determines that the P2PE Application complies with the P2PE Standard, the assessor prepares an MMS Application P2PE Report on Validation (MMS Application P-ROV) for submission to the merchant. As with the MMS Solution P-ROVs, the Application P-ROV and related P-AOV is retained by the merchant.*

Note that it is not necessary for the merchant to sign a Vendor Release Agreement, as the application is not being listed on the PCI SSC website.

As with the validity period of an MMS P2PE assessment, the validity period of a P2PE assessment for a non-listed MMS P2PE application is three years, the same as for PCI-listed P2PE applications (as defined in the P2PE Program Guide). After three years, a full re-assessment of the application must be completed against the then current version of the P2PE Standard. Additionally, to maintain the P2PE validation for the MMS and the application, the merchant is required to complete an Annual Revalidation using an MMS P2PE Attestation of Validation (P-AOV) as documented in the P2PE Program Guide. Similar to the MMS P-ROV, the merchant should retain these MMS P-AOVs.

Q 6 How should a P2PE assessment of a merchant-managed solution be documented?

A *Once the P2PE Assessor performing the assessment determines that the merchant-managed solution (MMS) is in compliance with the P2PE Standard, the assessor prepares an MMS P2PE Report on Validation (P-ROV) for submission to the merchant. MMS P-ROVs are not submitted to PCI SSC but are retained by the merchant:*

- *To support use of the P2PE SAQ (or completion of a merchant ROC with fewer applicable PCI DSS requirements) for the merchant's retail locations; and/or*
- *To provide when requested by the merchant's acquirer or a payment brand.*

The MMS P-ROV must be accompanied by an MMS P2PE Attestation of Validation (P-AOV). It is not necessary for the merchant to sign the Vendor Release Agreement as the solution is not eligible for listing on the PCI SSC website.

The MMS P-ROV and the MMS AOV templates are available on PCI SSC's website.

Q 7 For how long is a P2PE assessment of a merchant-managed solution valid?

A *The validity period of a P2PE assessment for merchant-managed solutions is three years—the same as for PCI-listed P2PE Solutions—as defined in the P2PE Program Guide. After three years, a full re-assessment of the solution must be completed against the then-current version of the P2PE Standard. Additionally, to maintain the P2PE validation, the merchant is required to complete an Annual Revalidation using an MMS P2PE Attestation of Validation (P-AOV as documented in the P2PE Program Guide. Similar to the MMS P-ROV, the merchant should retain these MMS P-AOVs:*

- *To support use of the P2PE SAQ (or completion of a merchant ROC with fewer applicable PCI DSS requirements) for the merchant's retail locations; and/or*
- *To provide when requested by the merchant's acquirer or a payment brand.*

The MMS P-AOV is available on PCI SSC's website.

Q 8 What is the benefit to a merchant of undergoing a PCI P2PE assessment with a P2PE Assessor? Which PCI DSS requirements are applicable to their stores/retail locations and which are applicable for their P2PE decryption environment and other in-scope environments?

A *A merchant that has had its MMS assessed by a P2PE Assessor has the assurance of that assessment to clearly define which areas of its environment are in-scope for PCI DSS assessment(s) and which can potentially use SAQ P2PE. See this FAQ for more details about use of SAQ requirements by merchants required to undergo an onsite assessment: Can SAQ eligibility criteria be used for determining applicability of PCI DSS requirements for onsite assessments?*

The table below provides a summary of typical PCI DSS and P2PE validation requirements for merchants with and without a PCI-validated MMS:

Validation Focus	Standard	Validation Frequency and Documentation – With a PCI-validated MMS*	Validation Frequency and Documentation – Without a PCI-validated MMS*
Retail stores/locations	PCI DSS	Annually: SAQ P2PE or partial ROC	Annually: Full SAQ or ROC
Data center(s) & other in-scope environments, including the P2PE decryption environment	PCI DSS	Annually: Full SAQ or ROC	Annually: Full SAQ or ROC
P2PE Solution	P2PE	Every three years: Full MMS P2PE P-ROV Annually: P2PE Annual Revalidation using an MMS P-AOV	N/A

* *Merchant PCI DSS validation requirements are defined by the payment brands—merchants should contact their acquirer or the payment brands directly to determine their requirements.*