Payment Card Industry (PCI)

Point-to-Point Encryption P2PE Merchant-Managed Solution

Template for Report on Validation for use with P2PE v3.1 for P2PE Merchant-Managed Solution Assessments

September 2021

Document Changes

Date	Use with P2PE Standard Version	Template Revision	Description
December 2019	P2PE v3.0	Revision 1.0	This template is for P2PE Reports on Validation for Merchant-Managed Solutions assessed against the P2PE v3.0 Standard. This document serves as both the Reporting Template and Reporting Instructions document; there are not separate documents for this under P2PE v3.0.
September 2021	P2PE v3.1	Revision 1.0	This template includes the following updates: - Updates from v3.0 P2PE Standard references to v3.1. - Revisions made within the Introduction through Section 3 to add clarity and consistency, both within this P-ROV and across all v3.1 P-ROVs as applicable. - Context of “PCI-listed” P2PE Products updated to “Validated”. Includes revision to diagram in Introduction. - Revision to the description for the use of Not Applicable to add clarity and guidance. - Reformatting and restructuring of tables in Sections 2 and 3 with additional guidance. - Certain tables/context were modified into new tables (e.g., 2.4.x) - Table numbering in sections 1 through 3 modified as needed to better align across all v3.1 P-ROVs. - New table in section 4 to document all requirements determined to be Not Applicable. - Errata updates to section 4. - Added check boxes to section 4 to each individual requirement to capture In Place, N/A, or Not In Place assessment findings.

Contents

Introduction to the P-ROV Template for P2PE Merchant-Managed Solution Assessments

This document, the *PCI Point-to-Point Encryption: Template for Report on Validation for use with P2PE v3.1 for P2PE Merchant-Managed Solution Assessments* ("MMS P-ROV Reporting Template"), is the mandatory template for completing a P2PE Report on Validation (P-ROV) for P2PE Merchant-Managed Solution assessments against the *P2PE: Security Requirements and Testing Procedures, v3.1 Standard* ("P2PE Standard").

Use of this Reporting Template is mandatory for all P2PE v3.1 Merchant-Managed Solution (MMS) assessments.

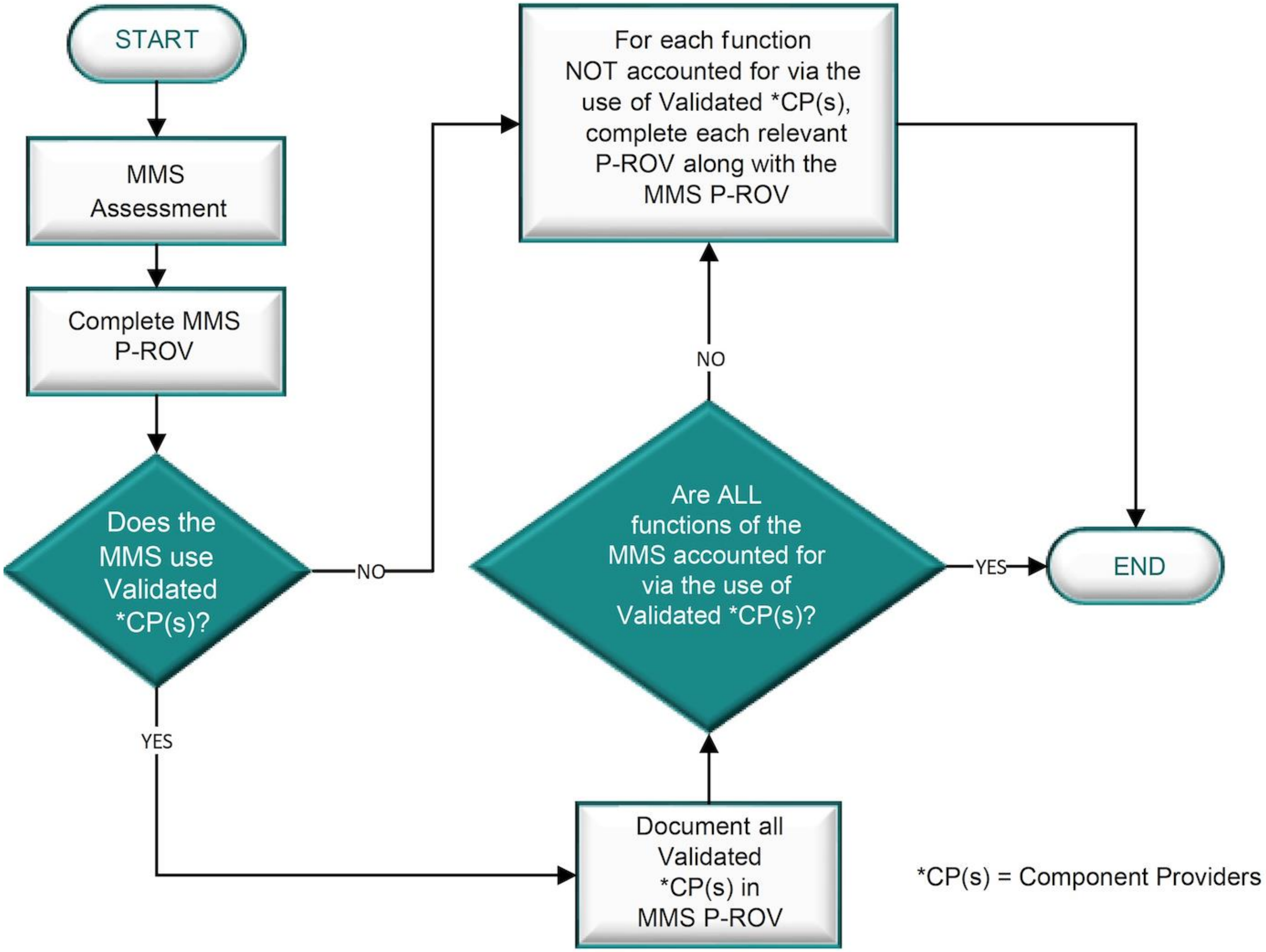
Note: MMS assessments are not submitted to PCI SSC – refer to the P2PE Program Guide for further details.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, as necessary. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable but limited to the title page.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as they complete reporting, but also provide context for the report recipient(s). Addition of text or sections is applicable within reason, as noted above.

A P2PE compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The P-ROV is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the P-ROV provides a ***summary of testing activities performed and information collected*** during the assessment of the P2PE Solution against the P2PE Standard. The information contained in the submitted P-ROV(s) must provide enough detail and coverage to verify that the P2PE submission is compliant with all applicable P2PE requirements.

Merchant-Managed Solution (MMS) assessments, ***at a minimum***, must complete this P-ROV template. For every function that is not outsourced to an applicable PCI-listed Component Provider, **EACH** applicable P-ROV must be completed in addition to this P-ROV as per the following diagram and table:


START
MMS Assessment
Complete MMS P-ROV
Does the MMS use Validated *CP(s)?
NO
YES
For each function NOT accounted for via the use of Validated *CP(s), complete each relevant P-ROV along with the MMS P-ROV
NO
Are ALL functions of the MMS accounted for via the use of Validated *CP(s)?
YES
END
Document all Validated *CP(s) in MMS P-ROV
*CP(s) = Component Providers

The following table summarizes the P2PE v3.1 P-ROVs and the applicability of each P-ROV relative to the assessment type.
Acronyms used: *CP = Component Provider*

P-ROV	APPLICABLE ASSESSMENTS	PURPOSE
Merchant-Managed Solution	Merchant-Managed Solution (MMS)	The MMS P-ROV is mandatory for all P2PE MMS assessments, at a minimum. Additional P-ROVs (below) may be required depending on the scope of the assessment.
Encryption Management Services (EMS)	Merchant-Managed Solution (MMS) Encryption Management CP (EMCP) POI Deployment CP (PDCP) POI Management CP (PMCP)	Encryption Management Services relates to the distribution, management, and use of PTS-approved POI devices in a P2PE [Merchant-Managed] Solution. **MMS assessments** that have not satisfied the entirety of their Encryption Management Services (Domain 1 with Domain 5) via the use of applicable Validated P2PE Component Providers must complete the EMS P-ROV in addition to the MMS Solution P-ROV.
P2PE Application	P2PE Application	Any assessment that utilizes software on the PTS-approved POI devices intended for use in a P2PE [Merchant-Managed] Solution that has the potential to access clear-text account data must complete the P2PE Application P-ROV (one for each application).
Decryption Management Services (DMS)	Merchant-Managed Solution (MMS) Decryption Management CP (DMCP)	Decryption Management Services relates to the management of a decryption environment, including applicable account-data decryption devices used to support a P2PE [Merchant-Managed] Solution. **MMS assessments** that have not satisfied the entirety of their Decryption Management Services with applicable Validated P2PE Component Providers must complete the DMS P-ROV in addition to the MMS P-ROV.
Key Management Services (KMS)	Merchant-Managed Solution (MMS) Key Injection Facility (KIF) Key Management CP (KMCP) Key Loading CP (KLCP) CA/RA	Key Management Services relates to the generation, conveyance, management, and loading of cryptographic keys including the management of associated devices. **MMS assessments** that have not satisfied the entirety key management services requirements (Domain 5) either through the use of Validated P2PE Component Providers and/or through the assessment of their Encryption Management Services and/or Decryption Management Services must complete the KMS P-ROV. E.g., if the P2PE Merchant-Managed Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account-data encryption, or the operation of an applicable CA/RA. Or if any other relevant key management service that has not already been assessed as part of the inclusion of a Validated P2PE Component Provider and/or as part of the Domain 1 and Domain 4 assessment scope of the MMS assessment, then the MMS assessment must include the use of the KMS P-ROV.

P-ROV Sections

The P-ROV includes the following sections that must be completed in their entirety:

- Section 1: Contact Information and Report Date
- Section 2: Summary Overview
- Section 3: Details and Scope of P2PE Assessment
- Section 4: Findings and Observations

This Reporting Template includes tables with Reporting Instructions built in. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

P-ROV Summary of Findings

This version of the P2PE Reporting Template reflects an ongoing effort to simplify assessor summary reporting. All summary findings for “In Place,” “Not in Place,” and “Not Applicable” are found at the beginning of section 4, “Findings and Observations,” and are only addressed at that high-level. The summary of the overall compliance status is at section 2.8, “Summary of P2PE Assessment Compliance Status.”

The following table is a representation when considering which selection to make. Assessors must select only one response at the sub-requirement level, and the selected response must be consistent with reporting within the remainder of the P-ROV and other required documents, such as Component P-ROVs and the relevant P2PE Attestation of Validation (P-AOV).

RESPONSE	WHEN TO USE THIS RESPONSE
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated. Requirements fulfilled by other P2PE Components or Third Parties should be In Place, unless the requirement does not apply.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	‘Not Applicable’, or ‘N/A’, is only acceptable as a finding where the requirement, through testing and review, is determined to not apply to the P2PE Product. All N/A responses require reporting on testing performed (including interviews conducted and documentation reviewed) and must explain how it was determined that the requirement does not apply within the scope of the assessment for the P2PE Product. ***Note:*** *‘Not Applicable’ cannot be used by entities that provide only partial aspects of a defined Component Provider service to validate to that Component Provider type. Refer to the “P2PE Applicability of Requirements” in the P2PE Program Guide.*

Note: *Checkboxes have been added to the “Summary of Assessment Findings” so that the assessor may double click to check the applicable summary result. Hover over the box you’d like to mark and click once to mark with an ‘x.’ To remove a mark, hover over the box and click again. Mac users may instead need to use the space bar to add the mark.*

P-ROV Reporting Details

The reporting instructions in the Reporting Template are clear as to the intention of the response required. There is no need to repeat the testing procedure or the reporting instruction within each assessor response. As noted earlier, responses should be specific, but simple. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

Assessor responses will generally fall into categories such as the following:

- **"Identify the P2PE Assessor who confirms…"**

  Indicates only an affirmative response where further reporting is deemed unnecessary by PCI SSC. The P2PE Assessor's name or a Not Applicable response are the two appropriate responses here. A Not Applicable response will require brief reporting to explain how this was confirmed via testing.

- **Document name or interviewee reference**

  At section 3.6, "Documentation Reviewed," and section 3.7, "Individuals Interviewed," there is a space for a reference number; ***it is the P2PE Assessor's choice*** to use the document name/interviewee job title or the reference number in responses. A listing is sufficient here, no further detail required.

- **Sample reviewed**

  Brief list is expected or sample identifier. Where applicable, it is the P2PE Assessor's choice to list out each sample within the reporting or to utilize sample identifiers from the sampling summary table.

- **Brief description/short answer – "Describe how…"**

  These responses must be a narrative response that provides explanation as to the observation—both a summary of what was witnessed and how that verified the criteria of the testing procedure.

Do’s and Don’ts: Reporting Expectations

DO:	DON’T:
▪ Complete all applicable P-ROVs based on the assessment. ▪ Complete all sections in the order specified, with concise detail. ▪ Read and understand the intent of each Requirement and Testing Procedure. ▪ Provide a response for every Testing Procedure, even if N/A. ▪ Provide sufficient detail and information to demonstrate a finding of “in place” or “not applicable.” ▪ Describe how a Requirement was verified as the Reporting Instruction directs, not just that it was verified. ▪ Ensure all parts of the Testing Procedure are addressed. ▪ Ensure the response covers all applicable application and/or system components. ▪ Perform an internal quality assurance review of the P-ROV for clarity, accuracy, and quality. ▪ Perform an internal quality assurance review of all submitted P-ROVs and the details within the PCI SSC Portal. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don’t report items in the “In Place” column unless they have been verified as being “in place.” ▪ Don’t include forward-looking statements or project plans in responses. ▪ Don’t simply repeat or echo the Testing Procedure in the response. ▪ Don’t copy responses from one Testing Procedure to another. ▪ Don’t copy responses from previous assessments. ▪ Don’t include information irrelevant to the assessment. ▪ Don’t mark “N/A” without providing an explanation and justification for why it is “N/A”.

P-ROV Merchant-Managed Solution Template for the P2PE v3.1 Standard

The use of this template is mandatory for creating a P2PE Report on Validation (P-ROV) for P2PE Merchant-Managed Solutions assessed against the P2PE Standard. Additional P-ROVs may be required based on the scope of the assessment. Refer back to the diagram and table in the Introduction section. Complete the remainder of this P-ROV as instructed.

1. Contact Information and Report Date

1.1 Contact Information				
MMS Provider Contact Information				
Company name:		Company URL:		
Company contact name:		Contact e-mail address:		
Contact phone number:		Company address:		
P2PE Assessor Company and Lead Assessor Contact Information				
Company name:		Assessor company credentials:	□ QSA (P2PE)	□ PA-QSA (P2PE)
Company Servicing Markets for P2PE: (see https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_assessors)				
Assessor name:		Assessor credentials:	□ QSA (P2PE)	□ PA-QSA (P2PE)
Assessor phone number:		Assessor e-mail address:		
Confirm that internal QA was fully performed on the entire P2PE assessment documentation, per requirements in the relevant program documentation.		□ Yes □ No *(If **No**, this is not in accordance with PCI Program requirements)*		
QA reviewer name:		QA reviewer credentials: (*Leave blank if not applicable*)		
QA reviewer phone number:		QA reviewer e-mail address:		
Provide details for any additional P2PE Assessors involved with the P2PE assessment. Add additional rows as needed.				
Assessor name:		Assessor credentials:	□ QSA (P2PE)	□ PA-QSA (P2PE)
Assessor phone number:		Assessor e-mail address:		

1.2 Date and Timeframe of Assessment

Date of Report: (DD-MMM-YYYY) *Ex: 01-Jan-2021*		**Timeframe of Assessment:** (*From* DD-MMM-YYYY *To* DD-MMM-YYYY)	

1.3 Additional Services Provided by PA-QSA(P2PE) / QSA(P2PE) / P2PE QSA Company

The current version of the “Qualification Requirements *for Point-to-Point Encryption (P2PE)™ Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE)” (*P2PE QSA Qualification Requirements*)*, section “Independence”, specifies requirements for P2PE QSAs around disclosure of such services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the sections below after review of this portion of the P2PE QSA Qualification Requirements to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the PA-QSA(P2PE) / QSA (P2PE) / P2PE QSA company, including but not limited to whether the assessed entity uses any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	
▪ Describe efforts made to ensure no conflict of interest resulted from the above mentioned services provided by the PA-QSA(P2PE) / QSA(P2PE) / QSA company:	

1.4 P2PE Standard Version Used for Assessment

Version of the P2PE Standard used for this assessment (*must be v3.1*):	

2. Summary Overview

2.1 Merchant-Managed Solution Details	
Merchant-Managed Solution Name:	
Description of the Merchant-Managed Solution Provider:	
Description of the implementation of this Merchant-Managed Solution:	

2.2 Validated P2PE Component Providers

Document the use of ALL Validated P2PE Component Providers being used by the MMS to help satisfy requirements of the MMS assessment.

Note 1: *PCI-listed P2PE Component Providers must be considered Validated. Refer to the P2PE Program Guide for additional details.*

Note 2: *For requirement applicability information, refer to the “P2PE Applicability of Requirements” section in the P2PE Program Guide.*

Complete the EMS, DMS, and KMS tables below.

<table>
<tr><th colspan="4">Encryption Management Services (EMS)</th></tr>
<tr><td colspan="4">If the MMS does not use a Validated EMCP, only uses a Validated PDCP **or** a PMCP, or otherwise has not satisfied the entirety of the EMS-related requirements as it pertains to the full scope of the MMS assessment, then the Encryption Management Services (EMS) P-ROV must be completed for all applicable requirements in addition to this MMS P-ROV.</td></tr>
<tr><td rowspan="3">Are Validated EMS CPs being used to help satisfy requirements of this MMS assessment?</td><td colspan="3">□ No (*If **No**, complete an EMS P-ROV and leave the remainder of this Encryption Management Services section blank)*</td></tr>
<tr><td rowspan="2">□ Yes (*If **Yes**, complete the remainder of this EMS table*)</td><td rowspan="2">Is an EMS P-ROV still required to account for any remaining EMS-related requirements based on the full scope of the assessment?
(*E.g., where only a PMCP or a PDCP is being used, or otherwise where the MMS is providing functionality/services that are **not** covered by the Validated EMS P2PE Components being used.*)</td><td>□ Yes (*If **Yes**, complete an EMS P-ROV*)</td></tr>
<tr><td>□ No (*If **No**, ensure all applicable EMS requirements as they relate to the full scope of the MMS are satisfied through the use of Validated EMS CPs below*)</td></tr>
</table>

Document all Validated Encryption Management Services (EMS) Component Providers (CPs) being used to help satisfy requirements for the MMS assessment.

For every Component below, document the PTS Approval #s associated with their respective Validated P2PE Component listing that are being included in the scope of this MMS assessment. The PTS approval #s here must also be present in Table 2.5.

Note:

- *POI Device Types associated with PDCPs and PMCPs are only assessed to a subset of applicable Domain 1 and Domain 5 requirements. Therefore, only where a POI Device Type is supported by an EMCP or BOTH a Validated PDCP and a PMCP below is it excluded from requiring any additional assessment. Otherwise, each POI Device Type must be assessed to all applicable requirements in Domains 1 and 5 that were not covered under the assessment scope of the Component Types being used in the scope of this Solution assessment (this will be unique for each Solution assessment).*
- *The same applies to POI Device Types associated with Validated P2PE Applications – those POI devices must be accounted for via the use of Validated Components below, or otherwise they must be assessed to all applicable Domain 1 and 5 requirements that have not been covered under the assessment scope of the Component Types being used in the scope of this Solution assessment (this will be unique for each Solution assessment).*

Check **only** one per row. Insert additional rows as necessary.

Validated EMS P2PE Components			**P2PE Component Provider Name**	**P2PE Component Name**	**Validated Listing Reference #**	**PTS Approval #(s) (*comma delimited*)**
EMCP	**PDCP**	**PMCP**				
□	□	□				
□	□	□				
□	□	□				

Encryption Management Services (EMS) Continued
Describe how the Validated EMS-related P2PE Component Provider(s) are being used to satisfy applicable EMS P2PE requirements for this MMS assessment. If more than one Validated P2PE Component Provider is being used, clearly distinguish between them in the description. The use of multiple CPs of the same type must be clearly described. Clearly document if the MMS implements additional functionality/services that are **not** covered by the Validated EMS P2PE Components being used (*which means an EMS P-ROV must be used)*. Provide more detail than simply, e.g., "*The EMCP is satisfying Domains 1 & 5*". Do **not** leave blank unless there aren't any Validated EMS CPs being used.
<EMS CPs Description>

<table>
<tr><th colspan="4">Decryption Management Services (DMS)</th></tr>
<tr><td colspan="4">If the MMS does not use a Validated DMCP or otherwise has not satisfied the entirety of the DMS-related requirements as it pertains to the full scope of the MMS assessment, then the Decryption Management Services (DMS) P-ROV must be completed for all applicable requirements in addition to this MMS P-ROV.</td></tr>
<tr><td rowspan="3">Are Validated DMS CPs being used to help satisfy requirements of this MMS assessment?</td><td colspan="3">□ No (<i>If <b>No</b>, complete a DMS P-ROV and leave the remainder of this Decryption Management Services section blank)</i></td></tr>
<tr><td rowspan="2">□ Yes (<i>If <b>Yes</b>, complete the remainder of this DMS table</i>)</td><td rowspan="2">Is a DMS P-ROV still required to account for any remaining DMS-related requirements based on the full scope of the assessment?
(<i>E.g., where the MMS is providing functionality/services that are <b>not</b> covered by the Validated DMS P2PE Components being used.)</i></td><td>□ Yes (<i>If <b>Yes</b>, complete a DMS P-ROV</i>)</td></tr>
<tr><td>□ No (<i>If <b>No</b>, ensure all applicable DMS requirements as they relate to the full scope of the MMS are satisfied through the use of Validated DMS CPs below</i>)</td></tr>
<tr><td colspan="4">Document all Validated Decryption Management Services (DMS) Component Providers (CPs) being used to help satisfy requirements for the MMS assessment.
<b><i>Note:</i></b> <i>The use of multiple CPs of the same type (e.g., where multiple KIFs are used to service different regions) must be clearly described below.</i>
Insert additional rows as necessary.</td></tr>
</table>

Validated DMS P2PE Components	**P2PE Component Provider Name**	**P2PE Component Name**	**Validated Listing Reference #**
DMCP			
□			
□			

Decryption Management Services (EMS) Continued
Describe how the Validated DMS-related P2PE Component Provider(s) are being used to satisfy applicable DMS P2PE requirements for this MMS assessment. If more than one Validated P2PE Component Provider is being used, clearly distinguish between them in the description. Clearly document if the MMS implements additional functionality/services that are **not** covered by the Validated DMS P2PE Components being used. Provide more detail than simply, e.g., "*The DMCP is satisfying Domains 4 & 5*". Do **not** leave blank unless there aren't any Validated DMS CPs being used.
<DMS CP(s) Description>

Key Management Services (KMS)

MMS assessments that have not satisfied the Key Management Services (KMS) requirements (Domain 5) either through the use of Validated P2PE Component Providers (CPs) and/or through the assessment of their Encryption Management Services EMS) and/or Decryption Management Services must complete the KMS P-ROV for all applicable requirements in addition to this MMS P-ROV.

It may be possible, depending on the scope of the MMS assessment, that a KMS P-ROV is not required even when there aren't any KMS CPs being used. This is because a MMS does not assess to Domain 5 in isolation. It is assessed to Domain 5 in the context of Domain 1(EMS) and Domain 4(DMS). The assessor must accurately identify the full scope of the MMS assessment as per Table 3.1.

Note: *Remote Key Distribution (RKD) requirements are **additional** requirements to an assessment. It is not possible to assess the RKD requirements in isolation. Refer to the "P2PE Applicability of Requirements" in the P2PE Program Guide.*

Are Validated KMS CPs being used to help satisfy requirements of this MMS assessment?	□ Yes (*If **Yes**, complete the remainder of this KMS table*)	Is a KMS P-ROV still required to account for any remaining KMS-related requirements based on the scope of the assessment? (*E.g., where the MMS is providing functionality/services that are **not** covered in other aspects of the assessment)*	□ Yes (*If **Yes**, complete a KMS P-ROV*)
	□ No (*If **No**, this* **may, or may not,** *require the use of the KMS P-ROV, depending on the full scope of the MMS assessment)*		□ No (*If **No**, ensure all applicable Domain 5 requirements for BOTH EMS and DMS are satisfied in addition to any other functionality/services as they relate to the full scope of the MMS)*

Document all Validated Key Management Services (KMS) Component Providers (CPs) being used to help satisfy requirements for the MMS assessment.

Note: *The use of multiple CPs of the same type (e.g., where multiple KIFs are used to service different regions) must be clearly described below.*

Check **only** one per row. Insert additional rows as necessary.

Validated KMS P2PE Components				**P2PE Component Provider Name**	**P2PE Component Name**	**Validated Listing Reference #**
KIF	**KMCP**	**KLCP**	**CA/RA**			
□	□	□	□			
□	□	□	□			
□	□	□	□			
□	□	□	□			

Key Management Services (KMS) Continued
Describe how the Validated KMS-related P2PE Component Provider(s) are being used to satisfy applicable P2PE requirements for this MMS assessment. If more than one Validated P2PE Component Provider is being used, clearly distinguish between them in the description. Clearly document if the MMS implements additional functionality/services that are **not** covered by the Validated DMS P2PE Components being used. Provide more detail than simply, e.g., "*The KIF is satisfying Domain 5*".
<KMS CP(s) Description>

2.3 Third-Party Entities Involved in the MMS

Use Table 2.2 for the use of Validated P2PE Component Providers.

Third-party entities are entities that are **not** PCI-listed P2PE Component Providers. Third-party entities must be assessed as applicable for each P2PE assessment in which the third-party service is used to satisfy applicable P2PE requirements. Refer to the P2PE Standard and the P2PE Program Guide for further information.

Note: *If the EMS, DMS, and/or KMS P-ROVs are being used as part of this assessment, document the use of Third Parties relative to those services (requirements) in their respective P-ROVs. There is no need to duplicate information regarding Third Parties from those P-ROVs here. However, ensure information is not excluded here where it is not being documented in another P-ROV (e.g., when no other P-ROVs are being used as part of the MMS assessment and/or when there is information unique to the MMS that is otherwise not captured in another P-ROV).*

Insert additional rows as necessary.

Is the EMS P-ROV being used?	□ Yes (*Document EMS-related Third Parties in the EMS P-ROV*)	□ No (*Document any EMS-related Third Parties below*)
Is the DMS P-ROV being used?	□ Yes (*Document DMS-related Third Parties in the DMS P-ROV*)	□ No (*Document any DMS-related Third Parties below*)
Is the KMS P-ROV being used?	□ Yes (*Document KMS-related Third Parties in the KMS P-ROV*)	□ No (*Document any KMS-related Third Parties below*)
Are there Third-Parties that are otherwise not documented in another P-ROV?	□ Yes (*If **Yes**, provide details below)*	□ No (*If **No**, leave remainder of this table blank*)

Entity Name	Entity Location(s)	Role / Function

Provide any additional details regarding the use of Third Parties, as necessary, otherwise check ***No Additional Details***.	□ No Additional Details
<Additional Details, as needed>	

2.4.a Non-payment Software		
Use Table 2.4.b to document Validated P2PE Applications. Non-payment software is any software/files that **does not have** the potential to access clear-text account data. (*Refer to P2PE Glossary*) Any software that **does have** the potential to access clear-text account data must be assessed to Domain 2 – refer to Table 2.4.b. ***Note:*** *"P2PE Applications" and "P2PE non-payment software" (refer to P2PE Glossary) do not meet the PTS POI definition of "firmware", and as such they are not reviewed as part of the POI device's PTS POI assessment (i.e., they cannot be excluded from the scope of a P2PE assessment). Therefore, any software intended for use in a P2PE solution that does not meet the PTS POI definition of "firmware" must be assessed in accordance with the PCI P2PE Standard and is subject to all applicable P2PE security requirements.*		
Is non-payment software in scope for this MMS assessment?	□ Yes (*If **Yes,** assess and document ALL Non-payment Software in the EMS P-ROV*)	□ No

2.4.b Validated P2PE Applications

A P2PE Application P-ROV and associated assessment of each non-Validated application to Domain 2 is required. Refer to the P2PE Program Guide for details. This table is for Validated P2PE Applications ONLY - use Table 2.4.c for non-Validated P2PE Applications.

ONLY list the PTS Approval #s from each Validated P2PE Application in use that are actually supported by the Solution under assessment.

Each PTS Approval # here must be in Table 2.5 - i.e., all POI Device Types associated with a Validated P2PE Application must have been assessed to all applicable requirements in Domains 1 and 5. As POI Device Types associated with Validated P2PE Applications are only assessed to Domain 2, each POI Device Type supported by a Validated P2PE Application listed here must be:

- Included in the POI Device Types supported by a Validated EMCP, or by BOTH a Validated PDCP AND a Validated PMCP, being used in the scope of this Solution assessment, **OR,**
- Be assessed to all unaccounted for Domain 1 and Domain 5 requirements, which will depend on each unique Solution assessment.

Note 1: *"P2PE Applications" and "P2PE non-payment software" (refer to P2PE Glossary) do not meet the PTS POI definition of "firmware", and as such they are not reviewed as part of the POI device's PTS POI assessment (i.e., they cannot be excluded from the scope of a P2PE assessment). Therefore, any software intended for use in a P2PE solution that does not meet the PTS POI definition of "firmware" must be assessed in accordance with the PCI P2PE Standard and is subject to all applicable P2PE security requirements.*

Note 2: *PCI-listed P2PE Applications must be considered Validated. Refer to the P2PE Program Guide for additional details.*

https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_applications

Insert additional rows as needed.

Is the EMS P-ROV being used as part of this MMS assessment?	☐ Yes (*If **Yes,** document ALL Validated P2PE Applications in the EMS P-ROV and leave the remainder of this table blank*)
	☐ No (*If **No**, document ALL Validated P2PE Applications below*)

P2PE Application Listing Reference #	**Application Name**	**Application Version #(s) (*comma delimited*)**	**Application Vendor Name**	**PTS Approval #(s) (*comma delimited*)**

2.4.c Non-Validated P2PE Applications

This table is for non-Validated P2PE Applications ONLY - use Table 2.4.b for Validated P2PE Applications.

Each PTS Approval # here must be in Table 2.5 (i.e., all POI Device Types associated with non-Validated P2PE Applications must have been assessed to all applicable requirements in Domains 1 and 5.)

Note: *“P2PE Applications” and “P2PE non-payment software” (refer to P2PE Glossary) do not meet the PTS POI definition of “firmware”, and as such they are not reviewed as part of the POI device’s PTS POI assessment (i.e., they cannot be excluded from the scope of a P2PE assessment). Therefore, any software intended for use in a P2PE solution that does not meet the PTS POI definition of "firmware" must be assessed in accordance with the PCI P2PE Standard and is subject to all applicable P2PE security requirements.*

Are any non-Validated P2PE Applications included in the scope of the MMS assessment?	□ No (*If **No**, leave remainder of this table blank*)		
	□ Yes	If ***Yes***, is the EMS P-ROV being used as part of this MMS assessment?	□ Yes (*If **Yes**, document ALL non-Validated P2PE Applications in the EMS P-ROV and leave the remainder of this table blank)*
			□ No (*If **No**, document ALL non-Validated P2PE Applications below*)

Application Name	**Application Version #**	**P2PE Application P-ROV Completed (*one per application*)**	**PTS Approval #(s) (*comma delimited*)**
		□ Yes	
		□ Yes	
		□ Yes	

2.5 PTS-approved POI Devices Supported

Instructions:

- Only list each unique PTS Approval # once.
- List ALL associated hardware (HW) and firmware (FW) versions supported by the Solution and tested as part of the P2PE assessment.
- Ensure all the information below is correct, accurate, and there are no discrepancies between the information listed here and the information present on the POI device's associated PTS Approval listing.
- Do **NOT** include POI devices (including HW and/or FW) that are ineligible for P2PE (e.g., non-SRED).
- Do **NOT** include HW and/or FW on the POI device listing that was NOT tested as part of the P2PE assessment.

***Note 1**: Be advised there can be POI device approval listings that appear similar/identical on the PCI SSC list of Approved PTS devices, however, they are associated with different major versions of the PTS POI Standard. Be sure the correct listing is being referenced and utilized in the assessment.*

***Note 2**: Clicking the PTS Approval # on the list of Approved POI Devices will display additional information. Be advised that the designators shown under "Functions Provided" do NOT necessarily apply to every HW and FW version for that PTS approval listing. Ensure that the requisite P2PE requirements are met and satisfied per POI Device Type (refer to the P2PE Glossary) included in the assessment. For each applicable PTS Approval #:*

- *Do **NOT** infer every HW and/or FW listed is SRED approved.*
- *Do **NOT** infer the account data capture or communication interface designators apply to every HW and/or FW listed.*

***Note 3:** POI Device Types (including those supported by a Validated P2PE Applications from Table 2.4.b and non-Validated P2PE Applications in Table 2.4.c) **must** be assessed to all applicable requirements in Domains 1 and Domain 5. The scope of the assessment for POI devices will be unique for each P2PE MMS assessment.*

- *POI Device Types associated with Validated PDCPs and PMCPs are only assessed to a subset of applicable Domain 1 and Domain 5 requirements. Therefore:*
  - *Only a POI Device Type that is supported by an EMCP or BOTH a Validated PDCP and a PMCP, as listed in Table 2.2, is excluded from requiring any additional assessment. **OR**,*
  - *Each POI Device Type must be assessed to all applicable requirements in Domains 1 and 5 that were not covered under the assessment scope of the Component Type(s) being used in the scope of this MMS assessment (this will be unique for each assessment).*
- *POI Device Types associated with Validated P2PE Applications are only assessed to Domain 2 – those POI devices must be accounted for via the use of applicable Validated Components, or otherwise they must be assessed to all applicable Domain 1 and 5 requirements that have not been covered under the assessment scope of the Component Types being used in the scope of this MMS assessment (this will be unique for each assessment).*

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Is the EMS P-ROV being used as part of this Solution assessment?	☐ Yes (*If **Yes,** document ALL PTS-approved POI devices in the EMS P-ROV and leave the remainder of this table blank*)
	☐ No (If No, document *ALL PTS-approved POI devices below*)

PTS-approved POI Devices Supported Continued Add additional rows as necessary.					
PTS Approval # ***(One unique # per row)***	**Make / Mfr.**	**Model Name / Number**	**Hardware (HW) #(s) Tested**	**Firmware (FW) #(s) Tested**	**For each PTS Approval #, denote the manner that the PTS-approved POI Device Types were assessed to all applicable requirements in Domains 1 and 5:** *"Entirely through the use of applicable Validated P2PE Components"* ***Note: If any PTS POI Device Type does not meet the criteria above, it requires an assessment to all or part of the requirements in Domains 1 and 5. As this requires the use of the EMS P-ROV, leave this table blank and document all PTS POI device information in the EMS P-ROV.***

2.6 Secure Cryptographic Devices (SCDs)

List the SCD types used in the MMS

This includes all SCDs that apply to any of the applicable P2PE requirements relative to this assessment. E.g., SCDs used to generate or load cryptographic keys, encrypt keys, transfer keys, or to sign applications and/or whitelists to be loaded onto POI devices. Examples include HSMs, key-injection/loading devices (KLDs), etc.

Note 1: *PTS-approved POI Device information must be entered in Table 2.5. Do* ***not*** *enter it here.*

Note 2*: If the EMS, DMS, and/or KMS P-ROVs are being used as part of this assessment, document the use of SCDs relative to those services in their respective P-ROVs. There is no need to duplicate information regarding SCDs from those P-ROVs here. However, ensure information is not excluded here where it is not being documented in another P-ROV (e.g., when no other P-ROVs are being used as part of the Solution assessment).*

Insert additional rows as necessary.

Is the EMS P-ROV being used?	□ Yes (*Document EMS-related SCDs in the EMS P-ROV*)	□ No (*Document any EMS-related SCDs below*)
Is the DMS P-ROV being used?	□ Yes (*Document DMS-related SCDs in the DMS P-ROV*)	□ No (*Document any DMS-related SCDs below*)
Is the KMS P-ROV being used?	□ Yes (*Document KMS-related SCDs in the KMS P-ROV*)	□ No (*Document any KMS-related SCDs below*)
Are there SCDs that are otherwise not documented in another P-ROV?	□ Yes (*If* ***Yes****, provide details below*)	□ No (*If* ***No****, leave details blank*)

Identifier Type	**PTS and/or FIPS Approval #**	**Manufacturer / Model Name / Number**	**Hardware #(s)** *(comma delimited)*	**Firmware #(s)** *(comma delimited)*	**Location**	**Number of Devices per Location**	**Approved Key function(s) & Purpose**

2.7 Additional Encryption Implementations

Are additional account-data encryption implementations supported within the scope of this assessment? (*E.g., this could be a multi-acquirer scenario.*) ***Note 1:*** *While P2PE Applications are not permitted to encrypt clear-text account data, they might still be involved in supporting additional encryption implementations. P2PE Applications detailed below must be able to be cross-referenced to Table 2.4.b above.* ***Note 2:*** *While non-payment software is not permitted to have access to clear-text account data, it might still be involved in supporting additional encryption implementations. Non-payment software detailed below must be able to be cross-referenced to Table 2.4.a in the EMS P-ROV.*	□ Yes (*If **Yes**, provide details below*)
	□ No (*If **No,** leave details blank*)

Complete the following information for **ONLY** the relevant POI devices, P2PE Applications and/or non-payment software that is involved in supporting additional encryption implementations.

Insert additional rows as necessary.

PTS Approval # ***(One unique # per row)***	**POI Device Firmware** ***(comma delimited)***	**P2PE Application** **Listing Reference #**	**Non-Payment Software Details** ***(Name, version#)***

Describe the additional account data encryption implementations and the involvement of the POI device firmware, P2PE Application, and/or non-payment software as detailed above.

Where there is more than one implementation, clearly describe each implementation along with the applicable entity (e.g., acquirer) managing it.

2.8 Summary of P2PE Assessment Compliance Status

P2PE Merchant-Managed Solution (MMS)		
P2PE MMS Functions	**Compliant**	**Comments (*optional*)**
P2PE Merchant-Managed Solution Management (Domain 3 + Appendix A)	□ Yes □ No □ N/A	
Encryption Management Services (Domain 1 and Domain 5)	□ Yes □ No □ N/A	
Decryption Management Services (Domain 4 and Domain 5)	□ Yes □ No □ N/A	
Key Management Services (Applicable if there are any Domain 5 requirements that were not satisfied within the Encryption Management Services and the Decryption Management Services assessment scope.)	□ Yes □ No □ N/A	
P2PE Application(s) (Domain 2)	□ Yes □ No □ N/A	

3. Details and Scope of P2PE Assessment

3.1 Scoping Details
Complete this table as it applies to the entire Merchant-Managed Solution, even where EMS, DMS, KMS and/or P2PE Application P-ROVs are being used as part of this assessment. **Describe how the accuracy of the scope for the entire P2PE Merchant-Managed Solution assessment was validated, including:**
• The methods or processes used to identify all elements in scope of the P2PE assessment:
• How it was confirmed that the scope of the assessment is accurate and covers all components and facilities for the MMS:

3.2 Merchant-managed Solution Diagram	
Complete this table as it applies to the entire MMS, even where EMS, DMS, KMS and/or P2PE Application P-ROVs are being used as part of this assessment. Provide one or more ***high-level*** diagrams to illustrate the functioning of the MMS, including: ▪ Locations of critical facilities, including the MMS' decryption environment, key-injection and loading facilities, etc. ▪ Location of critical components within the P2PE decryption environment, such as HSMs and other SCDs, cryptographic key stores, etc., as applicable ▪ Location of systems performing key-management functions ▪ Connections into and out of the decryption environment ▪ Connectivity between the requisite functions of the MMS ▪ Other necessary components, as applicable to the MMS	
Provide any additional information below that is not adequately captured within the diagram(s). Otherwise, check ***No Additional Details***.	□ No Additional Details
<Additional Details, as needed>	

<Insert Solution diagram(s) here>

3.3 Overview of MMS Data Flows

Complete this table as it applies to the entire MMS, even where EMS, DMS, KMS and/or P2PE Application P-ROVs are being used as part of this assessment.

Provide a ***high-level*** data-flow diagram of the MMS that illustrates:

- Flows and locations of encrypted account data
- Flows and locations of clear-text account data
- All flows and locations of truncated account data
- Location of critical system components (e.g., HSMs)
- All entities the MMS connects to for payment transmission or processing, including processors/acquirers

Note*: The diagram should identify where merchant entities fit into the data flow, without attempting to identify individual merchants. For example, encrypted account data could be illustrated as flowing between an icon that represents all merchant customers and an icon that represents the solution provider's decryption environment. Document if any intermediate proxies exist between merchant customers and the decryption environment.*

Provide any additional information below that is not adequately captured within the diagram(s). Otherwise, check ***No Additional Details***.	□ No Additional Details
<Additional Details, as needed>	

<Insert diagram(s) of MMS Data Flows here>

3.4 Key-management Processes	
Complete this table as it applies to the entire Solution, even where EMS, DMS, KMS and/or P2PE Application P-ROVs are being used as part of this assessment. Provide one or more ***high-level*** diagrams showing all key-management processes, including: ▪ Key Generation ▪ Key Distribution / Loading / Injection onto POI devices ▪ Other Key Distribution / Loading / Injection activities ▪ Key Storage ▪ Key Usage ▪ Key Archiving (if applicable) ▪ Any other relevant information **Note:** Include both logical and physical components—e.g., network traffic flows, locations of safes, use of secure couriers, etc.	
Provide any additional information below that is not adequately captured within the diagram(s). Otherwise, check No Additional Details.	□ No Additional Details
<Additional Details, as needed>	

<Insert diagram(s) of Key-management Processes here>

3.5 Facilities

Facilities used by the P2PE Assessor for this assessment

***Note:** If the EMS, DMS, KMS, and/or P2PE Application P-ROVs are being used as part of this assessment, document the use of facilities relative to those services in their respective P-ROVs. There is no need to duplicate information regarding facilities from those P-ROVs here. However, ensure information is not excluded here where it is not being documented in another P-ROV.*

Is the EMS P-ROV being used?	□ Yes (*Document EMS-related facilities in the EMS P-ROV*)	□ No (*Document any EMS-related facilities below*)
Is the DMS P-ROV being used?	□ Yes (*Document DMS-related facilities in the DMS P-ROV*)	□ No (*Document any DMS-related facilities below*)
Is the KMS P-ROV being used?	□ Yes (*Document KMS-related facilities in the KMS P-ROV*)	□ No (*Document any KMS-related facilities below*)
Are any P2PE Application P-ROVs being used?	□ Yes (*Document P2PE Application related facilities in the P2PE Application P-ROV(s)*)	□ No (*Document below as applicable*)

Facilities INCLUDED in the scope of this assessment (*insert additional rows as necessary*)

Were any facilities **included** in the scope of the assessment (*that are not otherwise captured in other P-ROVs*)?	□ Yes (*If **Yes,** document below*)	□ No (*If **No,** leave details blank*)

Description and purpose of facility included in assessment	**Address of facility**

Relevant facilities EXCLUDED from the scope of this assessment (*insert additional rows as necessary)*

***Note:** Does not apply to merchant locations.*

Were any relevant facilities **excluded** from the scope of the assessment (*that are not otherwise captured in other P-ROVs*)?	□ Yes (*If **Yes,** document below*)	□ No (*If **No,** leave details blank*)

Description and purpose of facility excluded from assessment	**Address of facility**	**Explanation why the facility was excluded from the assessment**

3.6 Documentation Reviewed

Identify and list all reviewed documents below. Add additional rows as needed.

Note: *If the PIM or P2PE Application Implementation Guide consists of more than one document, the brief description below should explain the purpose of each document it includes, e.g., if it is for different POI Device Types, different functions, different uses of the Solution (e.g., for different customer types), etc.*

There is no need to duplicate documents that appear in other P-ROVs included unless they are relevant to the Solution Management Controls.

P2PE Instruction Manual (PIM)

Reference # (*optional use*)	**Document Name (*Title of the PIM*)**	**Version Number of the PIM**	**Document Date (*latest version date*)**

P2PE Application Implementation Guide(s) (IG)

Reference # (*optional use*)	**Document Name (*Title of the IG*)**	**Version Number of the IG**	**Document date (*latest version date*)**	**Which P2PE Application is addressed? (*must align with Table 2.4.b*)**

All other documentation reviewed for this P2PE Assessment

Reference # (*optional use*)	**Document Name (*including version, if applicable*)**	**Document date (*latest version date*)**	**Document Purpose (*brief summary*)**

3.7 Individuals Interviewed

List of all personnel interviewed for this assessment

There is no need to duplicate interviewees that appear in other P-ROVs included unless they are relevant to the Solution Management Controls.

Reference # **(*optional use*)**	**Interviewee's Name**	**Job Title**	**Company**	**Summary of Topics Covered** **(*brief summary*)**

3.8 (Table not currently used)

3.9 Key Matrix

List all cryptographic key types used in the Solution

Reference Annex C in the P2PE Standard.

Note: *There is no need to duplicate Key Matrix information in Table 3.9 from other P-ROVs here. However, ensure all key types not documented in other P-ROVs are documented here.*

Key ID: Retain generic ID or use specific IDs from assessment.	**Key Length:** Full length (*include parity bits as applicable*).
Key Type: E.g., DEK, MFK, BDK, KEK, IEK, PEK, MAC, Public, Private, etc.	**Key Storage:** Smartcard, SCD, HSMs, Components, etc.
Algorithm: E.g., TDEA, AES, RSA, DSA, etc.	**Key Destruction:** List destruction methods ***for each*** storage method.
Key Mgmt: E.g., DUKPT, MK/SK, Fixed, One-time use, etc.	**Key Distribution:** E.g., Courier, Remote, etc.

Key ID	**Key Type**	**Algorithm**	**Key Mgmt**	**Key Length (bits)**	**Fill out all the information below for each key type**		
Key_1					**Description & Purpose:**		
					KEY	**Creation:**	
						Distribution:	
						Storage:	
						Destruction:	
Key_2					**Description & Purpose:**		
					KEY	**Creation:**	
						Distribution:	
						Storage:	
						Destruction:	

Copy the entire table below as needed and paste a new one to use for every remaining key type

Key_N					**Description & Purpose:**		
					KEY	**Creation:**	
						Distribution:	
						Storage:	
						Destruction:	

4. Findings and Observations

"In Place" may be a mix of "In Place" and "Not Applicable" responses, however it must not include any "Not in Place" responses.

Reference *Appendix I: P2PE Applicability of Requirements* in the P2PE v3.x Program Guide.

P2PE Merchant-Managed Solution – Summary of Findings

P2PE Validation Requirements	Summary of Findings (check one for EVERY row)		
	In Place	N/A	Not in Place
DOMAIN 3			
3A P2PE solution management			
3A-1 *The solution provider maintains documentation detailing the P2PE solution architecture and data flows.*	□	□	□
3A-2 *The solution provider manages and monitors status reporting from P2PE component providers.*	□	□	□
3A-3 *Solution provider implements processes to respond to notifications from merchants, component providers and/or third parties, and provide notifications about any suspicious activity involving the P2PE solution.*	□	□	□
3A-4 *If the solution provider allows a merchant to stop P2PE encryption of account data, the solution provider manages the related process for merchants.*	□	□	□
3B Third-party management			
3B-1 *The solution provider facilitates and maintains formal agreements with all third parties contracted to perform P2PE functions on behalf of the solution provider.*	□	□	□
3C Creation and maintenance of *P2PE Instruction Manual* for merchants			
3C-1 *Solution provider develops, maintains, and disseminates a* P2PE Instruction Manual *to merchants.*	□	□	□

P2PE Validation Requirements		Summary of Findings (check one for EVERY row)		
		In Place	**N/A**	**Not in Place**
Appendix A				
MM-A	Restrict access between the merchant decryption environment and all other networks/systems.			
MM-A-1	*The merchant decryption environment must be dedicated to decryption operations.*	□	□	□
MM-A-2	*Restrict access between the merchant decryption environment and all other networks/systems.*	□	□	□
MM-B	Restrict traffic between the encryption environment and any other CDE.			
MM-B-1	*Traffic between the encryption environment and any other CDE is restricted.*	□	□	□
MM-C	Restrict personnel access between encryption environment and decryption environment.			
MM-C-1	*Merchant in-store (encryption environment) personnel do not have logical access to the decryption environment, any CDEs, or account-data decryption keys.*	□	□	□

P2PE Merchant-Managed Solution – Reporting

P2PE Merchant-Managed Solution – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
3A-1.1 Current documentation must be maintained to describe or illustrate the architecture of the overall P2PE solution and include the following: • Identification of all parts of the overall solution managed by the solution provider • Identification of any parts of the overall solution outsourced to third-party service providers • Identification of P2PE controls covered by each third-party service provider		□	□	□
3A-1.1.a Interview relevant personnel and review documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the overall P2PE solution.	Documented procedures reviewed:	*<Report Findings Here>*		
	Relevant personnel interviewed:	*<Report Findings Here>*		
3A-1.1.b Interview relevant personnel and review documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document is current.	Documented procedures reviewed:	*<Report Findings Here>*		
	Relevant personnel interviewed:	*<Report Findings Here>*		
3A-1.1.c Interview relevant personnel and review documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document: • Identifies all components of the overall solution managed by the solution provider • Identifies all components of the overall solution that have been outsourced to third-party solution providers • Identifies all P2PE controls covered by each third-party service provider	Documented procedures reviewed:	*<Report Findings Here>*		
	Relevant personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3A-1.2 Current documentation (including a data-flow diagram) must include details of the account-data flow from the POI device (the point the card data is captured and encrypted) through to the point the encrypted card data is decrypted and the clear-text data exits the decryption environment.		□	□	□
3A-1.2 Examine the data-flow diagram and interview personnel to verify the diagram: • Shows all account data flows across systems and networks from the point the card data is captured through to the point the card data exits the decryption environment. • Is kept current and updated as needed upon changes to the environment.	Data-flow diagram reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
3A-1.3 Where there is a legal or regulatory obligation in a region for merchants to print full PAN on merchant receipts, it is allowable for the merchant to have access to full PAN for this purpose but the solution provider must document specifics about the legal or regulatory obligation including at least the following: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies *Note that Domain 1 (at 1B-1.1.1) and Domain 2 (at 2A-3.1.2) also include requirements that must be met for any POI device and any P2PE application, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*		□	□	□
3A-1.3.a Review solution provider's documentation about the legal/regulatory obligation that requires merchants to have access to full PANs for receipt printing purposes to verify that the documentation includes at least the following details about the legal/regulatory obligation: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies	Documented solution provider's procedures reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3A-1.3.b Perform independent review of, or conduct interviews with responsible solution provider personnel, to verify that the exception to facilitate merchants' access to full PANs is based on a legal/regulatory obligation and not solely for convenience.	Responsible solution provider personnel interviewed:	*<Report Findings Here>*		
	OR Describe how independent review verified that the exception to facilitate merchants' access to full PANs is based on a legal/regulatory obligation and not solely for convenience:			
	<Report Findings Here>			
3A-2.1 Where P2PE component providers are used, a methodology must be implemented to manage and monitor status reporting from P2PE component providers, including: • Ensuring reports are received from all P2PE component providers as specified in the "Component Providers ONLY: Report Status to Solution Providers" sections of Domains 1, 5, and/or 6 (as applicable to the component provider). • Confirming reports include at least the details specified in the "Component Providers ONLY: Report Status to Solution Providers" sections of Domains 1, 5, and/or 6 (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider. • Following up with the component provider to resolve any questions or changes in expected performance of the component provider.		□	□	□
	Documented procedures reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3A-2.1 Where component providers are used, interview responsible personnel, review documentation, and observe processes to verify the solution provider has implemented a methodology for managing and monitoring status reporting from P2PE component providers, including processes for: • Ensuring reports are received from all P2PE component providers as specified in the "Component providers ONLY: report status to solution providers" sections of this Standard (as applicable to the component provider) • Confirming reports include at least the details specified in the "Component providers ONLY: report status to solution providers" sections of this Standard (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider • Following up with the component provider to resolve any questions or changes in expected performance of the component provider	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe the processes observed that verified that the solution provider has implemented a methodology for managing and monitoring status reporting from P2PE component providers, including processes for: • Ensuring reports are received from all P2PE component providers as specified in the "Component providers ONLY: report status to solution providers" sections of this Standard (as applicable to the component provider) • Confirming reports include at least the details specified in the "Component providers ONLY: report status to solution providers" sections of this Standard (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider • Following up with the component provider to resolve any questions or changes in expected performance of the component provider			
	<Report Findings Here>			
3A-2.2 Processes must be implemented to ensure P2PE controls are maintained when changes to the P2PE solution occur including, but not limited to: • Changes in third-party service providers • Changes in overall solution architecture		□	□	□
3A-2.2.a Interview responsible personnel and review documentation to verify the solution provider has a formal process for ensuring P2PE controls are maintained when changes to the P2PE solution occur, including procedures for addressing the following: • Changes in third-party service providers • Changes in overall solution architecture	Documented procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor’s Findings		
		In Place	N/A	Not In Place
3A-2.2.b For a sample of changes, verify changes were documented and the solution updated accordingly.	Sample of changes reviewed:	*<Report Findings Here>*		
3A-3.1 Processes must be implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity, and provide immediate notification to all applicable parties of suspicious activity including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures ***Note:*** *“Immediate” means promptly or as soon as possible.*		□	□	□
3A-3.1 Examine documented procedures and interview personnel to verify processes are implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity and provide immediate notification to all applicable parties, including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures	Documented procedures reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
3A-3.2 Upon detection of any suspicious activity defined at **3A-3.1**, the POI device must be immediately removed, shut down, or taken offline until the integrity of the device is verified and the P2PE encryption mechanism is restored.		□	□	□
3A-3.2 Review documented procedures and interview responsible personnel to verify that upon detection of any suspicious activity defined at 3A-3.1, POI devices are immediately removed, shut down, or taken offline.	Documented procedures reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
3A-3.2.1 The POI device must not be re-enabled until it is confirmed that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has provided written notification (signed by a merchant executive officer) formally requesting stopping of P2PE encryption services, according to the solution provider's procedures (as defined in Requirement **3A-4.1**).		□	□	□
3A-3.2.1 Examine documented procedures and interview personnel to verify the POI devices must not be re-enabled until it is confirmed that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has provided written notification (signed by a merchant executive officer) requesting stopping of P2PE encryption services, according to the solution provider's procedures (as defined in Requirement **3A-4.1**).	Documented procedures reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	**N/A**	**Not In Place**
3A-3.3 The solution provider must maintain a record, at minimum of one year, of all suspicious activity, to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that the issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled		□	□	□
3A-3.3 Examine documented procedures and related records, and interview personnel to verify they maintain records of all suspicious activity, including the following details: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled	Documented procedures reviewed:	*<Report Findings Here>*		
	Related records reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3A-3.4 Procedures must incorporate any applicable incident response procedures defined by the PCI payment brands, including timeframes for reporting incidents.		□	□	□
3A-3.4.a Examine documented incident-response plans to verify they incorporate procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.	Documented incident-response plans reviewed:	*<Report Findings Here>*		
3A-3.4.b Interview responsible personnel to verify that any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents, are known and implemented.	Responsible personnel interviewed:	*<Report Findings Here>*		
3A-3.5 Processes must be implemented to ensure any P2PE control failures are addressed including, but not limited to: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Updating the solution and/or controls to prevent cause from recurring		□	□	□
3A-3.5.a Interview responsible personnel and review documentation to verify the solution provider has a formal process for any P2PE control failures, including procedures for addressing the following: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Implementing controls to prevent cause from recurring	Responsible personnel interviewed:	*<Report Findings Here>*		
	Documentation reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3A-3.5.b For a sample of P2PE control failures, interview personnel and review supporting document to verify that: • Identification occurred. • Corrective actions were implemented and documented. • The solution and/or control was updated accordingly.	Sample of P2PE control failures:	*<Report Findings Here>*		
	Supporting document reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
3B-1.1 Solution provider must have formal agreements in place with all third parties that perform P2PE functions on behalf of the solution provider, including: • All functions for which each third party is responsible • Agreement to maintain P2PE controls for which they are responsible • Notification and documentation of any changes affecting the third party governed by P2PE requirements. • Notification of any security-related incidents • Defining and maintaining appropriate service level agreements (SLAs) • Maintaining compliance with applicable P2PE and/or PCI DSS requirements as needed • Agreement to provide proof of compliance with P2PE requirements and/or PCI DSS requirements as needed • Agreement to provide reports to solution provider as required in the "Component Providers ONLY: Report Status to Solution Providers" section of the applicable P2PE Domain		□	□	□

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3B-1.1.a Examine documented procedures to verify the solution provider has a formalized process in place to establish agreements with all third parties performing services or functions governed by any other domain within this standard. The formalized agreement must include: • All functions each third party is responsible for • Maintaining P2PE controls for which they are responsible • Notification and documentation of any changes affecting the third party governed by P2PE requirements • Notification of any security-related incidents • Defining and maintaining appropriate service level agreements (SLAs) • Maintaining compliance with applicable P2PE and/or PCI DSS requirements as needed • Agreement to provide proof of compliance with P2PE requirements and/or PCI DSS requirements as needed • Agreement to provide reports to solution provider as required in the "Component providers ONLY: report status to solution providers" section of the applicable P2PE Domain	Documented procedures reviewed:	*<Report Findings Here>*		
3B-1.1.b If the solution provider utilizes any third parties, examine the business agreements and verify the elements delineated in **3B-1.1.a** are present and adequately accounted for.	Identify the P2PE Assessor who confirms that the business agreements for third parties utilized by the solution provider were reviewed and verified to have the elements delineated in **3B-1.1.a** present and adequately accounted for:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3B-1.2 For all third parties that have been contracted by the solution provider to manage any of the SCD types used in the P2PE solution, the solution provider must establish formal agreements with the third parties to ensure those third parties provide the Solution Provider with the following: • Notification of any changes that require a Designated Change per the P2PE Program Guide • Details of the change, including the reason for the change • Updated list of any dependencies included in the Designated Change (e.g., POI devices, P2PE applications, , and/or HSMs) used in the solution • Evidence of adherence to PCI's process for P2PE Designated Changes to Solutions		□	□	□
3B-1.2 Verify formal agreements established for all third parties managing SCDs on behalf of the solution provider require: • Notification of any changes that require a Designated Change per the P2PE Program Guide • Details of the change, including the reason for the change • Updated list of any dependencies included in the Designated Change (e.g., POI devices, P2PE applications, and/or HSMs) used in the solution • Evidence of adherence to PCI's process for P2PE Designated Changes to Solutions	Identify the P2PE Assessor who confirms that the business agreements for third parties managing SCDs on behalf of the solution provider were reviewed and verified to require all elements at 3B-1.2:	*<Report Findings Here>*		
3C-1.1 The PIM must be developed, maintained, distributed to merchants, and provided to merchants upon request. Content for the PIM must be in accordance with the mandatory PIM Template.		□	□	□
3C-1.1.a Examine the P2PE Instruction Manual (PIM) to verify it covers all related instructions, guidance and requirements as specified in the PIM Template.	Identify the P2PE Assessor who confirms that the PIM covers all related instructions, guidance and requirements as specified in the PIN Template:	*<Report Findings Here>*		
3C-1.1.b Examine documented procedures to verify mechanisms are defined to distribute the PIM to all merchants using the P2PE solution, and to provide the PIM to merchants upon request.	Documented procedures reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3C-1.1.c Interview responsible personnel and observe processes to verify PIM is distributed to all merchants using the P2PE solution and that the PIM is provided to merchants upon request.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe processes observed to verify PIM is distributed to all merchants using the P2PE solution and that the PIM is provided to merchants upon request:			
	<Report Findings Here>			
3C-1.1.d Examine the PIM to verify that all devices specified in the PIM are PCI-approved POI devices that were assessed as part of this P2PE solution assessment.	Identify the P2PE Assessor who confirms that all devices specified in the PIM are PCI-approved POI devices that were assessed as part of this P2PE solution assessment:	*<Report Findings Here>*		
3C-1.1.e Examine the PIM to verify the following: • All P2PE applications specified in the PIM are assessed for this solution (per Domain 1). • All P2PE applications specified in the PIM are either PCI-listed P2PE applications or assessed to Domain 2 as part of this P2PE solution assessment.	Identify the P2PE Assessor who confirms that all P2PE applications specified in the PIM are assessed for this solution (per Domain 1) and that all P2PE applications specified in the PIM are either PCI-listed P2PE applications or assessed to Domain 2 as part of this P2PE solution assessment:	*<Report Findings Here>*		
3C-1.1.f Examine the PIM to verify that all P2PE non-payment software specified in the PIM were assessed as part of this P2PE solution assessment (per Requirement **1C-2**).	Identify the P2PE Assessor who confirms that all P2PE non-payment software specified in the PIM were assessed as part of this P2PE solution assessment (per Requirement **1C-2**):	*<Report Findings Here>*		
3C-1.1.g Configure each POI device type, settings, etc. in accordance with all instructions in the PIM and confirm the following: • The PIM provides accurate instructions. • The PIM instructions facilitate a securely installed P2PE solution.	Describe how it was confirmed that by configuring each POI device type, settings, etc. in accordance with all instructions in the PIM, the PIM provides accurate instructions and those instructions facilitate a securely installed P2PE solution:			
	<Report Findings Here>			

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
3C-1.2 Review P2PE Instruction Manual (PIM) at least annually and upon changes to the solution or the P2PE requirements. Update PIM as needed to keep the documentation current with: • Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and • Any changes to the requirements in this document.		□	□	□
3C-1.1.e Examine the PIM to verify the following: • All P2PE applications specified in the PIM are assessed for this solution (per Domain 1). • All P2PE applications specified in the PIM are either PCI-listed P2PE applications or assessed to Domain 2 as part of this P2PE solution assessment.	Identify the P2PE Assessor who confirms that all P2PE applications specified in the PIM are assessed for this solution (per Domain 1) and that all P2PE applications specified in the PIM are either PCI-listed P2PE applications or assessed to Domain 2 as part of this P2PE solution assessment:	*<Report Findings Here>*		
3C-1.1.f Examine the PIM to verify that all P2PE non-payment software specified in the PIM were assessed as part of this P2PE solution assessment (per Requirement **1C-2**).	Identify the P2PE Assessor who confirms that all P2PE non-payment software specified in the PIM were assessed as part of this P2PE solution assessment (per Requirement **1C-2**):	*<Report Findings Here>*		
3C-1.1.g Configure each POI device type, settings, etc. in accordance with all instructions in the PIM and confirm the following: • The PIM provides accurate instructions. • The PIM instructions facilitate a securely installed P2PE solution.	Describe how it was confirmed that by configuring each POI device type, settings, etc. in accordance with all instructions in the PIM, the PIM provides accurate instructions and those instructions facilitate a securely installed P2PE solution:			
	<Report Findings Here>			
3C-1.2 Review P2PE Instruction Manual (PIM) at least annually and upon changes to the solution or the P2PE requirements. Update PIM as needed to keep the documentation current with: • Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and • Any changes to the requirements in this document.		□	□	□

<table>
<tr><th colspan="5">P2PE Merchant-Managed Solution – Reporting</th></tr>
<tr><th rowspan="2">Requirements and Testing Procedures</th><th rowspan="2">Reporting Instructions</th><th colspan="3">Assessor's Findings</th></tr>
<tr><th>In Place</th><th>N/A</th><th>Not In Place</th></tr>
<tr><td><b>3C-1.2.a</b> Examine documented procedures to verify they include:
• PIM must be reviewed at least annually and upon changes to the solution or changes to the P2PE requirements.
• PIM must be updated as needed to keep the document current with:
– Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and
– Any changes to the P2PE requirements.</td><td>Documented procedures reviewed:</td><td colspan="3"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td rowspan="3"><b>3C-1.2.b</b> Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify:
• PIM is reviewed at least annually and upon changes to the solution or changes to the PCI P2PE requirements.
• PIM is updated as needed to keep the document current with:
– Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and
– Any changes to the P2PE requirements.</td><td>Responsible personnel interviewed:</td><td colspan="3"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td colspan="4">Describe how processes for reviewing and updating the PIM verified that the PIM is updated at least annually, upon changes to the solution or changes to the PCI P2PE requirements, and as needed to keep the document current with any changes to the P2PE solution and any changes to the P2PE requirements:</td></tr>
<tr><td colspan="4"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td colspan="2"><b>3C-1.2.1</b> Communicate PIM updates to affected merchants, and provide merchants with an updated PIM as needed.</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td><b>3C-1.2.1.a</b> Examine documented procedures to verify they include communicating PIM updates to affected merchants and providing an updated PIM as needed.</td><td>Documented procedures reviewed:</td><td colspan="3"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td rowspan="2"><b>3C-1.2.1.b</b> Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify PIM updates are communicated to affected merchants and an updated PIM is provided to merchants as needed.</td><td>Responsible personnel interviewed:</td><td colspan="3"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td colspan="4">Describe how processes for reviewing and updating the PIM verified that PIM updates are communicated to affected merchants and an updated PIM is provided to merchants as needed:</td></tr>
</table>

P2PE Merchant-Managed Solution – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor’s Findings**		
		In Place	**N/A**	**Not In Place**
	<Report Findings Here>			
APPENDIX A				
MM-A-1.1 Current documentation must be maintained that describes, or illustrates, the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.		□	□	□
MM-A-1.1.a Interview responsible personnel and review documentation to verify that procedures exist for maintaining documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.	Documented procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
MM-A-1.1.b Interview responsible personnel and review merchant documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs to verify that the document is kept current.	Merchant documentation reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
MM-A-1.2 Decryption systems must reside on a network that is dedicated to decryption operations. Note: The decryption environment must exist within a cardholder data environment (CDE).		□	□	□
MM-A-1.2.a Examine network diagrams to verify that decryption systems are located on a network that is dedicated to decryption operations.	Network diagram(s) reviewed:	*<Report Findings Here>*		
MM-A-1.2.b Inspect network and system configurations to verify that decryption systems are located on a network that is dedicated to decryption operations.	Describe how network and system configurations verified that decryption systems are located on a network that is dedicated to decryption operations:			
	<Report Findings Here>			

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
MM-A-1.3 Systems in the decryption environment must be dedicated to performing and/or supporting decryption and key-management operations: • Services, protocols, daemons, etc. necessary for performing and/or supporting decryption operations must be documented and justified. • Functions not required for performing or supporting decryption operations must be disabled or isolated (e.g., using logical partitions) from decryption operations. *Note: Security functions (e.g., logging and monitoring controls) are examples of functions supporting decryption operations. It is not required that supporting functions be present in the merchant decryption environment; these functions may be resident in the CDE. However, any supporting functions that are present in the decryption environment must be wholly dedicated to the decryption environment.*		□	□	□
MM-A-1.3.a Inspect network and system configuration settings to verify that only necessary services, protocols, daemons, etc. are enabled, and any functions not required for performing or supporting decryption operations are disabled or isolated from decryption operations.	Describe how network and system configuration settings verified that only necessary services, protocols, daemons, etc. are enabled, and any functions not required for performing or supporting decryption operations are disabled or isolated from decryption operations:			
	<Report Findings Here>			
MM-A-1.3.b Review the documented record of services, protocols, daemons, etc. that are required by the decryption systems and verify that each service includes justification.	Documented record of services, protocols, daemons, etc. reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
MM-A-1.4 Systems providing logical authentication services to system components within the decryption environment must: • Reside within the decryption environment • Be dedicated to supporting the decryption environment. **Note:** Logical authentication services may be internal to the HSM management system.		□	□	□
MM-A-1.4.a Examine documented policies and procedures, and interview responsible personnel to verify that systems providing logical authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
MM-A-1.4.b Review system configurations and observe processes to verify that systems providing authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.	Describe how system configurations verified that systems providing authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment:			
	<Report Findings Here>			
MM-A-1.5 Logical administrative/privileged access to systems within the decryption environment must be authorized and must originate from within the merchant decryption environment.		□	□	□
MM-A-1.5.a Examine documented policies and procedures, and interview responsible personnel to verify that logical administrative/privileged access to the systems within the decryption environment must be authorized and originate from within the merchant decryption environment.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor’s Findings		
		In Place	N/A	Not In Place
MM-A-1.5.b Examine firewall/router configurations to verify that logical administrative/privileged access to systems within the decryption environment is authorized and originates from within the merchant decryption environment.	Describe how firewall/router configurations verified that logical administrative/privileged access to systems within the decryption environment is authorized and originates from within the merchant decryption environment:			
	<Report Findings Here>			
MM-A-1.6 All remote access features on all systems in the merchant decryption environment must be permanently disabled and/or otherwise prevented from being used.		□	□	□
MM-A-1.6 Review system configurations and observe processes to verify that all remote access features on all systems within the merchant decryption environment are permanently disabled and/or otherwise prevented from being used.	Describe how system configurations verified that all remote access features on all systems within the merchant decryption environment are permanently disabled and/or otherwise prevented from being used:			
	<Report Findings Here>			
MM-A-1.7 Systems in the merchant decryption environment must not store account data.		□	□	□
MM-A-1.7.a Review configurations of all devices and systems in the merchant decryption environment to confirm none of the systems store account data.	Identify the P2PE Assessor who confirms that configurations of all devices and systems in the merchant decryption environment were reviewed and confirmed that none of the systems store account data:	*<Report Findings Here>*		
	Describe how configurations of all devices and systems in the merchant decryption environment confirmed that none of the systems store account data:			
	<Report Findings Here>			
MM-A-1.7.b Review data flows and interview personnel to verify that account data is not stored in the merchant decryption environment.	Personnel interviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
MM-A-2.1 Firewalls must be in place to restrict connections between the merchant decryption environment and all other networks. Firewalls must be configured to restrict traffic as follows:		□	□	□
MM-A-2.1 Review documentation and observe network configurations to verify that firewalls are in place between the merchant decryption environment and all other networks.	Documentation reviewed:	*<Report Findings Here>*		
	Describe how network configurations verified that firewalls are in place between the merchant decryption environment and all other networks:			
	<Report Findings Here>			
MM-A-2.1.1 Inbound and outbound traffic to/from the decryption environment must be restricted to only IP addresses within the CDE.		□	□	□
MM-A-2.1.1 Examine firewall and router configurations to verify that inbound and outbound traffic to/from the decryption environment is limited to only IP addresses within the CDE.	Describe how firewall and router configurations verified that inbound and outbound traffic to/from the decryption environment is limited to only IP addresses within the CDE:			
	<Report Findings Here>			
MM-A-2.1.2 Inbound and outbound traffic between the decryption environment and any CDE must be restricted to only that which is necessary for performing and/or supporting decryption operations, with all other traffic specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).		□	□	□
MM-A-2.1.2.a Review firewall configuration standards to verify that inbound and outbound traffic necessary for performing and/or supporting decryption operations is identified and documented.	Firewall configuration standards reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
MM-A-2.1.2.b Examine firewall configurations to verify that inbound and outbound traffic between the decryption environment and any CDE is limited to only that which is necessary for performing and/or supporting decryption operations, and all other traffic is specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).	Describe how firewall configurations verified that inbound and outbound traffic between the decryption environment and any CDE is limited to only that which is necessary for performing and/or supporting decryption operations, and all other traffic is specifically denied: *<Report Findings Here>*			
MM-A-2.2 Inbound and outbound traffic between the merchant CDE and the encryption environment must be restricted to approved POI devices located within the encryption environment.		□	□	□
MM-A-2.2 Examine network and system configurations to verify that inbound and outbound traffic between the merchant CDE and the encryption environment is restricted to approved POI devices located within the encryption environment.	Describe how network and system configurations verified that inbound and outbound traffic between the merchant CDE and the encryption environment is restricted to approved POI devices located within the encryption environment: *<Report Findings Here>*			
MM-A-2.3 Processes must be implemented to prevent unauthorized physical connections (e.g., wireless access) to the decryption environment as follows: • Wireless connections to the decryption environment are prohibited. • Processes are implemented to detect and immediately (as soon as possible) respond to physical connections (e.g., wireless connections) to the decryption environment.		□	□	□
MM-A-2.3.a Review document policies and procedures to verify that wireless connections to the decryption environment are prohibited**.**	Documented policies and procedures reviewed:	*<Report Findings Here>*		

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
MM-A-2.3.b Observe processes and interview personnel to verify a methodology is implemented to immediately (e.g., ASAP) detect, identify, and eliminate any unauthorized physical connections (e.g., wireless access points) that connect to the decryption environment.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how observed processes verified that a methodology is implemented to immediately detect, identify, and eliminate any unauthorized physical connections that connect to the decryption environment:			
	<Report Findings Here>			
MM-A-2.3.c Examine firewall/router configurations to confirm that all wireless networks are prevented from connecting to the decryption environment.	Describe how observed processes verified that a methodology is implemented to immediately detect, identify, and eliminate any unauthorized physical connections that connect to the decryption environment:			
	<Report Findings Here>			
MM-B-1.1 Traffic between the encryption environment and any other CDE must be limited as follows: • Only those systems (e.g., POI devices) directly related to supporting P2PE transactions, and • Only traffic that is necessary for transaction processing and/or terminal management purposes. • All other traffic between the encryption environment and any other CDE must be specifically denied.		☐	☐	☐
MM-B-1.1.a Review documentation to verify that inbound and outbound traffic necessary for transaction processing and/or terminal management purposes is identified and documented.	Documentation reviewed:	*<Report Findings Here>*		
MM-B-1.1.b Examine firewall configurations to verify that any traffic between the encryption environment and any other CDE is limited as follows: • Only those systems (e.g., POI devices) directly related to supporting P2PE transactions, and	Describe how firewall configurations verified that any traffic between the encryption environment and any other CDE is limited to only those systems directly related to supporting P2PE transactions:			
	<Report Findings Here>			

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
• Only traffic that is necessary for transaction processing and/or terminal management purposes. • Verify all other traffic between those two networks is specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).	Describe how firewall configurations verified that any traffic between the encryption environment and any other CDE is limited to only traffic that is necessary for transaction processing and/or terminal management purposes:			
	<Report Findings Here>			
MM-B-1.1.c Observe traffic between the encryption environment and any other CDE to verify the traffic is limited to systems directly related to supporting P2PE transactions, transaction processing, and/or terminal-management functions.	Describe how the observed traffic between the encryption environment and any other CDE verified that the traffic is limited to systems directly related to supporting P2PE transactions, transaction processing, and/or terminal-management functions:			
	<Report Findings Here>			
MM-B-1.2 Processes must be implemented to prevent clear-text account data from being transmitted from the CDE back to the encryption environment.		□	□	□
MM-B-1.2.a Review documented policies and procedures for the CDE to verify that the transmission of clear-text account data from the CDE back to the encryption environment is prohibited.	Documented policies and procedures for the CDE. reviewed:	*<Report Findings Here>*		
MM-B-1.2.b Observe processes and interview personnel to verify clear-text account data is prevented from being transmitted from the CDE back to the encryption environment.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how firewall configurations verified that any traffic between the encryption environment and any other CDE is limited to only those systems directly related to supporting P2PE transactions:			
	<Report Findings Here>			
MM-B-1.2.c Using forensic techniques, observe traffic between the encryption environment and the CDE to verify clear-text account data is not transmitted from the CDE back to the encryption environment.	Forensic techniques used:	*<Report Findings Here>*		
	Describe how the observed traffic between the encryption environment and the CDE verified that clear-text account data is not transmitted from the CDE back to the encryption environment:			
	<Report Findings Here>			

P2PE Merchant-Managed Solution – Reporting

Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
		In Place	N/A	Not In Place
MM-C-1.1 Separation of duties must exist such that encryption environment personnel are prohibited from accessing any system components in the decryption environment or any CDE. Access-control mechanisms must include both physical and logical controls. ***Note**: Access restrictions between the encryption and decryption environment are not intended to prohibit employees who work in the decryption environment or CDE from shopping in the stores. This requirement is focused on logical access controls, not physical.*		□	□	□
MM-C-1.1.a Examine documented policies and procedures, and interview responsible personnel to verify that encryption environment personnel are prohibited from accessing any system components in the decryption environment or the CDE.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
MM-C-1.1.b For a sample of system components in the CDE and the decryption environment, review system configurations and access-control lists to verify that encryption environment personnel do not have access to any system components in the decryption environment or the CDE.	Sample of system components in the CDE:	*<Report Findings Here>*		
	Sample of system components in the decryption environment:	*<Report Findings Here>*		
	Describe how system configurations and access control lists verified that encryption environment personnel do not have access to any system components in the decryption environment or the CDE:			
	<Report Findings Here>			
	Describe how the observed traffic between the encryption environment and the CDE verified that clear-text account data is not transmitted from the CDE back to the encryption environment:			
	<Report Findings Here>			