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

Program Guide

Version 1.0

December 2022

Document Changes

Date	Version	Description
December 2022	1.0	Initial public release

Table of Contents

1 Introduction

This document, the Mobile Payments on Commercial off-the-shelf Program Guide provides an overview of the PCI SSC Mobile Payments on Commercial off-the-shelf (COTS) Standard (MPoC)™ Program operated and managed by PCI Security Standards Council, LLC (PCI SSC).

The MPoC Program Guide describes MPoC Program Requirements for candidate and existing MPoC Product Evaluation and Validation against the *MPoC Standard* by a PCI Recognized Laboratory, subsequent Acceptance by PCI SSC, and Listing on the Website (https://www.pcisecuritystandards.org/).

1.1 MPoC Program Background

The MPoC Program is based, in part, on the previous PCI Software-based PIN on COTS (PCI SPoC) and PCI Contactless Payments on COTS (PCI CPoC) programs. It allows for the acceptance of PIN and / or PAN data through COTS-native interfaces on a COTS device, as well as through external devices such as a PCI PTS POI SCRP. The MPoC Program does not supersede or replace the existing PCI SPoC or PCI CPoC programs. Listing of an MPoC Product does not imply or convey suitability or Validation with the PCI SPoC or PCI CPoC programs.

A solution already Listed as Validated to the PCI SPoC or PCI CPoC programs may be presented as a candidate MPoC Product for Evaluation to the MPoC Program, and if Validated during a full Evaluation may be Accepted by PCI SSC and subsequently Listed as an MPoC Product.

1.2 MPoC Program Overview

An entity with a candidate product (hereinafter referred to as "candidate MPoC Vendor" with a "candidate MPoC Product") can pursue Acceptance and Listing of their candidate MPoC Product under the MPoC Program.

The decision to undergo Acceptance and Listing of a candidate MPoC Product is a business decision of the candidate MPoC Vendor. The process for achieving Acceptance and Listing can only be triggered if the candidate MPoC Vendor enters into an agreement with an MPoC Lab to perform an Evaluation of the candidate MPoC Product against the *MPoC Standard* (referred to in the VRA as a "Contracted Assessment"), under the conditions and scope contractually agreed upon between the candidate MPoC Vendor and the MPoC Lab. If the Contracted Assessment (and corresponding Evaluation) concludes Validation is achieved, then the MPoC Lab submits the required evidence to PCI SSC for review and, if eligible, Acceptance and subsequent Listing by PCI SSC.

Only an MPoC Lab is permitted under the MPoC Program to Evaluate and Validate compliance of a candidate MPoC Product against the *MPoC Standard* and submit the Evaluation evidence to PCI SSC for Acceptance (if PCI SSC deems the submission eligible) and subsequent Listing. Candidate MPoC Vendors cannot submit evidence directly to PCI SSC and must enter a Contracted Assessment agreement with an MPoC Lab. Entities should reference the Website for MPoC Labs' contact information.

Each MPoC Product type eligible for the MPoC Program is supported by, defined, and described in the *MPoC Standard*. Possible MPoC Products include each of the following types:

- MPoC Software.

- MPoC Attestation and Monitoring Service (MPoC A&M Service).

- MPoC Solution (merchant-attended).

The *MPoC Standard* identifies each type of candidate MPoC Vendor responsible for each eligible MPoC Product type:

- MPoC Software Vendor.

- MPoC Attestation and Monitoring Service Provider (MPoC A&M Service Provider).

- MPoC Solution Provider.

A candidate MPoC Product becomes an officially recognized MPoC Product (and no longer a candidate) upon Acceptance by PCI SSC. This Acceptance denotes that the MPoC Product and MPoC Vendor have been successfully Validated by an MPoC Lab and are considered to have met all relevant requirements of the *MPoC Standard* and MPoC Program as of the date of such Acceptance.

Acceptance of an MPoC Product is accompanied by Listing of the MPoC Product on the Website. The List of Validated MPoC Products on the Website is the authoritative source for the Validation and Acceptance by PCI SSC for any MPoC Products. Any claims regarding the Acceptance of an MPoC Product can be verified by referencing the Listing on the Website.

MPoC Product Listings have a 3-Year Listing lifecycle that starts on the date of initial Acceptance by PCI SSC. MPoC Vendors with MPoC Products Listed on the Website must continue to adhere to MPoC Program Requirements after initial Acceptance, including implementing robust-risk management practices as an integral part of their business as usual (BAU) operational process.

Maintenance of Good Standing under the MPoC Program is not a 'point-in-time' event. Per MPoC Program Requirements maintenance of Good Standing is an on-going process.

To maintain Good Standing, and thereby avoid early administrative Expiry (section 4.1.1), MPoC Vendors must follow MPoC Program Requirements for Maintaining Good Standing (section 4) during the entire 3-Year Listing lifecycle. Before the conclusion of the MPoC Products' 3-Year Listing lifecycle, the MPoC Vendor should decide if they will pursue another 3-Year Listing lifecycle for their MPoC Product as per this Program Guide, or alternatively allow their MPoC Product to Expire (section 5).

1.3 Related Publications

Use this Program Guide with the latest versions of (or successor documents to) the following PCI SSC publications, which are available on the Website:

Table 1: Related Publications

Document Name	Description
Payment Card Industry (PCI) Mobile Payments on COTS Security and Test Requirements (*MPoC Security & Test Requirements, or MPoC Standard*)	Defines security requirements, test requirements, and guidance for entities involved in the development, deployment, and operation of the mobile payment acceptance products (MPoC Products) that use COTS devices. Provides details of the testing processes performed by the PCI Recognized Laboratory (MPoC Lab) that perform the Validation testing (Evaluation) of the MPoC Product(s).
MPoC Product Attestation of Validation (AOV)	The *AOV* is a form for MPoC Labs to use to attest to the results of an MPoC Product Evaluation.
MPoC Product Evaluation Report Template	The *MPoC Product Evaluation Report Template* is the form that MPoC Labs must use to document the MPoC Product Evaluation and Validation.
Vendor Release Agreement (VRA)	The *VRA* establishes the terms and conditions under which PCI SSC Accepts and Lists Validated MPoC Products.
Technical FAQs	Technical FAQs are updated on a regular basis to clarify the MPoC Program Requirements and may also address new security threats. As such, technical FAQs supersede any specifically conflicting provisions of the Program Guide and related publications in this table and are effective immediately upon publication.

1.4 Updates to Documents and Security Requirements

This Program Guide is reviewed regularly and may be modified to reflect continual improvement and quality management of the MPoC Program.

PCI SSC reserves the right to add, change, amend, or withdraw security requirements, test requirements, guidance, training, and / or other requirements at any time.

PCI SSC may provide interim updates to the PCI community through a variety of means, including e-mail bulletins and newsletters, frequently asked questions (FAQs), the Website, and other communication methods.

If a change to the MPoC Program is required, PCI SSC endeavors to work closely with stakeholders to help minimize the impact of any changes.

Technical FAQs are updated on a regular basis to clarify the MPoC Program Requirements and may also address new security threats. As such, technical FAQs supersede any specifically conflicting provisions of the Program Guide and related publications (Table 1) and are effective immediately upon publication.

1.5 Terminology

For the purposes of this Program Guide, the following terms have the meanings set forth in Table 2.

Table 2: MPoC Program Terminology

Term	Definition
Accepted / Acceptance / Accept	Acceptance is the action of being accepted for Listing by PCI SSC, as outlined in Section 3 of this document. See *Website*. See *Vendor Release Agreement* (or VRA). See *List* (or Listing).
AOV	Acronym for *Attestation of Validation.* As applicable to the MPoC Program, the *AOV* is a form for MPoC Labs and MPoC Vendors to attest to the results of an MPoC Evaluation, declaring the MPoC Product's Validation status against the *MPoC Standard*. See *Validation*.
Attestation and Monitoring Software (or A&M software)	Attestation & Monitoring Software is defined in the *MPoC Standard*.
Change	Any variation to an MPoC Product after initial Acceptance and before the Re-Validation date. Changes are classified in the MPoC Program as *no impact Change*, *administrative Change*, or *implementation Change*. See Section *4.2* for more details on types of Changes.
Contracted Assessment	Contracted Assessment is defined in the VRA. See *Vendor Release Agreement* (or VRA).
Evaluation / Evaluated / Evaluate	Evaluation is an in-depth examination of an (existing) MPoC Product or candidate (new) MPoC Product against the *MPoC Standard* as per Program Requirements.
Evaluation Report *(or MPoC Product Evaluation Report)* *(or Reports on Validation (ROV))*	*Also referred to as "Assessment Report" in the VRA.* The Evaluation Report contains the Evaluation and Validation or Re-Validation results for all test requirements in the *MPoC Standard* as determined by the MPoC Lab during the Evaluation.
Expired (Expiry / Expire)	Expired MPoC Products are no longer Accepted by PCI SSC. Expired means on-going Acceptance (approval) by PCI SSC of the former MPoC Product stopped at a point-in-time.
FAQ / FAQs	Acronym for *Frequently Asked Question(s).* *See 1.3 Related Publications.*
Good Standing	Good Standing that the applicable MPoC Vendor and MPoC Product are in compliance with all applicable MPoC Program Requirements, including but not limited to requirements for initial Acceptance. See *MPoC Program Requirements*.

Term	Definition
List *(or Listing)* *(or Listed)* *(or Listable)*	As part of its ongoing payment security initiatives, the PCI Security Standards Council makes available on its Website a List of MPoC Products that have been Evaluated and Validated by an MPoC Lab for compliance against corresponding PCI SSC *MPoC Standard* and subsequently Accepted and Listed by PCI SSC.
Live Testing	Live testing means testing of an MPoC Product as it is fielded or supplied to consumers of that MPoC Product.
Merchant-attended	Merchant-attended is defined in the *MPoC Standard*.
MSR *(Magnetic Stripe Reader)*	MSR is defined in the *MPoC Standard*.
MPoC Application	MPoC Application is defined in the *MPoC Standard*.
MPoC A&M Service *(MPoC Attestation and Monitoring Service)*	A type of MPoC Product that is a service offering. The MPoC A&M Service operates the attestation and monitoring functionality of Listed MPoC Software Product(s). The MPoC A&M Service is provided by an MPoC A&M Service Provider and is supported by the MPoC Standard for standalone Evaluation, Validation, Acceptance and Listing on the Website. Also see *MPoC A&M Service Provider*.
MPoC A&M Service Provider	MPoC A&M Service Provider is defined in the *MPoC Standard*.
MPoC Lab	MPoC Labs are PCI Recognized Laboratories qualified by PCI SSC to perform Evaluations of candidate MPoC Products and existing MPoC Products against the *MPoC Standard*. MPoC Labs are also qualified by PCI SSC to perform Evaluations of optional non-PTS approved MSRs for MPoC Program purposes. See *PCI Recognized Laboratory*.
MPoC Product	*Product* as defined in the VRA and applicable for the MPoC Program means a complete MPoC Solution (Product), MPoC Software (Product), or MPoC A&M Service (Product), development process or combination of any of the foregoing with respect to which Validation or Acceptance may be sought on a standalone basis as part of this MPoC Program.
MPoC Product Expired List	Refers to the grouping of and inclusion of all *Expired (former) MPoC Product Listings* on the Website. Also see *Expired* Also see *List*.
MPoC Program	PCI SSC's MPoC Program Requirements for qualification of MPoC Labs and applicable employees thereof. See *MPoC Program Requirements*.
MPoC Program Documents	The *MPoC Standard* and Program Guide, all written agreements executed between PCI SSC and the applicable MPoC Vendor in connection with the MPoC Program, all other materials, requirements, obligations, policies, and procedures published from time to time by PCI SSC on the Website or elsewhere relating to the MPoC Program, and all successor versions of the foregoing, in each case, as amended from time to time.

Term	Definition
MPoC Program Requirements	With respect to a given MPoC Vendor, all requirements, obligations, policies and procedures applicable to such MPoC Vendor or otherwise generally applicable to MPoC Vendors, as set forth in the corresponding MPoC Program Documents, the VRA or otherwise established by PCI SSC from time to time in connection with the MPoC Program, including without limitation, those relating to disclosure, PCI SSC's quality assurance initiatives, and / or export control and administration, and such MPoC Vendor's warranties pursuant to the VRA..
MPoC SDK	MPoC SDK is defined in the *MPoC Standard*.
MPoC Software *(Mobile Payments on COTS (MPoC) Software)*	A type of MPoC Product and component supported by the *MPoC Standard* for standalone Evaluation, Validation, Acceptance and Listing on the Website. MPoC Software is defined in the *MPoC Standard*. Also see *MPoC Product*.
MPoC Software Vendor	MPoC Software Vendor is defined in the *MPoC Standard*.
MPoC Solution *(also Mobile Payments on COTS (MPoC) Solution)*	MPoC Solution is defined in the *MPoC Standard*. Also see *MPoC Product*.
MPoC Solution Provider	MPoC Solution Provider is defined in the *MPoC Standard*.
MPoC Standard	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Mobile Payments on COTS Security and Test Requirements*, any / all testing procedures, appendices, annexes, exhibits, schedules, and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website.
MPoC Vendor	An MPoC Solution Provider, or MPoC Software Vendor, or MPoC A&M Service Provider. Vendors with *candidate* MPoC Products pursuing Evaluation, Validation, Acceptance and Listing may be referred to as *candidate* MPoC Vendors if they do not have other Listed MPoC Products. A *candidate* MPoC Vendor becomes an MPoC Vendor upon initial Acceptance of a candidate MPoC Product by PCI SSC. Also see *Acceptance*.
Non-PTS approved MSR	Non-PTS approved MSR is defined in the *MPoC Standard*.
Participating Payment Brand *(or Payment Brand)*	A global payment card brand or scheme that is also a limited liability company member of PCI SSC (or affiliate thereof).
PCI PTS Approved Device list	The list of PCI PTS-approved PIN transaction security devices made available on the *Website*.
PCI Recognized Laboratory	A laboratory qualified by PCI SSC to perform evaluations of devices and solutions against the requirements of applicable PCI SSC Standards. Also see *MPoC Lab*.
PCI SSC	Acronym for Payment Card Industry Security Standards Council, LLC.
Portal	The MPoC Lab (on behalf of the MPoC Vendor) must submit all MPoC Product Validation-related documents to PCI SSC through PCI SSC's secure Website (Portal).
Program Guide	The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) Mobile Payments on COTS (MPoC) Program Guide,* as from time to time amended and made available on the Website.

Term	Definition
PTS Lab	See *PCI Recognized Laboratory*
Red-lined	Clearly indicates any modifications by way of accessibility color or accessibility font so that any iterations, modifications, deletions, moves, etc. are clearly visible when viewed digitally or printed.
Re-Validation Date	The Expiry date of an MPoC Product that is in Good Standing.
Re-Validation (or Re-Validate)	A full Evaluation where the MPoC Lab re-confirms Validation of an existing MPoC Product against the *MPoC Standard. Re-Validation is not applicable to Expired (former) MPoC Products.* See Section *4 Maintaining Good* Standing. See Section *6 MPoC Program Fees*.
SCRP (Secure Card Reader – PIN.)	SCRP is defined in the *MPoC Standard*.
Third Party Rider	See *Third Party Product Provider*
Third Party Product (TPP)	A component (device, application, code, product) or service that is incorporated into and / or referenced by the applicable MPoC Product. See *VRA* Section *1.1*
Third Party Product Provider (TPP Provider)	A device, application, product, or service (whether or not eligible for Validation or Acceptance on a standalone basis as part of a Program) that is incorporated into and / or referenced by any MPoC Product. See *VRA* Section *1.1*
Unattended	*Unattended is defined in the MPoC Standard.*
Validation (or Validate, or Validated)	The MPoC Lab's determination of compliance with the applicable *MPoC Standard* and Test Requirements. Validation is attested by the MPoC Lab and documented in the AOV. See *AOV.*
Vendor Release Agreement (or VRA)	The then-current and applicable form of release agreement that PCI SSC requires to be executed by MPoC Vendors (and any Third-Party Riders) in connection with the MPoC Program. The VRA template is available on the Website.
Website	The then-current PCI SSC Website (and its accompanying web pages) currently available at www.pcisecuritystandards.org. See *List*. See *Good Standing*.

2 Roles and Responsibilities

This section provides an overview of the roles and responsibilities of the various MPoC Program stakeholder groups.

2.1 MPoC Vendors

MPoC Vendors are responsible for:

- Ensuring compliance with all applicable laws, statutes, regulations, and rules (including privacy laws without limitation) that apply to their activities as MPoC Vendors and their MPoC Products, and any related services or products.

- Creating MPoC Products compliant with the *MPoC Standard*.

- Contracting with an MPoC Lab as per MPoC Program Requirements.

- Submitting their candidate MPoC Products and supporting documentation to the MPoC Lab for Evaluation and authorizing the same MPoC Lab to submit resulting Evaluation Reports (Reports on Validation) and related information (such as the VRA) to PCI SSC upon successful Validation of the candidate MPoC Product.

- The determination that they themselves (the candidate MPoC Vendor), and their candidate MPoC Product satisfy all applicable requirements of the *MPoC Standard* and MPoC Program prior to submission for Evaluation, Validation by an MPoC Lab and subsequent Acceptance and Listing by PCI SSC under the MPoC Program.

- Implementing a robust risk-management practice as an integral part of their BAU operational process to support MPoC Program Requirements for maintenance of Acceptance, following initial Acceptance by PCI SSC.

- Maintaining compliance of their MPoC Product with the *MPoC Standard* and MPoC Program Guide version(s) used during the initial Evaluation, and any FAQ or MPoC Program updates, or any other updates which may be applicable while the applicable MPoC Product is on the List of Validated MPoC Products.

- Maintaining Good Standing and adherence to the 3-Year Listing lifecycle of the MPoC Program as described in Section *4 Maintaining Good Standing*.

- Complying with the VRA including Appendix B for any Third Party Product Providers.

- Ensuring that any Third Party Products are integrated into the overall MPoC Product correctly and securely.

- Creating implementation guidance in accordance with the requirements of the *MPoC Standard*.

- Providing their MPoC Product customers with a copy of the applicable implementation guidance.

- Paying all invoices from PCI SSC for MPoC Program fees in a timely fashion.

- Staying up to date with *MPoC Standard* and MPoC Program documents, statements, and guidance on the Website as well as industry trends and best practices.

2.1.1 Use of Third Party Product Providers

As described in the *MPoC Standard*, an MPoC Solution may be entirely managed by an MPoC Solution Provider, or certain services and / or components may be outsourced to one or more Third Party Product Providers (TPP Providers) to perform these functions on behalf of the MPoC Solution Provider.

All TPP Providers that perform functions on behalf of a MPoC Solution Provider must be Evaluated as per applicable *MPoC Standard* test requirements and Appendix B of the VRA.

There are two options for TPP Providers developing software, performing functions on behalf of, or providing services to the MPoC Solution provider to Validate compliance against the *MPoC Standard*:

- Solution components that fit into the MPoC Product types of either an MPoC Software product or MPoC A&M Service may be separately Evaluated against the *MPoC Standard* by an MPoC Lab and (if found compliant to all applicable requirements), Validated, Accepted, and Listed on the PCI SSC website. Or:

- Have the function(s) (i.e. software, functions, services) reviewed during the Evaluation of each candidate MPoC Product.

2.1.2 Use of Payment Device Hardware Vendors

PCI PTS POI devices with an approval class of SCRP (PCI PTS POI SCRP), as well as Non-PTS approved MSR hardware are eligible for secure integration into an MPoC Solution or MPoC Software, as described in the *MPoC Standard*.

PCI PTS POI SCRPs are listed in the PCI PTS Approved Device list on the Website.

Note: MPoC Labs are qualified by PCI SSC to perform Evaluations of optional non-PTS approved MSRs for MPoC Program purposes.

2.2 PCI Recognized Laboratories Qualified as MPoC Labs

PCI Recognized Laboratories, including those qualified to perform Evaluations against the *MPoC Standard* (MPoC Labs), are Listed on the Website. Not all PCI Recognized Laboratories are qualified to perform Evaluations against the *MPoC Standard*. The recognition process is continuous and requires competencies to remain adequate to maintain MPoC Lab recognition.

MPoC Labs are PCI Recognized Laboratories qualified by PCI SSC to perform Evaluations of candidate MPoC Products for Acceptance and Listing on the Website. MPoC Labs are also qualified by PCI SSC to Evaluate existing MPoC Products as part of the MPoC Program's Requirements for maintaining Good Standing (see Sections *3 Acceptance Process* and *4 Maintaining Good Standing*).

MPoC Labs are responsible for:

- Meeting and maintaining the required MPoC Program requirements applicable to MPoC Labs, including but not limited to any associated fees, physical / logical / procedural controls, equipment, skills, and experience necessary to execute all test activities.

- Evaluating candidate or existing MPoC Products in accordance with the *MPoC Standard* and the MPoC Program Guide.

- Providing a determination regarding whether the candidate or existing MPoC Product meets the *MPoC Standard* test requirements.

- Documenting each Evaluation in an Evaluation Report using the applicable reporting template(s) as required by PCI SSC.

- Providing adequate documentation within the applicable reporting template to demonstrate the candidate or existing MPoC Product meets the *MPoC Standard* test requirements.

- Uploading all Evaluation submission requirements to PCI SSC per Appendix A - *Part 7. Submission to PCI SSC – Required Documentation*.

- Determine the type of Evaluation required for any implementation Change as per Section *4.2.3 Implementation Change.*

- Uploading any Change submission requirements to PCI SSC as per Appendix A – *Part 10. Change Documentation*.

- Maintaining an internal quality assurance process for their MPoC Product Evaluation efforts.

- Staying up to date with PCI SSC statements and guidance, industry trends and best practices.

- Satisfying all applicable MPoC Program Requirements at all times.

Note: Candidate and existing MPoC Product compliance with the MPoC Standard is determined solely by the applicable MPoC Lab based upon that MPoC Lab's Evaluation of the MPoC Product, as documented in a corresponding Evaluation Report prepared by that MPoC Lab and submitted to PCI SSC. Entities interested in becoming an MPoC Lab should contact PCI SSC.

2.3 Participating Payment Brands

The Participating Payment Brands independently develop and enforce the various aspects of their respective compliance programs, including but not limited to related requirements, mandates, and due dates.

2.4 PCI Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the PCI SSC standards. In relation to the *MPoC Standard*, PCI SSC:

- Maintains and updates the *MPoC Standard*.

- Qualifies MPoC Labs to Evaluate and Validate MPoC Products for compliance with the *MPoC Standard*.

- Hosts the List including Validated MPoC Products on the Website.

- Hosts the List including Expired MPoC Products on the Website.

- Reviews all MPoC Product *Evaluation Reports* and related Change submissions from MPoC Laboratories to PCI SSC for quality assurance and compliance with baseline quality standards and confirms that:

  – Submissions adequately report the compliance of candidate MPoC Products in their associated submissions.

  – Detail provided in such submissions meets PCI SSC's reporting, documentation, and evidence requirements (i.e. Evaluation Report Template, AOV, VRA).

  – MPoC Product Evaluation is performed against the *MPoC Standard* in accordance with MPoC Program Requirements.

Note: Compliance of a given MPoC Product with the MPoC Standard is determined solely by the applicable MPoC Lab based upon that MPoC Lab's Evaluation of the MPoC Product, as documented in corresponding evidence requirements prepared by that MPoC Lab and submitted to PCI SSC.

3 Acceptance Process

Acceptance eligibility is based on Evaluation and Validation submission evidence submitted by an MPoC Lab to PCI SSC following Evaluation of the candidate MPoC Product, and during an MPoC Product's Listing 3-year lifecycle for maintaining Acceptance.

PCI SSC does not independently confirm the determinations for Acceptance, findings or information contained in submissions to PCI SSC and does not perform any testing or analysis of the corresponding MPoC Products, or related functionality, performance, suitability, or compliance with the *MPoC Standard*.

Listing is the authoritative source of Acceptance and ongoing approval Acceptance of any MPoC Product.

3.1 Self-Assessment

Self-Assessment by a Candidate MPoC Vendor prior to submission to an MPoC Lab is recommended. Submission of reports generated through Self-Assessment as defined in the VRA is not permitted under the MPoC Program. PCI SSC will only accept reports on candidate MPoC Products which have been produced by an MPoC Lab.

If an MPoC Lab is also the candidate MPoC Vendor, Self-assessment by that MPoC Lab is not permitted.

3.2 Contracted Assessment

Any entity pursing Acceptance and Listing of their candidate MPoC Product must have the candidate MPoC Product Evaluated against the *MPoC Standard* by an MPoC Lab, and Validated for compliance with the *MPoC Standard* by the same MPoC Lab, and the supporting evidence submitted to PCI SSC by the same MPoC Lab.

Evaluation

1. The candidate MPoC Vendor contracts with an MPoC Lab to have the MPoC Lab Evaluate the candidate MPoC Product against the *MPoC Standard*. The candidate MPoC Vendor negotiates the fees and any associated confidentiality and non-disclosure agreements with the MPoC Lab. Each new Validation or Re-Validation requires Evaluation against the then-current version(s) of the *MPoC Standard*.

   Evaluation conclusions fall into four categories: Validated, Re-Validated, not-Validated, not-Re-Validated.

   > **Note:** *Before the candidate MPoC Vendor enters a Contracted Assessment agreement with an MPoC Lab, both parties should agree upon the involvement of same MPoC Lab after (and if) initial Acceptance is achieved. It can be beneficial for the MPoC Lab that completes the Evaluation submission to PCI SSC for initial Acceptance, to be the same MPoC Lab to Evaluate post-Acceptance (refer to Section 4 Maintaining Good Standing). Changing MPoC Labs after initial Acceptance and prior to annual checkpoints or during annual checkpoints requires a full Evaluation.*
   >
   > *Former MPoC Products that are Expired are considered candidate (new) MPoC Products and may pursue Evaluation as a candidate MPoC Product. If Acceptance is achieved, the MPoC*

2. The MPoC Vendor provides the MPoC Lab with access and documentation as defined in Appendix A *Part 3. Evaluation - Required Access & Materials*. The MPoC Lab performs an Evaluation of the MPoC Product.

Validation or Re-Validation:

3. Validation or Re-Validation is achieved if the MPoC Lab determines that the candidate MPoC Product or existing MPoC Product complies with the *MPoC Standard*.
The MPoC Lab completes all steps required to finalize the Evaluation Report, including any internal quality assurance steps to confirm the Evaluation Report correctly and sufficiently outlines the Validation of the MPoC Product, and meets all requirements of the MPoC Program and MPoC Lab quality requirements.
The MPoC Lab requests a signed *AOV* from the MPoC Vendor and countersigns the *AOV*.

Submission to PCI SSC:

4. A current VRA for the candidate MPoC Vendor or existing MPoC Vendor is obtained by the MPoC Lab.

5. The MPoC Lab submits the corresponding *Evaluation Report*, supporting documents, countersigned AOV (for each candidate MPoC Product), the MPoC Vendor's signed *VRA*, and any other requested or relevant documentation to PCI SSC through the Portal in accordance with applicable PCI SSC templates, guidance, and instructions.

Review by PCI SSC:

6. PCI SSC issues an invoice to the MPoC Vendor for the applicable Acceptance fee.

7. After the MPoC Vendor pays the invoice, PCI SSC pre-screens the submissions in the Portal to ensure that all required documentation has been included, and the basic submission requirements have been satisfied. Information in the submitted documents must be consistent with the entries in the "Details" fields within the Portal.

8. If the submission is complete, then PCI SSC completes a full review to confirm that the submission meets the MPoC Program eligibility requirements.

9. The Portal is used by PCI SSC and the MPoC Lab to track communications related to a submission, including eligibility questions.

10. If it is determined that the candidate MPoC Product is ineligible for Validation under the MPoC Program, the *Evaluation Report* is rejected. For subsequent reviews, if an *Evaluation Report* requires multiple iterations before PCI SSC accepts the report, each report that the MPoC Lab submits must be redlined to show differences from the original submission and each iteration.

11. If it is determined that the candidate MPoC Product is eligible for Validation under the MPoC Program, PCI SSC conducts a complete review of the *Evaluation Report* and supporting documentation provided or subsequently requested by PCI SSC. PCI SSC identifies issues or questions for resolution by the MPoC Lab. Subsequent MPoC Lab responses and information are reviewed, and the cycle repeats until satisfactory responses have been received, or the submission is rejected or withdrawn. The MPoC Lab should address all comments and feedback in a timely manner.

12. Once PCI SSC has confirmed that the submission meets the MPoC Program Requirements, PCI SSC notifies the MPoC Lab and MPoC Vendor that the MPoC Product has successfully completed the submission process.

Acceptance:

13. PCI SSC countersigns the *AOV* and sends a copy to the MPoC Vendor and the MPoC Lab. The date that PCI SSC countersigns the *AOV* is the initial date of Acceptance, and this date is used to determine any future MPoC Program lifecycle dates, such as annual checkpoints and Re-Validation.

Listing:

14. PCI SCC adds the MPoC Product to the List of Validated MPoC Products on the Website. Listing is the authoritative source of Acceptance status and ongoing approval of any MPoC Product.

Maintaining Acceptance and Listing:

15. Maintenance of Good Standing follows a three-year (36 months) Listing lifecycle. Within the three-year cycle, there are three continual and on-going categories of maintenance activities required of MPoC Vendors to maintain Good Standing status. It is the sole responsibility of the MPoC Vendor to maintain compliance of their MPoC Product.

4　Maintaining Good Standing

Note: *For Expired (or Expiring) Listings, see Section 5 Renewing Expiring Listings and Section 4.1.1 Early Administrative Expiry.*

Upon initial Acceptance, the candidate MPoC Product becomes an MPoC Product (see Section *3 Acceptance Process*). It is the sole responsibility of the MPoC Vendor to maintain compliance of their MPoC Product with the *MPoC Standard* version used for the Evaluation, submission, and initial Acceptance. Failure to do so subjects the Listing to early administrative Expiration. Maintaining Good Standing and adherence to the 3-Year Listing lifecycle is the sole responsibility of the MPoC Vendor.

Maintenance of Good Standing status follows a three-year Listing lifecycle beginning on the date of initial Acceptance. Within the three-year Listing lifecycle, there are three continual and on-going categories of maintenance activities required of MPoC Vendors to maintain Good Standing status as shown in Table 3.

Table 3: Categories of Maintenance Activities

Categories of maintenance activities required of MPoC Vendors during the 3-year Listing lifecycle.
MPoC Program 3-Year Listing Lifecycle (Section *4.1*).
Changes to MPoC Products and Listings (Section *4.2*).
VRA Obligations for (Section *4.3*).

Note: *As described in the VRA, PCI SSC may delist, suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, compliance with remediation requirements) Acceptance and subsequent Listing of any MPoC Product in accordance with applicable MPoC Program Requirements.*

4.1　MPoC Program 3-Year Listing Lifecycle

Good Standing of any MPoC Product follows a 3-Year MPoC Program Listing lifecycle described in Table 4. The MPoC Vendor and their MPoC Product must be reviewed each calendar year by an MPoC Lab for on-going BAU practices as required by the *MPoC Standard*, and subsequently submitted to PCI SSC to maintain Good Standing. Maintaining Good Standing and adherence to the 3-Year Listing lifecycle is the sole responsibility of the MPoC Vendor.

Where a different MPoC Lab is to be used for Validation of any on-going BAU practices (annual checkpoints), Re-Validation is required.

The 3-year MPoC Program Listing lifecycle timeline starts on the initial Acceptance date of the MPoC Product and ends after 3 consecutive calendar years. Initial Acceptance is the date that PCI SSC Accepts the *candidate (new)* MPoC Product as an MPoC Product.

Note: *As described in Appendix A Part 9. Listing Delay. At all times, the Acceptance date of an MPoC Product is the date used to determine any future dates, such as annual checkpoints, and a Listing cannot occur until all subordinate Listings are on the Website.*

Table 4 (on next page) describes the MPoC Program's 3-year Listing lifecycle for MPoC Vendors:

Table 4: MPoC Program 3-Year Listing Lifecycle

During Year 1 of 3
MPoC Vendors should prepare for Annual Checkpoint #1:

To avoid early administrative Expiry (Section *4.1.1*) - Starting on Day 1 (the date of initial Acceptance) – up to 12 Months after initial Acceptance:

The MPoC Vendor adopts the *MPoC Standard* requirements applicable to their MPoC Product as BAU to ensure their MPoC Product remains in compliance with the *MPoC Standard*.

Compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* is BAU and directly aligned with security requirement timeframes as defined in *Table 2. Security Requirement Timeframes* of the *MPoC Standard*.

- No impact Changes are BAU and have supporting evidence as per the *MPoC Standard*. No impact Changes are not reported to the MPoC Lab until the following year (Annual Checkpoint #1).
- Administrative or implementation Changes are reported to the MPoC Lab as follows:
    - Any administrative Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
    - Any implementation Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
- Any implementation Changes that result in previously not-applicable requirements of the *MPoC Standard* becoming applicable after the Change, are adopted as per the *MPoC Standard*.

Compliance with the VRA is BAU.

Annual Checkpoint #1
MPoC Vendors should begin this checkpoint on or before the start of Year 2:

To avoid early administrative Expiry (Section *4.1.1*) - Annual Checkpoint #1 is due on or up to 90 days before the 12 Month anniversary of initial Acceptance.

The previous year's (Year 1) BAU compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* must be Evaluated by the same MPoC Lab that Validated the MPoC Product for initial Acceptance (or else a full Evaluation is required).

The MPoC Vendor must attest and provide to the MPoC Lab for review:

- Confirmation of all No impact Changes that occurred 0-12 Months after initial Acceptance. All No impact Changes are reported to the MPoC Lab.
- Confirmation any administration Changes from 0-12 Months after Initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported administration Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.
- Confirmation any implementation Changes from 0-12 Months after initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported implementation Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.

The MPoC Vendor will permit the MPoC Lab to perform Live Testing of the MPoC Product to ensure that the MPoC Product complies with the *MPoC Standard*.

The MPoC Lab must submit to PCI SSC via the Portal on or up to 90 days before the start of Year 2:

- **VRA**: A copy of the duly executed VRA. The VRA must include Appendix B of the VRA and the VRA must be current and updated to include any Third Party Riders where applicable.
- **AOV**: Updated AOV including any new Third Party Riders, duly executed by both the MPoC Vendor and MPoC Lab.
- **Evaluation Report** and any supporting documentation and evidence as per the MPoC Evaluation Report Template. The Evaluation Report must be Red-lined to clearly indicate any iterations / updates / modifications from the original Evaluation Report that was submitted and resulted in initial Acceptance.

PCI SSC has to review and Accept annual checkpoint submissions. PCI SSC does the following:

- Reviews the submission for completeness.
- When completeness is established, PCI SSC signs and returns a copy of the updated *AOV* to the MPoC Vendor and MPoC Lab.
- Updates the annual checkpoint date on the Website.

During Year 2 of 3
MPoC Vendors should begin to prepare for Annual Checkpoint #2:

To avoid early administrative Expiry (Section *4.1.1*) starting on the 12-month anniversary of initial Acceptance - up to 24 Months after initial Acceptance – the following applies:

Compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* is BAU and directly aligned with security requirement timeframes as defined in *Table 2. Security Requirement Timeframes* of the *MPoC Standard*.

- No impact Changes are BAU and have supporting evidence as per the *MPoC Standard*. No impact Changes are not reported to the MPoC Lab until the following year (Annual Checkpoint #2).
- Administrative or implementation changes are reported to the MPoC Lab as follows:
    - Any Administrative Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
    - Any Implementation Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
- Any implementation Changes that result in previously not-applicable requirements of the *MPoC Standard* becoming applicable after the Change, are adopted as per the *MPoC Standard*.

Compliance with the VRA is BAU.

Annual Checkpoint #2
MPoC Vendors should begin this checkpoint on or before the start of Year 3 of 3:

To avoid early administrative Expiry (Section *4.1.1*) - Annual Checkpoint #2: is due on or up to 90 days before the 24th Month anniversary of initial Acceptance.

The previous year's (Year 2) BAU compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* must be Evaluated for by the same MPoC Lab that Validated the MPoC Product for initial Acceptance (or else a full Evaluation is required).

- The MPoC Vendor must attest and provide to the MPoC Lab for review:
    - Confirmation of all No impact Changes that occurred 12 to 24 Months after initial Acceptance. All No impact Changes are reported to the MPoC Lab.
    - Confirmation any Administration Changes from 12 to 24 Months after Initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported Administration Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.
    - Confirmation any Implementation Changes from 12-24 Months after initial Acceptance were already submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product. Any previously un-reported Implementation Changes that occurred from 0 to 12 months after initial Acceptance are reported to the MPoC Lab.
- The MPoC Vendor will permit the MPoC Lab to perform Live Testing of the MPoC Product to ensure that the MPoC Product complies with the *MPoC Standard*.

The MPoC Lab must submit to PCI SSC via the Portal on or up to 90 days before the start of Year 3:

- **VRA**: A copy of the duly executed VRA. The VRA must include Appendix B of the VRA and the VRA must be current and updated to include any Third Party Riders where applicable.
- **AOV**: Updated AOV including any new Third Party Riders, duly executed by both the MPoC Vendor and MPoC Lab.
- **Evaluation Report** and any supporting documentation and evidence as per the MPoC Evaluation Report Template. The Evaluation Report must be Red-lined to clearly indicate any iterations / updates / modifications from the original Evaluation Report that was submitted and resulted in initial Acceptance.

PCI SSC has to review and Accept annual checkpoint submissions. PCI SSC does the following:

- Reviews the submission for completeness.
- When completeness is established, PCI SSC signs and returns a copy of the updated *AOV* to the MPoC Vendor and MPoC Lab.
- Updates the annual checkpoint date on the Website.

During Year 3 of 3: The final year of the Listing lifecycle
MPoC Vendors should continue to follow MPoC Program Requirements to avoid early administrative Expiry:

To avoid early administrative Expiry (Section *4.1.1*) starting on the 24 month anniversary of initial Acceptance - up to 36 Months after initial Acceptance – the following applies:

Compliance of the MPoC Vendor and their MPoC Product with the *MPoC Standard* is BAU and directly aligned with security requirement timeframes as defined in *Table 2. Security Requirement Timeframes* of the *MPoC Standard*.

- No impact Changes are BAU and have supporting evidence as per the *MPoC Standard*. No impact Changes are not reported to the MPoC Lab until the following year and only if the MPoC Vendor chooses to Re-Validate (Re-Validation).
- Administrative or implementation changes are reported to the MPoC Lab as follows:
    - Any administrative Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
    - Any implementation Changes are submitted to PCI SSC by the same MPoC Lab that Validated the MPoC Product.
- Any implementation Changes that result in previously not-applicable requirements of the *MPoC Standard* becoming applicable after the Change, are adopted as per the *MPoC Standard*.

Compliance with the VRA is BAU.

Note: The MPoC Vendor should begin to plan their business decision to either pursue another 3-Year MPoC Product Acceptance and Listing with PCI SSC (Re-Validation) or permit their MPoC Product to Expire at the end of the 3-Year Listing lifecycle and be moved to PCI SSC's MPoC Product Expired List after at least 180 days past Expiry.

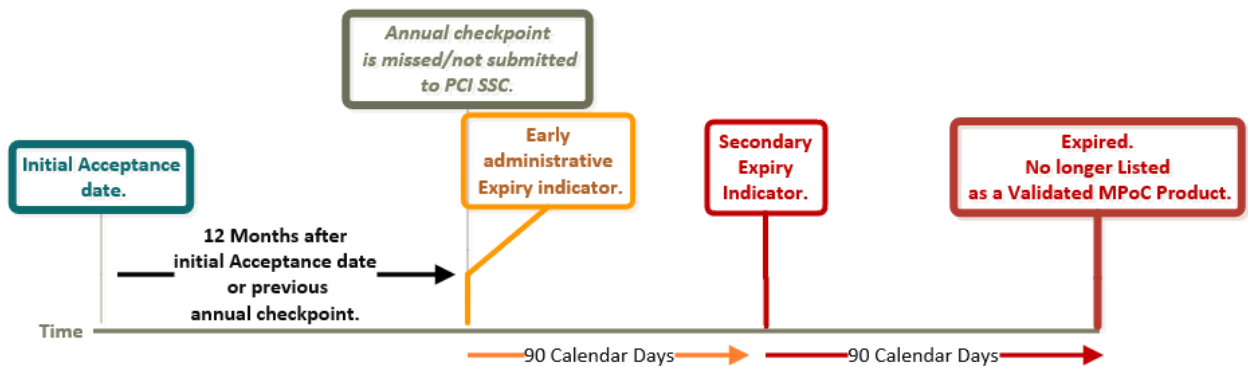| **Re-Validation** |
| :--- |
| **MPoC Vendors should begin Re-Validation before the end of Year 3 of 3:** |

To avoid Expiry, before the 36 month anniversary date since initial Acceptance, a full Evaluation on the existing MPoC Product (Re-Validation) is required to Re-Validate the existing MPoC Product's compliance with the *MPoC Standard*.

Refer to Section 5 *Renewing Expiring Listings*.

4.1.1   *Early Administrative Expiry*

As described in Figure 1, the MPoC Lab must submit the required documentation to PCI SSC through the Portal up to 90 days prior to each annual checkpoint. If PCI SSC does not receive the submission to the Portal on or before the annual checkpoint date, the Listing will be subject to early administrative Expiry as follows:

Figure 1: Early Administrative Expiry

As shown in Figure 1 above, if PCI SSC does not receive the submission on the Portal on or before the annual checkpoint date, an **early administrative Expiry indicator** is applied to the corresponding Listings' annual checkpoint date and any corresponding dependent Listings.

The **Early expiry indicator** remains for up to 90-calendar days past the annual checkpoint date after which a more severe **secondary Expiry indicator** is applied to the corresponding Listings annual checkpoint date and any corresponding dependent Listings for another 90 calendar-days.

After 180 days past the annual checkpoint date, the MPoC Product is no-longer considered an MPoC Product and is indicated as Expired on the Website.

If the annual checkpoint documentation (described in Table 4) is submitted by an MPoC Lab to PCI SSC within 180 days past the annual checkpoint date, PCI SSC does the following:

▪ Reviews the submission for completeness.

▪ When completeness is established, PCI SSC signs and returns a copy of the updated *AOV* to the MPoC Vendor and MPoC Lab.

▪ Removes the indicator(s) from the Listing and any dependent Listings.

▪ Updates the annual checkpoint date on the Website.

If the annual checkpoint documentation (described in Table 4) is not submitted by an MPoC Lab to PCI SSC within 180 days past the annual checkpoint date, PCI SSC does the following:

▪ The corresponding Listing is indicated as Expired on the Website, also known as the MPoC Product Expired List, and any dependent Listings are updated to reflect their MPoC Product's dependency on an Expired MPoC Product. (In some cases, if a dependent MPoC Product solely relies on an Expired MPoC Product, then it may affect the dependent MPoC Vendor's ability to meet MPoC Program Requirements.) The former MPoC Product that is now Expired, will remain on the Website indicated as Expired. If the former MPoC Vendor wants to restore an Expired MPoC Product to Good Standing, they must pursue Evaluation as an entirely new MPoC Vendor and MPoC Product (not Re-Validation) of the candidate MPoC Product and the former Expired MPoC Product will remain Expired on the Website.

4.2   Changes to MPoC Products and Listings

Changes to MPoC Products vary considerably across the spectrum of minimum to critical security impact to the MPoC Product and dependencies on that MPoC Product. (An example of a dependency may be if an MPoC A&M Service is Changed, and that same MPoC A&M Service is a Third Party Product integrated into an MPoC Software Product by an MPoC Software Vendor).

MPoC Vendors may Change Listed MPoC Products for various reasons: Changes do not impact the initial Acceptance date of the MPoC Product or any dependent MPoC Products.

Sometimes there is no impact, and no change to the MPoC Product at all, and instead there is a requested administrative update to the Listing details on the Website. The MPoC Program considers the objective nature of the *MPoC Standard* and the various types of Changes and impact of Changes to the compliance of the MPoC Product and dependencies with *MPoC Standard*.

As per the VRA (A.11) the MPoC Vendor shall promptly notify PCI SSC of change(s) to an MPoC Product in accordance with this MPoC Program (see Table 5 below for changes that require notification). As defined in Table 2 of the *MPoC Standard*, significant changes are changes that have potential impacts on the security of the solution. **Significant changes as described in the *MPoC Standard* are considered implementation Changes under the MPoC Program**.

PCI SSC reserves the right to reject any Change submission if it determines that the Change is ineligible.

Note: All Changes are permissible only for MPoC Products that have not Expired.

Table 5 (on next page) describes the MPoC Product and Listing Change types.

Table 5: Changes to MPoC Products and Listings

Change Type	Description	Action by the MPoC Vendor	Action by the MPoC Lab
No Impact Change	• Does not impact the MPoC Product's compliance with the *MPoC Standard*, and • Does not impact the corresponding Listing. Examples of no impact Changes include, but are not limited to, maintenance patches which do not change functionality, or routine key rotation. For details, see Section *4.2.1 No Impact Change*.	• Not reported at the time of the Change. • Reported as part of the MPoC Program annual requirements. See Section *4.1*.	The MPoC Lab reviews no impact Change(s) as part of each annual Checkpoint described in Section *4 Maintaining Good* Standing.
Administrative Change	• Does not impact the MPoC Product's compliance with the *MPoC Standard*, and • Impacts only 'administrative information' associated with the MPoC Product as documented in the corresponding MPoC Product Listing on the Website. For details, see Section *4.2.2 Administrative Change*.	• The MPoC Vendor must report the administrative Change to the same MPoC Lab that performed the original MPoC Product Evaluation, changing MPoC Labs requires a full Evaluation of the MPoC Product. • The MPoC Vendor contacts the MPoC Lab that performed the last complete and full MPoC Product Evaluation and reports the administrative Change (as soon as possible) to the MPoC Lab per Section *4.2.2 Administrative Change*.	The MPoC Lab reviews the administrative Change. If the MPoC Lab agrees that the Change is administrative, then the Lab submits the Change to PCI SSC per Section *4.2.2 Administrative Change*.
Implementation Change	An implementation Change: • Impacts the MPoC Product's Listing details and is not a 'no impact Change' or an 'administrative Change', or • Impacts the MPoC Product's compliance with the *MPoC Standard* or the security of the MPoC Product by making alterations to the intended function of the MPoC Product. This may be the case even if the impact does not require any Change to the MPoC Product Listing's details. For details, see Section *4.2.3 Implementation Change*.	The MPoC Vendor contacts the MPoC Lab that performed the last full MPoC Product Evaluation and requests an Evaluation (case-by-case) of the implementation Change as per Section *4.2.3 Implementation Change*. Changing MPoC Labs requires a full Evaluation of the MPoC Product.	On a case-to-case basis, the MPoC Lab works with the MPoC Vendor to determine the impact that the Change has before determining the type of Evaluation required. There are two types of Evaluations that apply to MPoC Product implementation Changes per Section *4.2.3 Implementation Change*.

4.2.1 No Impact Change

No impact Changes address situations where an MPoC Vendor must apply Changes to their MPoC Product as part of BAU activities to maintain compliance with security requirement timeframes as defined in *Table 2. Security Requirement Timeframes* of the *MPoC Standard*.

Examples of this type of Changes include activities to maintain MPoC Product security and/or rectify errors and faults in software (without modifying functionality), such as addressing vulnerabilities and penetration testing findings, or cryptographic key rotation when the end of the cryptoperiod is reached.

Note: Any changes that remove, modify or add functionality are considered implementation Changes.

It is important to note that no impact Changes do not override VRA obligations for reporting (4.3). For example, in the *MPoC Standard Table 2. Security Requirement Timeframes*, any Timeframes with "Immediately" or "Promptly".

Any no impact Changes made must be recorded so that they can be reviewed and Validated during the next Annual Checkpoint or Re-Validation.

4.2.2 Administrative Change

Administrative Changes are limited to updates where no Changes to a Listed MPoC Product have occurred, but the MPoC Vendor requests a Change to the way that the MPoC Product is Listed on the Website. Examples of administrative Changes include, but are not limited to:

▪ Corporate identity changes.
▪ Changes to Listing details that are not changes to the underlying MPoC Product, or components, or elements as described in *Part 1. MPoC Program Eligibility*

For details about the content of the Change analysis, see *Part 10. Change Documentation*.

The MPoC Vendor prepares a Change analysis using the Change Impact Template (available on the Website) and submits it to the MPoC Lab for review.

Note: The MPoC Vendor should submit the Change analysis to the same MPoC Lab that performed the original MPoC Product Evaluation - changing MPoC Labs requires a full Evaluation of the MPoC Product.

If the MPoC Lab does not agree that the Change is eligible as an administrative Change, the MPoC Lab works with the MPoC Vendor to resolve the disagreement.

If the MPoC Lab agrees that the Change is eligible as an administrative Change. The MPoC Lab notifies the MPoC Vendor that the Change is eligible.

The MPoC Vendor prepares the Change documentation (*Part 10. Change Documentation*), signs the corresponding *AOV*, and sends the documentation to the MPoC Lab.

If applicable, the MPoC Vendor completes a new *VRA*.

The MPoC Lab completes the Change documentation.

The MPoC Lab signs its concurrence on the *AOV* and forwards it, the Change documentation, and a new *VRA* (if applicable) to PCI SSC.

PCI SSC sends the Change fee invoice to the MPoC Vendor.

Upon payment of the invoice, PCI SSC reviews the submission.

Following a successful PCI SSC review of the Change, PCI SSC:

- Updates the corresponding List of Validated MPoC Products on the Website accordingly with the new information.
- Signs and returns a copy of the corresponding *AOV* to the MPoC Vendor and the MPoC Lab. The Re-Validation date of the updated Listing remains the same.

Should there be quality issues with any part of the submission, PCI SSC communicates them to the MPoC Lab. PCI SSC reserves the right to reject any Change submission if it determines that the Change is ineligible.

4.2.3   Implementation Change

An implementation Change is any variation to a MPoC Product or MPoC Product Listing that is not an administrative Change or a no impact Change. On a case-by-case basis, the MPoC Lab determines the type of Evaluation required for the implementation Change.

For example, adding an MPoC Application under an MPoC Solution or MPoC Software Product is an implementation Change.

MPoC Vendors should contact the MPoC Lab that performed the last full MPoC Product Evaluation for guidance. The MPoC Lab engaged by the MPoC Vendor for this purpose then determines whether a partial Evaluation or full Evaluation is required to maintain Good Standing and Listing of the MPoC Product eligible for the implementation Change. Since the number of possible implementation Changes and their impact cannot be determined in advance, the type of Evaluation must be considered on a case-by-case basis.

- Any implementation Change that requires a full Evaluation does not classify the changed MPoC Product as a new MPoC Product or new Listing, and therefore, does not reset the annual checkpoint dates or Re-Validation date (see Section *4 Maintaining Good Standing*).

The MPoC Vendor prepares a Change analysis using the Change Impact Template (available on the Website) and submits it to the MPoC Lab for review. For details about the content of the Change analysis, see *Part 10. Change Documentation*.

Note: The MPoC Vendor should submit the Change analysis to the same MPoC Lab that performed the original MPoC Product Evaluation - changing MPoC Labs requires full Evaluation.

If the MPoC Lab does not agree that the Change is eligible as an implementation Change, the MPoC Lab works with the MPoC Vendor to resolve the disagreement.

If the MPoC Lab agrees that the Change is eligible as an implementation Change. The MPoC Lab notifies the MPoC Vendor that the Change is eligible.

There are two types of Evaluations that apply to MPoC Product implementation Changes:

- A full (complete) MPoC Product Evaluation is required when:
  - Compliance of the Changed MPoC Product against the *MPoC Standard* can only be proven by a full MPoC Product Evaluation as determined by the MPoC Lab (See Appendix A – *Part 10. Change Documentation*).
- A partial MPoC Product Evaluation is allowed when:
  - Compliance of the Changed MPoC Product against the *MPoC Standard* can be proven by a partial MPoC Product Evaluation as determined by the MPoC Lab (See Appendix A – *Part 10. Change Documentation*).

The MPoC Vendor prepares the Change documentation (*Part 10. Change Documentation*), signs the corresponding *AOV*, and sends the documentation to the MPoC Lab.

If applicable, the MPoC Vendor completes a new *VRA*.

The MPoC Lab completes the Change documentation.

The MPoC Lab signs its concurrence on the *AOV* and forwards it, the Change documentation, and a new *VRA* (if applicable) to PCI SSC.

PCI SSC sends the Change fee invoice to the MPoC Vendor.

Upon payment of the invoice, PCI SSC reviews the submission.

Following a successful PCI SSC review of the Change, PCI SSC:

▪ Updates the corresponding List of Validated MPoC Products on the Website accordingly with the new information.

▪ Signs and returns a copy of the corresponding *AOV* to the MPoC Vendor and the MPoC Lab. The Re-Validation date of the updated Listing remains the same.

Note: Should there be quality issues with any part of the submission, PCI SSC communicates them to the MPoC Lab. PCI SSC reserves the right to reject any submission if it determines that an implementation Change is ineligible for the type of Evaluation performed by the MPoC Lab.
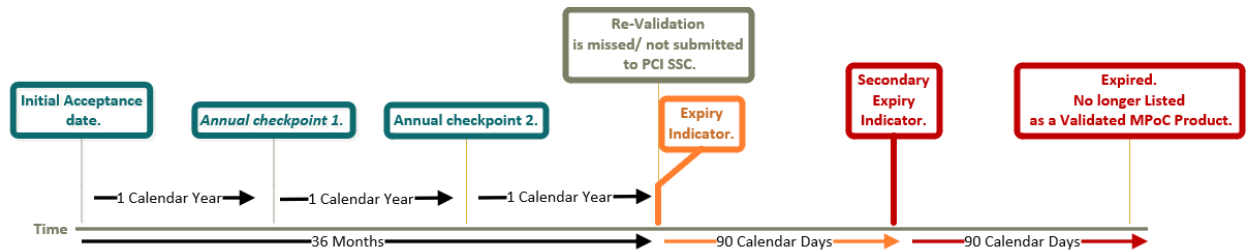
4.3 VRA Obligations for Notification

MPoC Vendors and TPP Providers must adhere to their obligations under the *VRA* at all times. Without limiting the foregoing, it is important to note that in the event of a Security Issue or Unique Security Issue (as defined in the *VRA*) relating to an MPoC Product or MPoC Vendor, or TPP Provider, the *VRA* requires the MPoC Vendor to notify PCI SSC.

5 Renewing Expiring Listings

The Re-Validation date (Expiry date) for an MPoC Product that is in Good Standing is the 36 month anniversary date since initial Acceptance of the MPoC Product. MPoC Products that are not Re-Validated on or before the Re-Validation date are not in Good Standing and are Expired after 180 calendar days as shown in in Figure 2, and described below.

Figure 2: Expiry

As an MPoC Product Listing approaches its Re-Validation date (Expiry date), two options are available to the MPoC Vendor:

▪ **Re-Validation**: If the MPoC Vendor wants the MPoC Product to remain in Good Standing all of the following must be completed before the Re-Validation date:

– The MPoC Vendor must engage an MPoC Lab to perform Re-Validation.

– The MPoC Lab Evaluates the MPoC Product against the current *MPoC Standard*, and if Re-Validation is achieved, submits results to PCI SSC for Acceptance.

– PCI SSC reviews and Accepts the Evaluation Report and Lists the MPoC Product on the Website.

Subject to the successful and timely completion of the above process, the resulting MPoC Product Listing has a new initial Acceptance date. Re-Validation requires a full Evaluation and follows the same process as the original MPoC Product Evaluation. (Refer to Section to Section *3 Acceptance Process*)*.* Where a new reference number is applied, any dependent Listings are also updated to reflect the new reference number.

▪ **Expiry**: An MPoC Product Listing for which Re-Validation and subsequent Acceptance by PCI SSC has not occurred on or before the Re-Validation date, will have an **Expiry indicator** applied to the Listing on the Website, and an indicator will also be applied to any dependent Listings for the first 90 days past expiry. The **Expiry indicator** remains for **up to 90-calendar days past the Re-Validation date** after which a more severe **secondary Expiry indicator** is applied to the corresponding Listings annual checkpoint date and any corresponding dependent Listings for another 90 calendar-days.

The Expired indicator will denote the MPoC Product's Re-Validation requirements as per MPoC Program Requirements is less than 180 days *past* the Re-Validation date. Any dependent MPoC Product Listings will also have an indicator to denote the dependent MPoC Product(s) integrate an MPoC Product that is a TPP (Third Party Product), and the TPP is less than 180 days past Expiry. (Refer to Section *2.1.1 Use of Third Party Product Providers*)

– If the MPoC Product undergoes Re-Validation and the submittal is received and Accepted by PCI SSC within 180-days past the Re-Validate date, a new initial Acceptance date applies to the MPoC Product, the 3-Year Listing lifecycle is reset, and the Expiry indicator is removed from the MPoC Product Listing. Dependent Listings are also updated.

– If the MPoC Product is not Re-Validated within 180-days past the Expiry date and submitted to PCI SSC within 180 days past the Expiry date, the corresponding Listing is indicated as Expired on the Website, also known as the MPoC Product Expired List, and any dependent Listings are updated to reflect their MPoC Product's dependency on an Expired MPoC Product. (In some cases, if a dependent MPoC Product solely relies on an Expired MPoC Product, then it may affect the dependent MPoC Vendor's ability to meet MPoC Program Requirements.) The former MPoC Product that is now Expired, will remain on the Website indicated as Expired. If the former MPoC Vendor wants to restore an Expired MPoC Product to Good Standing, they must pursue Evaluation as an entirely new MPoC Vendor and MPoC Product (not Re-Validation) of the candidate MPoC Product and the former Expired MPoC Product will remain Expired on the Website.

6 MPoC Program Fees

All MPoC Program fees are posted on the PCI SSC Website. MPoC Program fees are non-refundable and subject to change upon posting of revised fees on the Website. All such fees are payable directly to PCI SSC. PCI SSC bills the MPoC Vendor for all such fees – with the exception of any fees related to MPoC Lab management, or report submittal and review, which are billed to the MPoC Lab.

All MPoC Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

Note: All Evaluation-related fees are payable directly to the MPoC Lab, and are negotiated between the MPoC Lab and its customers per Section 3 Acceptance Process.

6.1 Initial Acceptance Fees

Prior to initial Acceptance of a candidate MPoC Product as a MPoC Product, the candidate MPoC Vendor must pay the applicable Acceptance fee to PCI SSC. For more information on the initial Acceptance process for candidate MPoC Products, see Section *3 Acceptance Process*.

6.2 Change Fees

To Accept and List a Change, a MPoC Product must already be Listed and not have reached the Re-Validation date (Expiry date). Prior to Acceptance of administrative or implementation Changes (Section *4.2*) to an MPoC Product, the MPoC Vendor must pay the applicable Change fee to PCI SSC. There are no fees for no impact Changes. No impact Changes are reported as part of the MPoC Program annual requirements (see Section *4.1 MPoC Program*). For more information on the Change process for MPoC Products, see Section *4 Maintaining Good Standing*.

Appendix A   MPoC Program Details

The following provides an overview of prerequisite considerations including eligibility considerations and other MPoC Program details.

Part 1. MPoC Program Eligibility

This section covers the factors affecting the eligibility and processes involved for different types of candidate MPoC Products.

Figure 3: MPoC Program Eligibility Considerations for Candidate MPoC Solutions

Figure 3 provides high-level eligibility considerations for candidate MPoC Solution Providers that pursue development of an MPoC Solution with one or more MPoC Applications.

Figure 4: MPoC Program Eligibility Considerations for Candidate MPoC Software

Figure 4 provides high level eligibility considerations for candidate MPoC Software Vendors that pursue development of MPoC Software Product(s) that offer MPoC SDK(s) and / or MPoC Application(s).

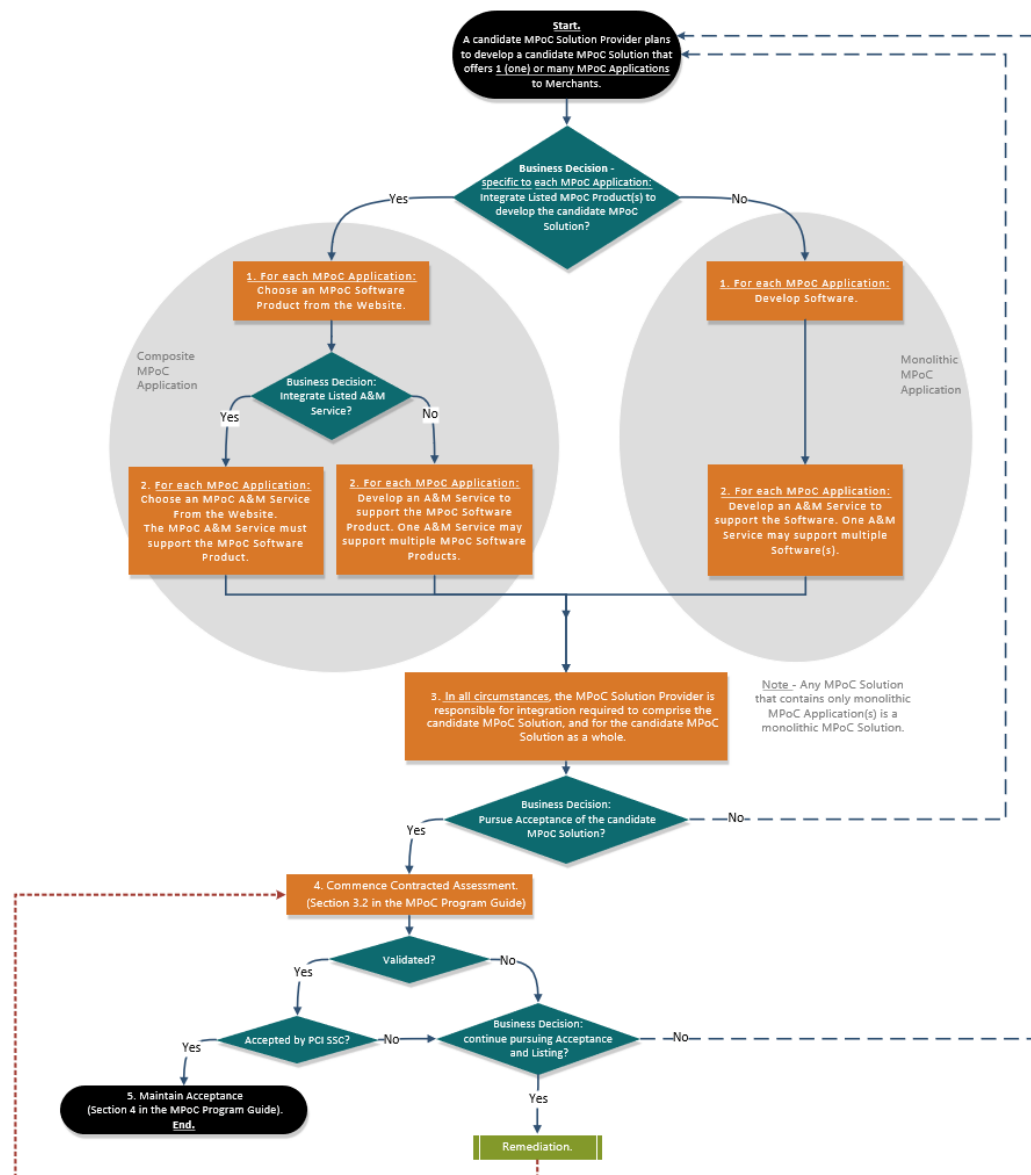## Figure 5: MPoC Program Eligibility Considerations for Candidate MPoC A&M Services
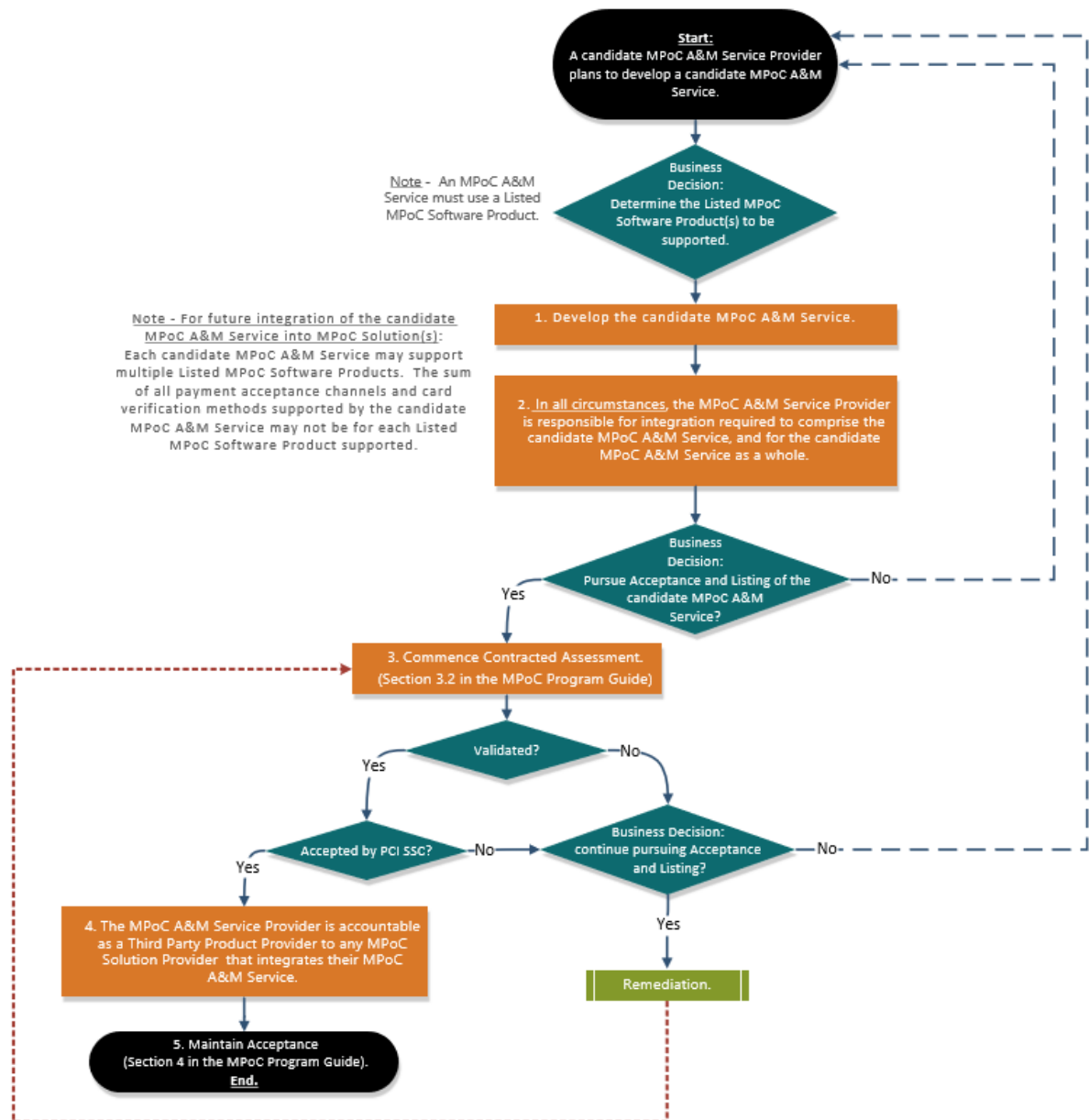

Figure 5 provides high-level eligibility considerations for candidate MPoC A&M Service Providers that pursue development of MPoC A&M Service offerings.

Table 6 describes the requirements and eligibility for the various components used in MPoC Products.

Table 6: MPoC Program Eligibility

MPoC Product	Eligibility

MPoC Solution	Each MPoC Solution must be merchant-attended. Unattended MPoC Solutions are not eligible for the MPoC Program.
	
	Each MPoC Solution must have at least one merchant-facing MPoC Application bound to (Evaluated as part of) the MPoC Solution. Each MPoC Application may be developed as monolithic or composite-based:
	
	• Monolithic Application Development:
	  – Each MPoC Application must be developed without integration of a Listed MPoC Software Product and without integration of a Listed MPoC A&M Service.
	  – Monolithic MPoC Applications that integrate MPoC A&M Services are not eligible for the MPoC Program.
	• Composite Development: The MPoC Application is developed via integration of a Listed MPoC Software Product and integration of either a Listed MPoC A&M Service, or the candidate MPoC Solution Provider may develop their own A&M Service.
	
	Each MPoC Application may support:
	• Offline payment transactions.
	• Multiple platforms and operating system versions.
	• The following payment acceptance channels:
	  – Manual PAN entry,
	  – COTS-native contactless interface,
	  – PCI PTS POI SCRP devices for chip-based contact, contactless, and MSR-based transactions,
	  – MSR devices Validated through the MSR appendix of the *MPoC Standard*.
	And cardholder verification methods:
	  – COTS-native PIN entry,
	  – No CVM,
	  – CDCVM.
	
	An MPoC Solution must have at least one MPoC Application(s) bound to the MPoC Solution. Each MPoC Application may support different platforms, operating system versions, payment acceptance channels, and cardholder verification methods.
	
	In all circumstances, the MPoC Solution Provider is responsible for integration required to comprise the candidate MPoC Solution, and for the candidate MPoC Solution as a whole.
	
	Note*: MPoC Applications are bound to the MPoC Solution (or MPoC Software) and are not supported by the MPoC Standard for standalone Evaluation, Validation, Acceptance and Listing on the Website.*

MPoC Product	Eligibility
MPoC Software	The MPoC Software is considered as two separate parts – the MPoC SDK (intended for integration into an MPoC Application) or complete MPoC Application itself, and the back-end software including the Attestation and Monitoring Software. Each MPoC Software product may be developed as: • An MPoC SDK. • An MPoC Application. *Note*: *MPoC Applications are bound to the MPoC Software (or MPoC Solution) and are not supported by the MPoC Standard for standalone Evaluation, Validation, Acceptance and Listing on the Website.* Each MPoC Software Product may have Evaluated and Listed: • One or more MPoC SDK's, each isolated or non-isolated. • One or more MPoC Applications, and each MPoC Application comprised of maximum two MPoC SDK's (the MPoC SDK's must be developed by the same MPoC Software Vendor and cannot be MPoC SDK's Listed by a different MPoC Software Vendor). Each MPoC Software Product may support: • Offline payment transactions. • Multiple platforms and operating system versions. • The following payment acceptance channels: – Manual PAN entry, – COTS-native contactless interface, – PCI PTS POI SCRP devices for chip-based contact, contactless, and MSR-based transactions, – MSR devices Validated through the MSR appendix of the *MPoC Standard*. And cardholder verification methods: – COTS-native PIN entry, – No CVM, – CDCVM. In all circumstances, the MPoC Software Vendor is responsible for integration required to comprise the candidate MPoC Software, and for the candidate MPoC Software Product as a whole. The MPoC Software Vendor is accountable as a Third Party Product Provider to any MPoC Solution Provider(s) and / or any MPoC A&M Service Provider(s) that integrate their MPoC Software Product(s).

MPoC Product	Eligibility
MPoC A&M Service	MPoC A&M Service is intended for integration into an MPoC Application (and MPoC Applications are bound to an MPoC Solution). An MPoC A&M Service must support at least one or more Listed MPoC Software Product(s). Candidate MPoC A&M Services that do not support MPoC Software Product(s) are not eligible for the MPoC Program. Candidate MPoC A&M Services that support one or more monolithic MPoC Application(s) are not eligible for the MPoC Program. The MPoC A&M Service may support multiple payment acceptance channels and card verification methods as determined by the MPoC Software Products supported. The sum of all payment acceptance channels, and card verification methods supported by the candidate MPoC A&M Service may not be for each Listed MPoC Software Product supported. In all circumstances, the MPoC A&M Service Provider is responsible for integration required to comprise the candidate MPoC A&M Service, and for the candidate MPoC A&M Service as a whole. The MPoC A&M Service Provider is accountable as a Third Party Product Provider to any MPoC Solution Provider(s) that integrates their MPoC A&M Service(s).

Part 2. Evaluation - Preparation & Guidance

It is the responsibility of the candidate MPoC Vendor to contact an MPoC Lab and enter into a contractual agreement with the MPoC Lab to Evaluate the candidate MPoC Product (see Section *2 Roles and Responsibilities*).

Before Evaluation, and if desired by the candidate MPoC Vendor, the MPoC Lab may perform a pre-Evaluation or gap analysis of a candidate MPoC Product. If the MPoC Lab notes deficiencies that would prevent a compliant result, the MPoC Lab may provide a list of deficiencies to the candidate MPoC Vendor to be addressed before the formal Evaluation begins.

Before starting an MPoC Product Evaluation, all MPoC Vendors (as detailed in Section *2.1*) and Entities involved (as detailed in Section *2 Roles and Responsibilities*) are encouraged to take the following preparatory actions:

1. Review the *MPoC Standard* and all related publications (Section *1.1*).
2. Determine the candidate MPoC Product and candidate MPoC Vendor readiness to comply with the *MPoC Standard*:
   a. Select the appropriate *MPoC Evaluation Report Template* (available on the MPoC Lab Portal).
   b. Perform a gap analysis between the MPoC Product and the *MPoC Standard*.
   c. Correct any gaps.

Part 3. Evaluation - Required Access & Materials

As per the *MPoC Standard*, documentation and samples required for the Evaluation of the MPoC Product or candidate MPoC Product should be agreed upon between the MPoC Vendor or candidate MPoC Vendor and the MPoC Lab.

The MPoC Vendor must provide sufficient evidence to enable an MPoC Lab to Validate the MPoC Product against the *MPoC Standard*.

Any evidence must clearly and concisely show that the security controls implemented by the MPoC Vendor conform to the *MPoC Standard*.

The MPoC Vendor must deliver all completed MPoC Product Evaluation-related materials to the MPoC Lab performing the Evaluation, not to PCI SSC.

Part 4. Evaluation and Review Time Considerations

The amount of time and effort necessary for an MPoC Lab to Evaluate and Validate a candidate MPoC Product, and the amount of time for an MPoC Product to achieve Acceptance (if eligible as determined by PCI SSC), can vary significantly depending on factors, such as:

- The number and types of gaps that the candidate MPoC Product has with the *MPoC Standard,* as determined by the MPoC Lab during the Evaluation. See Part 2 Evaluation – Preparation & Guidance.

- Prompt and comprehensive submission of all Validation artifacts to the MPoC Lab.

- Prompt payment of fees to PCI SSC upon submission. See Section 6 Program Fees.

- Appropriate agreements are in place with any MPoC Vendors or other TPP Providers of the candidate MPoC Solution or Product to ensure proper information disclosure, if required under the *VRA*. See Section *2 Roles and Responsibilities*).

- Quality of the required documentation provided by the candidate MPoC Vendor to the MPoC Lab. See *Part 3. Evaluation - Required Access & Materials*.

- During the Evaluation, questions from the MPoC Lab that need to be addressed by the MPoC Vendor. See *Part 5. Technical Support Throughout Evaluation and Review*.

- Quality of the submission by the MPoC Lab to PCI SSC. See *Part 7. Submission to PCI SSC – Required Documentation*.

Any Evaluation, Validation, and Acceptance schedules that the MPoC Lab or PCI SSC provides to the MPoC Vendor should be considered estimates. The MPoC Lab may base the Evaluation completion date on the assumption that the candidate MPoC Product will meet all applicable *MPoC Standard* requirements without remediation and / or additional cycles of review. If problems arise during the review or Acceptance process, discussions between the MPoC Lab (on behalf of the MPoC Vendor) and PCI SSC may delay or prematurely end the Evaluation. For example, an Evaluation may end if the candidate MPoC Vendor decides not to make the changes necessary to achieve compliance. Any back-end monitoring environment assessments may require additional time—the MPoC Vendor should consider this when planning the Evaluation schedule.

Part 5. Technical Support Throughout Evaluation and Review

It is the responsibility of the MPoC Vendor to contact a MPoC Lab and enter into a contractual agreement with the MPoC Lab to Evaluate the candidate MPoC Product (see Section *2 Roles and Responsibilities*). The contractual agreement should address any potential support needs required by the MPoC Lab from the MPoC Vendor, including but not limited to:

- During the Evaluation, questions may arise from the MPoC Lab that need to be addressed by the MPoC Vendor. It is recommended that the contractual agreement between the MPoC Lab and the MPoC Vendor include availability of an MPoC Vendor technical representative to discuss and respond to questions from the MPoC Lab in a timely manner. See *Part 4. Evaluation and Review Time Considerations*.

- After submission to PCI SSC for review, questions may arise from PCI SSC that need to be addressed by the MPoC Lab on behalf of the MPoC Vendor. It is recommended the contractual agreement between the MPoC Lab and the MPoC Vendor include availability of a MPoC Vendor technical representative to discuss and respond to questions from PCI SSC directed to the MPoC Lab. See *Part 4. Evaluation and Review Time Considerations*.

Part 6. Vendor Release Agreement (VRA)

For any candidate MPoC Solution or MPoC Product to be reviewed by PCI SSC, PCI SSC must have the MPoC Vendor's signed copy of the then-current version of the *VRA*. The VRA is available on the Website. See *Part 7. Submission to PCI SSC – Required Documentation*.

Among other things, the *VRA*:

- Covers confidentiality issues.
- Covers the candidate MPoC Vendor's agreement to the MPoC Program Requirements, policies, and procedures.
- Gives permission to the MPoC Lab to release Evaluation Reports and other related materials to PCI SSC for review.
- Requires MPoC Vendors to adopt and comply with industry-standard vulnerability handling policies.
- Ensures MPoC Vendors have all necessary rights and permissions to disclose information regarding TPP Providers.

For PCI SSC to review an MPoC *Evaluation Report*, PCI SSC must have received the MPoC Vendor's signed copy of the then-current *VRA* from the MPoC Lab. At the time of the submission of any MPoC *Evaluation Report* to PCI SSC:

- If PCI SSC does not already have the MPoC Vendor's signed copy of the then-current *VRA*, the MPoC Lab must provide the MPoC Vendor's signed copy of the then-current VRA to PCI SSC with the *Evaluation Report*.
- If PCI SSC has the MPoC Vendor's signed copy of the then-current *VRA*, the MPoC Lab is not required to re-submit the same *VRA* to PCI SSC at that time.

Part 7. Submission to PCI SSC – Required Documentation

Following an Evaluation or Re-Validation, the MPoC Lab uploads the submission to the Portal (see Section *3 Acceptance Process*).

The submission to the Portal must include:

- **VRA**: A copy of the duly executed then current VRA from the Website. The VRA must include Appendix B of the VRA and the VRA must be current and updated to include any Third Party Riders where applicable.
- **AOV**: Updated AOV including any new Third Party Riders, duly executed by both the MPoC Vendor and MPoC Lab.
- Evaluation Report and any supporting documentation and evidence as per the MPoC Evaluation Report Template. The Evaluation Report must be Red-lined to clearly indicate any iterations / updates / modifications based on questions from the report reviewers.

Part 8. Acceptance

Acceptance of a given MPoC Product by PCI SSC applies only to the specific MPoC Product that has been Validated by an MPoC Lab and subsequently determined eligible and Accepted by PCI SSC. If any aspect of an MPoC Product is different from what was Validated by the MPoC Lab and Accepted by PCI SSC—even if the different MPoC Product conforms to the basic product description of the Accepted MPoC Product —the alternate MPoC Product should not be considered Accepted or promoted as such by PCI SSC.

No MPoC Vendor or Third Party Product Provider may refer to an MPoC Product as "PCI Approved," "PCI SSC Approved", or otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of an MPoC Vendor or its MPoC Solution, MPoC Software Product, or MPoC A&M Service, except to the extent and subject to the terms and restrictions expressly set forth in the *VRA*, or in a countersigned *AOV* provided by PCI SSC. All other references to PCI SSC's acceptance of an MPoC Solution, MPoC Software Product, or MPoC A&M Service are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC Acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals. However, such Acceptance does not under any circumstances include or imply any endorsement or warranty regarding the applicable MPoC Vendor or the functionality, quality, or performance of the MPoC Product or any other product or service. PCI SSC does not warrant any products or services provided by Third Party Product Providers. PCI SSC Acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received Acceptance from PCI SSC shall be provided by the party providing such products or services, and not by PCI SSC or any Participating Payment Brand.

Part 9. Listing Delay

Vendors may choose to delay Listing a newly Accepted MPoC Product for up to a maximum of six months. Written notification to PCI SSC must be submitted through the MPoC Lab along with the *Evaluation Report*. In addition, the MPoC Lab must provide details as part of the submission indicating the duration of time that the MPoC Product Listing should be withheld.

A delayed Listing may include other PCI Listed items which are currently part of a separate delayed Listing. For example, an MPoC Solution Listing that implements an PCI PTS POI SCRP which has its Listing already delayed may be requested to be part of a separate delayed Listing. At all times, the Acceptance date of an MPoC Product is the date used to determine any future dates, such as annual checkpoints and Re-Validation, and a Listing cannot occur until all subordinate Listings are on the Website.

Part 10. Change Documentation

Table 7: Change Documentation

No Impact Changes	Administrative Changes	Implementation Changes
• Reported as part of the *MPoC Program Annual Requirements*. See Section *4.1 MPoC Program*	• *MPoC Product Attestation of Validation* (AOV) • *Change Impact* document [1] • Current *VRA* [2]	• *Change Impact* document [3] • Evidence of 3.1 as per the *MPoC Standard* and A.1.3.2 as per the *MPoC Standard*: The documented risk-assessment process is performed at least annually and upon significant changes and must address why partial Evaluation or Re-Validation is sufficient. • **VRA**: A copy of the duly executed VRA. The VRA must include Appendix B of the VRA and the VRA must be current and updated to include any Third Party Riders where applicable. • **AOV**: Updated AOV including any new Third Party Riders, duly executed by both the MPoC Vendor and MPoC Lab. • **Evaluation Report** and any supporting documentation and evidence as per the MPoC Evaluation Report Template. The Evaluation Report must be Red-lined to clearly indicate any iterations / updates / modifications from the original Evaluation Report that was submitted and resulted in initial Acceptance.

---

[1] The *Change Impact* template published on the Website is mandatory for the MPoC Lab when submitting Changes to PCI SSC on behalf of an MPoC Vendor.
[2] If applicable.
[3] The *Change Impact* template published on the Website is mandatory for the MPoC Lab when submitting Changes to PCI SSC on behalf of an MPoC Vendor.

Appendix B Elements for the List of Validated MPoC Solutions

Described in this Appendix are the Listing details available on the Website for MPoC Product type: MPoC Solution.

MPoC Solution Listing – Data Elements

Table 8 describes the MPoC Solution Listing fields, descriptions, and notes. MPoC Solution Listings are presented on the Website to include the sum of all functionalities that are available under that MPoC Solution.

Table 8: MPoC Solution Listing fields on the Website.

Field		Description	Notes
MPoC Solution Provider		The MPoC Solution Provider's company name.	The MPoC Solution name cannot be the same as the MPoC Solution Providers' name.
MPoC Solution Identifier	MPoC Solution	The name of the MPoC Solution under which the MPoC Solution is marketed. Provided by the MPoC Solution Provider.	
	Solution Details	Details of MPoC Application(s) Evaluated.	Every MPoC Solution will have at least 1 MPoC Application denoted under Solution Details. MPoC Solution Listings will inherit the indicator of any PCI SSC Listed dependencies or MPoC Applications to denote the MPoC Solution is dependent on MPoC Product, MPoC Application, or PCI PTS POI SCRP that is not in Good Standing with PCI SSC. If an MPoC Solution dependency has more than one indicator, the most severe indicator will be inherited by the MPoC Solution Listing.
	Reference #	A unique identifier assigned by PCI SSC.	This reference number is unique per MPoC Solution Provider and MPoC Solution and remains the same for the life of the Listing. A MPoC Solution Provider may have multiple Listed MPoC Products, each of which will have a unique Reference number.
Operating System(s) Supported		This field contains the sum of all operating system(s) and operating system(s) version(s) supported by all MPoC Application(s).	An MPoC Solution must have at least one MPoC Application, each MPoC Application may support 1 or more platform(s) and operating system version(s).
Account Data Entry Method(s) Supported		This field contains the sum of all account data entry methods supported by all MPoC Application(s).	Each MPoC Application may support different account data entry methods.

Field	Description	Notes
Evaluation Lab	The name of the MPoC Lab that performed the Evaluation and Validation of the MPoC Solution against the *MPoC Standard*, and subsequently that MPoC Solution is Accepted and Listed by PCI SSC.	The MPoC Lab that Evaluates an MPoC Solution may be different from the MPoC Lab that Evaluated the MPoC Application(s).
MPoC Standard Version	The version of the *MPoC Standard* to which the MPoC Solution was Evaluated.	Re-Validation applies if an MPoC Solution Provider chooses to have their MPoC Solution Evaluated against a newer version of the *MPoC Standard* during the 3-Year Listing lifecycle of the MPoC Solution.
Re-Validation Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC Solution is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.
Annual Checkpoint Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC Solution is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.

MPoC Solution Details Listing – Data Elements

Table 9 describes the MPoC Solution details Listing fields, descriptions, and notes. MPoC Solution details Listings are presented on the Website to include information about MPoC Application(s) offered under the MPoC Solution.

Table 9: MPoC Solution Details Listing fields on the Website.

Field	Description	Notes
MPoC Application(s) Evaluated	MPoC Application Name, MPoC Application Version, OS: Operating system(s) on which the MPoC Application was tested and Validated, OS Version(s): Major version(s) of the operating system on which the MPoC Application was tested and is supported.	Identifies each MPoC Application Evaluated as part of the complete MPoC Solution Evaluation. Identifies each MPoC Application Evaluated separately from the MPoC Solution Evaluation and as part of the complete MPoC Solution Evaluation. MPoC Application(s) in MPoC Solution Listings will inherit the indicator of any dependencies to denote the MPoC Application supports dependencies that are not in Good Standing with PCI SSC (i.e., an MPoC Application dependent on an MPoC Software Product that is not in Good Standing). If an MPoC Application dependency has more than one indicator, the most severe indicator will be inherited by the MPoC Application in MPoC Solution Details Listing.
Account Data Entry Method(s)	Account Data Entry Methods supported by the MPoC Application.	Each MPoC Application is not permitted to have or support only PIN Entry. Each MPoC Application is not permitted to have or support only PIN and magnetic stripe based transactions. Each MPoC Application must also support at least one form of chip-based cardholder data entry.
Evaluation Lab	The name of the MPoC Lab that Evaluated and Validated the MPoC Application.	Applicable to each MPoC Application Evaluated. MPoC Applications may be Evaluated by an MPoC Lab different from the MPoC Lab that Evaluates the MPoC Solution. MPoC Applications are not as themselves MPoC Products and are therefore not eligible under the MPoC Program for Listing independent of the MPoC Solution. MPoC Applications are a component of an MPoC Solution, and all components of an MPoC Solution are the responsibility of the MPoC Solution Provider. When a candidate MPoC Solution is submitted to PCI SSC, the submission must include Evaluation and Validation of the MPoC Application(s) regardless of if the MPoC Application(s) were Evaluated by a different MPoC Lab than the MPoC Solution.
MPoC Standard Version	The version of the *MPoC Standard* to which the MPoC Application was Evaluated.	Applicable to each MPoC Application Evaluated. The MPoC Application may be Evaluated against a different version of the *MPoC Standard* than the MPoC Solution.

Field	Description	Notes
Product(s) Supported	This field indicates if the MPoC Solution Provider uses a monolithic or composite approach for their MPoC Solution.	Applicable to each MPoC Application Evaluated. If the MPoC Application is monolithic and the MPoC Application supports PCI PTS POI SCRP, then the PTS Approval number, SCRP firmware version, and SCRP hardware version will be included in this field. MPoC Application(s) in MPoC Solution Listings will inherit the indicator of any dependencies to denote the MPoC Application supports dependencies that are not in Good Standing with PCI SSC (i.e., an MPoC Application dependent on an MPoC Software Product that is not in Good Standing). If an MPoC Application dependency has more than one indicator, the most severe indicator will be inherited by the MPoC Application in MPoC Solution Details Listing.
MPoC Application Re-Validation Due Date	This date is inherited from the MPoC Solution Listing.	If MPoC Program Requirements for the MPoC Solution are not met, MPoC Application(s) bound to the MPoC Solution are not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.

Appendix C Elements for the List of Validated MPoC Software

Described in this Appendix are the Listing details available on the Website for the MPoC Product type: MPoC Software.

MPoC Software Listing – Data Elements

Table 10 describes the MPoC Software Listing fields, descriptions, and notes. MPoC Software Listings are presented on the Website to include the totality of all functionalities that are available under that MPoC Software.

Table 10: MPoC Software Listing fields on the Website.

Field		Description	Notes
MPoC Software Vendor		The MPoC Software Vendor's company name.	The MPoC Software Product name cannot be the same as the MPoC Software Vendors' name.
MPoC Software Product Identifier	MPoC Software Product	The name of the MPoC Software Product under which the MPoC Software Product is sold. Provided by the MPoC Software Vendor.	
	MPoC Software Details	Details of MPoC Application(s) and / or MPoC SDK(s) Evaluated.	Each MPoC Software product will have at least 1 MPoC Application or MPoC SDK denoted under MPoC Software Details. Elements for Listing MPoC Software Details are described in *Table 11*.
	Reference #	A unique identifier assigned by PCI SSC.	This reference number is unique per MPoC Software Vendor and MPoC Software Product and remains the same for the life of the Listing. A MPoC Software Vendor may have multiple Listed MPoC Products, each of which will have a unique Reference number.
Operating System(s) Supported		This field contains all operating system(s) and operating system version(s) supported by the MPoC Software.	This field contains the totality of all operating systems and operating systems versions supported by the MPoC Software Product. An MPoC Software Product must support at least one platform. An MPoC Software Product may support multiple platforms and operating system versions.

Field	Description	Notes
Account Data Entry Method(s) Supported	The account data entry method(s) supported by the MPoC Software.	This field contains the totality of all account data entry methods supported by the MPoC Software Product. If the MPoC Software Product supports more than 1 platform and operating system version: This field does not denote that every platform supported under the MPoC Software Product will support every account data entry method in this field.
Evaluation Lab	The name of the MPoC Lab that performed the Evaluation and Validation of the MPoC Software Product against the *MPoC Standard*, and subsequently that MPoC Software is Accepted and Listed by PCI SSC as per this MPoC Software Product Listing.	Only MPoC Labs Listed on the Website are eligible to Evaluate and Validate candidate MPoC Software Products for Acceptance by PCI SSC and subsequent Listing.
MPoC Standard Version	The version of the *MPoC Standard* to which the MPoC Software was Evaluated.	Re-Validation applies if an MPoC Software Vendor chooses to have their MPoC Software Product Evaluated against a newer version of the *MPoC Standard* during the 3-Year Listing lifecycle of the MPoC Software Product. MPoC Software may be Evaluated against a different version of the *MPoC Standard* than any MPoC Solution or MPoC A&M Service into which it is securely integrated.
Re-Validation Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC Software Product Listing is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.
Annual Checkpoint Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC Software Product Listing is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.

MPoC Software Details Listing – Data Elements

Table 11 describes the MPoC Software details Listing fields, descriptions, and notes. MPoC Software details Listings are presented on the Website to specify functionalities of each MPoC Application and/or each MPoC SDK available under that MPoC Software.

Table 11: MPoC Software Details Listing fields on the Website.

Field	Description	Notes
MPoC Application(s) and/or MPoC SDK(s) Evaluated	MPoC Application name / MPoC SDK name and type (isolated or non-isolated), MPoC Application / MPoC SDK Version, OS: Operating system(s) on which the MPoC Application / MPoC SDK was tested and Validated, OS Version(s): Major version(s) of the operating system on which the MPoC Application / MPoC SDK was tested and is supported.	MPoC SDKs are intended for integration into an MPoC Application. MPoC SDKs may be isolated or non-Isolated. This field Identifies each MPoC Application / MPoC SDK Evaluated as part of the complete MPoC Software Evaluation. Composite-based MPoC Application(s) in MPoC Software Listings will inherit the indicator of any MPoC SDK dependencies or other dependencies (i.e., PCI PTS POI SCRP) to denote the MPoC Application supports dependencies that are not in Good Standing with PCI SSC. MPoC SDK(s) will inherit the indicator of any dependencies (i.e., PCI PTS POI SCRP) to denote the MPoC SDK supports dependencies that are not in Good Standing with PCI SSC. If an MPoC Application dependency has more than one indicator, the most severe indicator will be inherited by the MPoC Application / MPoC SDK in MPoC Software Details Listing.
Account Data Entry Method(s)	Account Data Entry Methods supported by the MPoC Application / MPoC SDK.	Each MPoC Application / MPoC SDK is not permitted to have or support only PIN Entry. Each MPoC Application is not permitted to have or support only PIN and magnetic stripe based transactions. • Each MPoC Application must also support at least one form of chip-based cardholder data entry.

Field	Description	Notes
Evaluation Lab	The name of the MPoC Lab that Evaluated and Validated the MPoC Application / MPoC SDK.	Applicable to each MPoC Application / MPoC SDK Evaluated. MPoC Applications / MPoC SDKs are not as themselves MPoC Products and are therefore not eligible under the MPoC Program for Listing independent of the MPoC Software. MPoC Applications / MPoC SDKs are bound to the MPoC Software Product and are the responsibility of the MPoC Software Vendor. When a candidate MPoC Software Product is submitted to PCI SSC, the submission must include Evaluation and Validation of the MPoC Application(s) and MPoC SDK(s) regardless of if the MPoC Application(s) / MPoC SDK(s) were Evaluated by a different MPoC Lab than the MPoC Software Product.
MPoC Standard Version	The version of the *MPoC Standard* to which the MPoC Application / MPoC SDK was Evaluated.	Applicable to each MPoC Application / MPoC SDK Evaluated.

Field	Description	Notes
Supported	This field indicates if the MPoC Software Provider uses a monolithic or composite approach for their MPoC Application. This field also indicates if the MPoC Software Provider supports NON-PTS Approved MSR, PCI PTS POI SCRP.	An MPoC Application is permitted to integrate up to two MPoC SDKs (although this is a not a requirement, and integration of one or no MPoC SDKs is also permitted). Each MPoC SDK may be Isolated or non-Isolated. An MPoC Application Listed as part of an MPoC Software Product must be developed by the MPoC Software vendor and must not integrate the MPoC SDK(s) of any other MPoC Software Product. Applicable to each MPoC Application / MPoC SDK Evaluated. If the MPoC Application supports PCI PTS POI SCRP, then the PCI PTS Approval number, SCRP firmware version, and SCRP hardware version will be included in this field. If the MPoC Application supports NON-PTS Approved MSR, then the designator will be included in this field. If the MPoC Application is composite-based, each MPoC SDK will be included in this field. MPoC Application(s) / MPoC SDKs in MPoC Solution Listings will inherit the indicator of any dependencies to denote the MPoC Application / MPoC SDK supports dependencies that are not in Good Standing with PCI SSC (i.e., an MPoC Application dependent on an MPoC SDK that is not in Good Standing. Or MPoC SDK dependent on a PCI PTS POI SCRP not in Good Standing). If an MPoC Application / MPoC SDK dependency has more than one indicator, the most severe indicator will be inherited by the MPoC Application / MPoC SDK in the MPoC Software Details Listing.
Re-Validation Due Date	This date is inherited from the MPoC Software Listing.	If MPoC Program Requirements for MPoC Software are not met, MPoC Application(s) / MPoC SDK(s) bound to that MPoC Software Product are not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity.

Appendix D Elements for the List of Validated MPoC A&M Services

Described in this Appendix are the Listing details available on the Website for the MPoC Product type: MPoC A&M Service.

MPoC A&M Service Listing – Data Elements

Table 12 describes the MPoC A&M Service Listing fields, descriptions, and notes. MPoC A&M Listings are presented on the Website to include the totality of all functionalities that are available under that MPoC A&M Service.

Table 12: MPoC A&M Service Listing fields on the Website.

Field		Description	Notes
MPoC A&M Service Provider		The MPoC A&M Service Provider's company name.	The MPoC A&M Service name cannot be the same as the MPoC A&M Service Providers' name.
MPoC A&M Service Identifier	MPoC A&M Service	The name of the MPoC A&M Service under which the MPoC A&M Service is marketed. Provided by the MPoC A&M Service Provider.	
	Reference #	A unique identifier assigned by PCI SSC.	This reference number is unique per MPoC A&M Service Provider and MPoC A&M Service and remains the same for the life of the Listing. An MPoC A&M Service Provider may have multiple Listed MPoC Products, each of which will have a unique Reference number.
Operating System(s) Supported		All operating system(s) and operating system version(s) supported by the MPoC A&M Service	An MPoC A&M Service must support at least one platform. An MPoC A&M Service may support multiple platforms and operating system versions.
Supported MPoC Software		Each MPoC Software Product name, version, and reference # supported by the MPoC A&M Service will be denoted here.	Each MPoC A&M Service must support at least one MPoC Software Product. Each MPoC A&M Service may support many MPoC Software Products. If a candidate MPoC Solution Provider pursues Acceptance of an MPoC Solution designed to securely integrate an MPoC A&M Service with monolithic software (and the absence of an MPoC Software Product) then: the monolithic software must first be Evaluated, Validated, Accepted and Listed as MPoC Software, and: The MPoC A&M Service must be Evaluated, Validated, Accepted and Listed denoting the MPoC Software is supported.

Field	Description	Notes
Evaluation Lab	The name of the MPoC Lab that performed the Evaluation and Validation of the MPoC A&M Service against the *MPoC Standard*, and subsequently that MPoC A&M Service is Accepted and Listed by PCI SSC.	Only MPoC Labs Listed on the Website are eligible to Evaluate and Validate candidate MPoC A&M Services for Acceptance by PCI SSC and subsequent Listing.
MPoC Standard Version	The version of the *MPoC Standard* to which the MPoC A&M Service was Evaluated.	Re-Validation applies if an MPoC A&M Service Provider chooses to have their MPoC A&M Service Evaluated against a newer version of the *MPoC Standard* during the 3-Year Listing lifecycle of the MPoC A&M Service. An MPoC A&M Service may be Evaluated against a different version of the *MPoC Standard* than any MPoC Solution it is security integrated into.
Re-Validation Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC A&M Service Listing is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity. MPoC A&M dependencies in MPoC A&M Service Listings will inherit the indicator of any dependencies to denote the MPoC A&M Service supports an MPoC Product (i.e., MPoC Software) that is not in Good Standing. If the dependency has more than one indicator, the most severe indicator will be inherited (i.e., MPoC A&M Services that support more than one MPoC Software Product).
Annual Checkpoint Due Date	Date Format: DD MMM YYYY	If MPoC Program Requirements are not met, this MPoC A&M Service Listing is not in Good Standing with PCI SSC and indicators are displayed on the Website to reflect the severity. MPoC A&M dependencies in MPoC A&M Service Listings will inherit the indicator of any dependencies to denote the MPoC A&M Service supports an MPoC Product (i.e., MPoC Software) that is not in Good Standing. If the dependency has more than one indicator, the most severe indicator will be inherited (i.e., MPoC A&M Services that support more than one MPoC Software Product)