Payment Card Industry (PCI)

Point-to-Point Encryption
P2PE Merchant-Managed Solution

Template for Report on Validation
for use with P2PE v3.0 for P2PE
Merchant-Managed Solution Assessments

December 2019

Document Changes

Date	Use with Version	Template Revision	Description
November 2015	P2PE v2.0, Revision 1.1	Revision 1.0	To introduce the template for submitting P2PE Reports on Validation for P2PE Solutions assessed against the P2PE v2 Standard. *This document serves as both the Reporting Template and Reporting Instructions document; there are not separate documents for this under P2PE v2 as there are still under P2PE v1*
December 2019	P2PE v3.0	Revision 1.0	P2PE Version 3.0 P-ROV for Merchant-Managed Solution Assessments

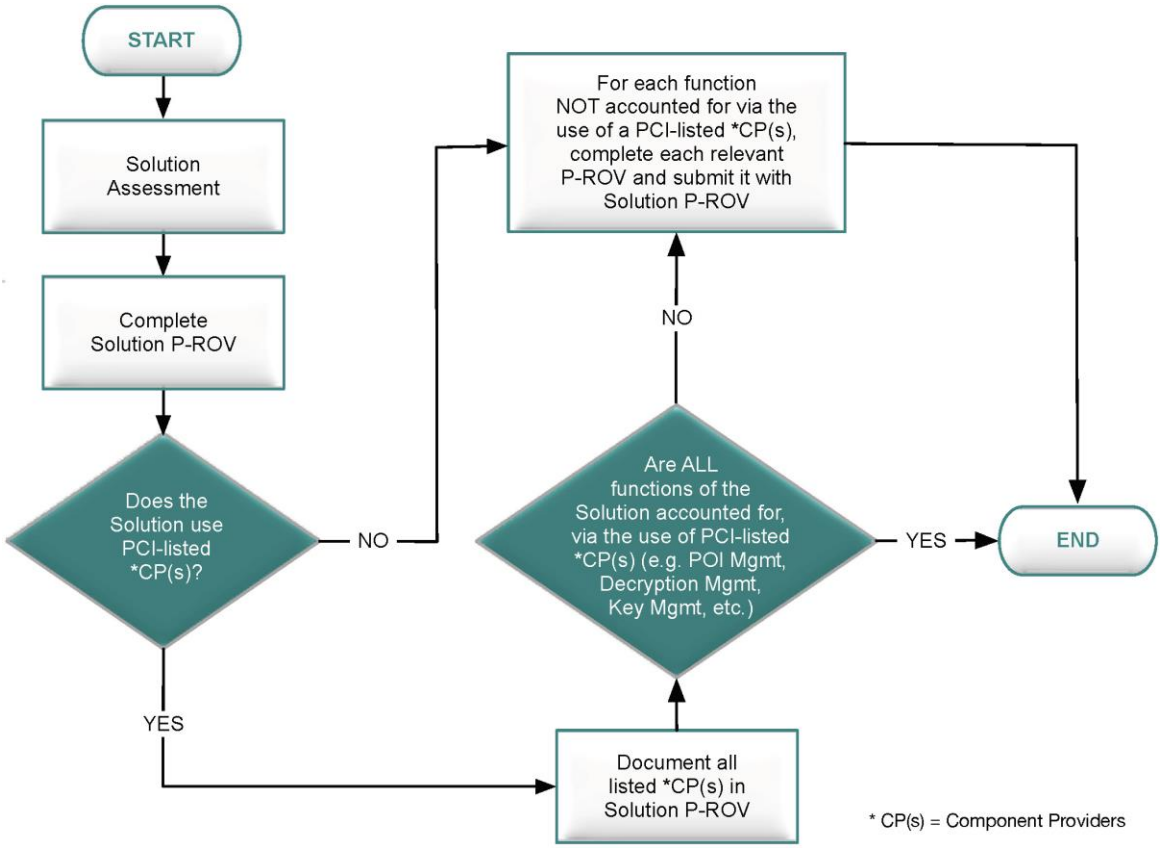
Contents

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 v3.0 for P2PE Merchant-Managed Solutions* ("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, v3.0* ("P2PE v3.0 Standard"). This Reporting Template provides reporting instructions and the template form for QSA (P2PE) and QSA (PA-P2PE) assessors to provide a more consistent level of reporting. MMS assessments are not submitted to PCI SSC - please see the P2PE Program Guide for further details.

Use of this Reporting Template is mandatory for all P2PE v3.0 P2PE Merchant-Managed Solution assessments.

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



The table below summarizes the P2PE v3.0 P-ROVs and the applicability of each P-ROV relative to the assessment type. The following acronyms are used: CP = Component Provider.

P-ROV Name	Used for the Following 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.
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 POI devices in a P2PE Merchant-Managed Solution. Merchant-Managed Solution assessments that do not outsource the entirety of their Encryption Management Services to PCI-Listed Component Providers, either to an EMCP or to BOTH a PDCP AND a PMCP, must complete this P-ROV in addition to the Solution P-ROV. Component Provider assessments for an EMCP, PDCP, or a PMCP must complete this P-ROV.
P2PE Application	P2PE Application	Any assessment that utilizes software on the POI devices intended for use in a P2PE Merchant-Managed Solution that has the potential to access clear-text cardholder data must complete this P-ROV.
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 devices (e.g., HSMs) used to support a P2PE Merchant-Managed Solution. Merchant-Managed Solution assessments that do not outsource the entirety of their Decryption Management Services to a PCI Listed DMCP must complete this P-ROV in addition to the Merchant-Managed Solution P-ROV. Component Provider assessments for a DMCP must complete this P-ROV.

P-ROV Name	Used for the Following Assessments	Purpose
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. Merchant-Managed Solution assessments that have not satisfied the key management services requirements (Domain 5) either through the use of PCI-listed 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 any other relevant key management service that has not already been assessed as part of the inclusion of a PCI-listed Component Provider, then the Solution assessment must include the use of the KMS P-ROV. Component Provider assessments for a KIF, KMCP, KLCP, or a CA/RA must complete this P-ROV.

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, or to change column width. 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 v3.0 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.

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 on-going 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. A summary of all findings is also at 2.7, "Summary of P2PE Compliance Status."

The following table is a representation when considering which selection to make. Remember, 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. This may be a mix of In Place and Not Applicable responses, but no Not in Place response. 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)	The requirement does not apply to the P2PE Product. All Not Applicable responses require reporting on testing testing performed (including interviews conducted and documentation reviewed) and must explain how it was determined that the requirement does not apply. There is no need to repeat lengthy responses where related requirements are not applicable.

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, the reporting instruction, or such 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 3.6, "Documentation Reviewed," and 3.7, "Individuals Interviewed," there is a space for a reference number and ***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. Again, where applicable, it is the P2PE Assessor's choice to list out each sample within reporting or to utilize sample identifiers from the sampling summary table.

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

  These are the only reporting instructions that will stretch across half of the table; the above are all a quarter-table's width to serve as a visual indicator of detail expected in response. 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.

P-ROV Merchant-managed Solution Template for P2PE v3.0 Standard

This template is to be used for creating a P2PE Report on Validation for P2PE Merchant-Managed Solutions assessed against P2PE v3.0. Content and format for this P-ROV is defined as follows.

1. Contact Information and Report Date

1.1 Contact Information				
P2PE MMS Provider contact information				
Company name:		Company URL:		
Company contact name:		Contact e-mail address:		
Contact phone number:		Company address:		
P2PE 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 submission, per requirements in relevant program documentation.		☐ Yes ☐ No (if no, this is not in accordance with PCI Program requirements)		
QA reviewer name:		Assessor credentials: (Leave blank if not applicable)		
QA reviewer phone number:		Assessor e-mail address:		
P2PE additional Assessor contact information *(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:		Timeframe of assessment:	

Additional services provided by PA-QSA(P2PE)/QSA (P2PE)/QSA company	
The P2PE QSA (P2PE) and PA-QSA (P2PE) Qualification Requirements v2.1, Section 2.2 "Independence" specifies requirements for 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 Validation Requirements, to ensure responses are consistent with documented obligations.	
▪ Disclose all services offered to the assessed entity by the PA-QSA(P2PE)/QSA (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:	

1.3 P2PE Version	
Version of the P2PE Standard used for the assessment (should be v3.0):	

2. Summary Overview

2.1 P2PE Submission Details	
P2PE MMS name (and version if applicable):	
Description of P2PE MMS Provider's business:	
Description of the typical use/implementation of this solution (Include specific industries or channels the solution is intended for):	

2.2 Summary of Component Providers Used by the Merchant-Managed Solution

Notes: *Where a function is NOT covered using a Component Provider, an additional P-ROV must be submitted - please indicate this using the column "Additional P-ROV included in this submission" below.*

PCI-Listed Components	Additional P-ROV included in submission	Included as a Listed Component	Component Provider Name	Component Name	PCI SSC Reference #	Comments
If the MMS does not use a PCI-listed EMCP, or only uses either a PDCP **or** a PMCP, then the Encryption Management Services (EMS) P-ROV must be completed for all applicable requirements and submitted in addition to this MMS P-ROV.						
Encryption Management Component Provider (*EMCP*)	☐ Yes ☐ No	☐ Yes ☐ No				
POI Deployment Component Provider (*PDCP*)	☐ Yes ☐ No	☐ Yes ☐ No				
POI Management Component Provider *(PMCP)*	☐ Yes ☐ No	☐ Yes ☐ No				
If the MMS uses applications that can access clear-text account data that is not PCI-listed P2PE Applications, then the P2PE Application P-ROV must be completed and submitted in addition to this MMS P-ROV for each P2PE Application.						
P2PE Application	☐ Yes ☐ No	☐ Yes ☐ No	Please include Applications in Table 2.3 below			
If the MMS does not use a PCI-listed Decryption Management Component Provider, then the Decryption Management Services (DMS) P-ROV must be completed for all applicable requirements and submitted in addition to this MMS P-ROV.						
Decryption Management Component Provider *(DMCP)*	☐ Yes ☐ No	☐ Yes ☐ No				
MMS assessments that have not satisfied the Key Management Services (KMS) requirements (Domain 5) either through the use of PCI-listed Component Providers and/or through the assessment of their Encryption Management Services and/or Decryption Management Services must complete the KMS P-ROV.						
Key Injection Facilities	☐ Yes ☐ No	☐ Yes ☐ No				
Key Management Component Provider (*KMCP*)	☐ Yes ☐ No	☐ Yes ☐ No				
Key Loading Component Provider (*KLCP*)	☐ Yes ☐ No	☐ Yes ☐ No				
Certification Authority / Registration Authority (CA/RA)	☐ Yes ☐ No	☐ Yes ☐ No				

2.2.a Other Third-Party Service Provider entities involved in P2PE Merchant-Managed Solution

This could include KIFs, CA/RAs, Encryption Management Services and Decryption Management Services who have opted NOT to list with PCI SSC as a P2PE Component and therefore must be assessed fully for each P2PE solution the service is used in. This could also include other third-party service providers in use as applicable, including authorized Integrator/Resellers and such.

"Other details" is to be used as needed. For example, if there is a third-party service provider providing decryption services but it not a P2PE Component at 2.2, use "Other details" to address data such as P2PE endpoint system identifier (e.g., Host System and HSM). Mark as "n/a" if no other details are needed.

Entity Name:	Role/Function:	Entity Location(s):	Other Details, if needed:

2.3 P2PE Applications used in the Merchant-Managed Solution

***Note**: If the Merchant-managed Solution uses applications that can access clear-text account data that are not PCI-listed P2PE Applications, then a P2PE Application P-ROV must be completed - i.e., the application must undergo a full assessment against Domain 2 by a PA-QSA (P2PE) - in addition to this P-ROV for each P2PE Application that is not already listed.*

Application Vendor Name:	Application Name:	Application Version #:	PCI SSC Reference #

2.4 PTS-approved POI Devices Supported

List of all POI device types supported and tested as part of Merchant-Managed Solution's P2PE Assessment

PTS Approval #:	Make/ Manufacturer:	Model Name/ Number:	Hardware #:	Firmware #(s):	Any additional Applications on POI devices (add rows as needed to report all applications)		
					Application Name:	Version #	CHD Access? (see note below)
							☐ Yes ☐ No
							☐ Yes ☐ No
							☐ Yes ☐ No
							☐ Yes ☐ No

***Note**: If the Merchant-Managed Solution uses applications that can access clear-text account data and are not PCI-listed P2PE Applications, a P2PE Application P-ROV must be completed—i.e., the application must undergo a full assessment against Domain 2 by a PA-QSA (P2PE)—in addition to this P-ROV for each P2PE Application that is not already listed.*

Functionality provided (for all POI device types supported)
The columns below represent review of the PTS Listing approval details (to be reported under “PTS Listing”) as well as the observed device configuration (to be reported under “P2PE”). This table will match what functionality was listed for PTS against what is observed as being utilized for P2PE in order to identify and resolve any discrepancies. SRED is not noted below, as it is addressed at Requirement 1A-1.1.

Model Name/ Number:	OP		ICCR		MSR		Contactless	
	PTS Listing	P2PE	PTS Listing	P2PE	PTS Listing	P2PE	PTS Listing	P2PE
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N

Note: *If there is a different response for PTS Listing compared to P2PE Functionality for account-data-capture interfaces provided with the POI device, this will need to be addressed (including at applicable Domain 1 1 testing procedures) to ensure such functionality is specifically disabled or configured to prevent their use in P2PE Solutions.*

External communication methods (for all POI device types supported)
Report in each column whether the device configurations for each of the PTS POI device types supported was observed to support the following external communication methods. Mobile Communications may include the following: GPRS, 2G, 3G, 4G, 5G etc.

Model Name/ Number:	Bluetooth	Ethernet	Serial	USB	Mobile Communications
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N
	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N	☐ Y ☐ N

2.5 All other Secure Cryptographic Devices (SCDs)

Details for all HSMs used in the MMS Solution

Identifier Type	PTS Approval or FIPS #:	Manufacturer/ Model Name/ Number:	Hardware#(s)	Firmware#(s)	Location:	# of devices per location:	Approved key function(s) & Purpose:

2.7 Summary of P2PE Compliance Status

P2PE Function	Compliant	Comments (optional):
P2PE Merchant-Managed Solution Management	☐ Yes ☐ No ☐ N/A	
Encryption Management Services		
Encryption Management	☐ Yes ☐ No ☐ N/A	
POI Deployment	☐ Yes ☐ No ☐ N/A	
POI Management	☐ Yes ☐ No ☐ N/A	
P2PE Application	☐ Yes ☐ No ☐ N/A	
Decryption Management Services		
Decryption Management	☐ Yes ☐ No ☐ N/A	
Key Management Services		
Key Injection Facility	☐ Yes ☐ No ☐ N/A	
Key Management	☐ Yes ☐ No ☐ N/A	
Key Loading	☐ Yes ☐ No ☐ N/A	
Certification Authority / Registration Authority	☐ Yes ☐ No ☐ N/A	

3. Details and Scope of P2PE Assessment

3.1 Scoping Details

Describe how the P2PE assessor validated the accuracy of the P2PE scope for the assessment, including:

- Describe the methods or processes used to identify all elements in scope of the P2PE assessment:

- Describe how the P2PE assessor confirmed that the scope of the assessment is accurate and covers all components and facilities for the MMS assessment:

3.2 MMS Network Diagram

Provide one or more ***high-level*** network diagrams to illustrate the functioning of the P2PE MMS, including:

- Locations of critical facilities, including the solution provider's decryption environment, key-injection and loading facilities, etc.
- Location of critical components within the P2PE decryption environment, such as the Host System, 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
- Other necessary components, as applicable to the particular MMS

<Insert P2PE Merchant-Managed Solution network diagram(s)>

3.3 Overview of P2PE MMS data flow

Provide a ***high-level*** data-flow diagram of the merchant-managed solution that illustrates:

- Flows and locations of encrypted account data
- Flows and locations of clear-text account data
- Location of critical system components (e.g., HSMs, Host System)
- All entities the solution 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 locations and an icon that represents the MMS provider's decryption environment.*

<Insert P2PE Merchant-Managed Solution data-flow diagram(s)>

3.4 Key-management processes

Description of Cryptographic Key Management Processes

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)

Note: *Include both logical and physical components—e.g., network traffic flows, locations of safes, use of secure couriers, etc.*

<Insert applicable diagram(s) showing all key-management processes>

Description of Cryptographic Keys used in P2PE Merchant-Managed Solution	
Provide a brief description of all types of cryptographic keys used in the solution, as follows:	
Key type / description	Purpose/ function of the key

3.5 Facilities

Lab environment used by the P2PE Assessor for this assessment	
Identify whether the lab was provided by the P2PE Assessor or the MMS Provider:	☐ P2PE Assessor's Lab ☐ MMS Provider's Lab
Address of the lab environment used for this assessment:	
Describe the lab environment used for this assessment:	

List of all facilities INCLUDED in this MMS assessment	
Description and purpose of facility included in assessment	Address of facility

List of facilities used in MMS assessment that were EXCLUDED from this Merchant-Managed Solution assessment*			
Description and purpose of facility excluded from assessment	Address of facility	Explanation why the facility was excluded from the assessment	Details of any separate assessments performed for the facility, including how the other assessment was verified to cover all components in scope for this Merchant-Managed Solution

**** Note:** Does not include merchant locations.*

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, such as if it is for a different POIs, for different functions, etc.*

There is no need to duplicate documents that appear in other P-ROVs included unless they are relevant to the MMS 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)	Which P2PE Application is addressed? (Must align with Section 2.3)

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 Section 2.3)

All other documentation reviewed for this P2PE Assessment:			
Reference # (optional use)	Document Name (including version, if applicable)	Document date (latest version date)	Document Purpose

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 MMS Management Controls.

Reference # (optional use)	Interviewee's Name	Company	Job Title

3.8 Device Samples for P2PE Assessment

Complete for all sampled devices in the P2PE assessment, including for every POI device type at Section 2.4 above and every other SCD type at Section 2.5 above.

***Note:** Use of the "Sample Reference #" is optional, but if not used here, all of the sample's serial numbers or other identifiers in the third column will need to be included in the reporting findings.*

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

Sample Ref #: (optional)	Sample Size	Serial Numbers of Tested Devices/Other Identifiers	Sampling Rationale

4. Findings and Observations

Where functions are marked as "Additional P-ROV included in submission" in Table **2.2 Summary of Components Consumed by Merchant-Managed Solution**, please ensure the relevant P-ROVs are included with the submission.

Reference *Appendix I: P2PE Applicability of Requirements* in the P2PE v3.0 Program Guide.

P2PE Merchant-Managed Solution – Summary of Findings

P2PE Validation Requirements	Summary of Findings (check one)		
	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)		
		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 and Assessor's Findings**	
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>*
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>*

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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.		
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	Documented procedures reviewed:	*<Report Findings Here>*
	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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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.*		

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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 and Assessor's Findings**	
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 and Assessor's Findings**	
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>*
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>*

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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 each third party is responsible for • 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.		
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>*

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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.		

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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>*

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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.		

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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.		

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
3C-1.2.a 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.	Documented procedures reviewed:	*<Report Findings Here>*
3C-1.2.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	Responsible personnel interviewed:	*<Report Findings Here>*
	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:	
	<Report Findings Here>	
3C-1.2.1 Communicate PIM updates to affected merchants, and provide merchants with an updated PIM as needed.		
3C-1.2.1.a Examine documented procedures to verify they include communicating PIM updates to affected merchants and providing an updated PIM as needed.	Documented procedures reviewed:	*<Report Findings Here>*
3C-1.2.1.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.	Responsible personnel interviewed:	*<Report Findings Here>*
	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:	
	<Report Findings Here>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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 and Assessor's Findings**	
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>*
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	Documented policies and procedures reviewed:	*<Report Findings Here>*

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
the decryption environment and are dedicated to supporting the decryption environment.	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>*
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	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:	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>*
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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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 • 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 those systems directly related to supporting P2PE transactions:	
	<Report Findings Here>	
	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>	

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>	
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.*		

P2PE Merchant-Managed Solution – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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>	