Payment Card Industry (PCI)

Point-to-Point Encryption
Encryption Management Services

Template for Report on Validation for use with P2PE v3.1 for P2PE Encryption Management Services Assessments

September 2021

Document Changes

Date	Use with P2PE Standard Version	Template Revision	Description
December 2019	P2PE v3.0	Revision 1.0	To introduce the template for submitting P2PE Reports on Validation for P2PE Solutions and Components assessed against the P2PE v3.0 Standard for Encryption Management Services. 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". - 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. - Instructions added where applicable regarding the use of this template for EMS Component assessments vs. Solution assessments. - 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. - Updates to section 4 to align with the updates from the P2PE v3.1 Standard, in addition to errata. - 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 Encryption Management Services

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

EMS Component Assessments: Use of this Reporting Template is mandatory for all P2PE v3.1 Encryption Management Services Component Provider assessments.

Solution Assessments: Use of this Reporting Template is mandatory for all P2PE v3.1 Solution (*and Merchant-managed Solution*) assessments, where the Solution Provider is directly responsible for all or part of the Encryption Management Services requirements (i.e., when they have not completely satisfied the full scope of their encryption management services via the use of Validated Encryption Management Services P2PE Component Providers).

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 comprehensive ***summary of testing activities performed and information collected*** during the assessment against the P2PE Standard. The information contained in a P-ROV must provide enough detail and coverage to verify that the P2PE submission is compliant with all applicable P2PE requirements.

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

P-ROV	APPLICABLE ASSESSMENTS	PURPOSE
Solution	Solution (SP)	The Solution P-ROV is mandatory for all P2PE Solution assessments, at a minimum. Additional P-ROVs (below) may be required depending on the scope of the assessment. ***Note:*** *A separate Merchant-Managed Solution (MMS) P-ROV is used for MMS assessments. References to "Solution P-ROV" below can be substituted with "MMS P-ROV" for MMS assessments.*
Encryption Management Services (EMS)	Solution (SP) 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 Solution. **Solution assessments** that have not satisfied the entirety of their Encryption Management Services (Domain 1 with Domain 5) via the use of Validated Component Providers must complete the EMS P-ROV in addition to the Solution P-ROV. **Component Provider assessments** for an EMCP, PDCP, or a PMCP must complete the EMS P-ROV.
P2PE Application	P2PE Application	Any assessment that utilizes software on the PTS-approved POI devices intended for use in a P2PE Solution that has the potential to access clear-text account data must complete a P2PE Application P-ROV (one for each application).
Decryption Management Services (DMS)	Solution (SP) 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 Solution. **Solution assessments** that have not satisfied the entirety of their Decryption Management Services (Domain 4 with Domain 5) to applicable Validated P2PE Component Providers must complete the DMS P-ROV in addition to the Solution P-ROV. **Component Provider assessments** for a DMCP must complete the DMS P-ROV.
Key Management Services (KMS)	Solution (SP) 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. **Solution assessments** that have not satisfied the entirety of 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 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 Validated P2PE Component Provider and/or as part of the Domain 1 and Domain 4 assessment scope of the Solution assessment, 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 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. 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. 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 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 is 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 type. ▪ 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 Encryption Management Services Template for the P2PE v3.1 Standard

This use of this template is mandatory for creating a P2PE Report on Validation (P-ROV) for submission to PCI SSC for P2PE Solutions (as applicable) and P2PE Components assessed to the P2PE Standard. Complete the remainder of this P-ROV as instructed.

1. Contact Information and Report Date

1.1 Contact Information				
Solution/Component 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 submission, 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) / P2PE QSA company.	

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

2. Summary Overview

2.1 P2PE Assessment Details			
Solution or Component Assessment			
Is this P-ROV being submitted as part of a Solution assessment or for an EMS Component assessment?	☐ Solution	If **Solution**, enter the Solution Name: (*Complete this P-ROV with the Solution P-ROV*)	
	☐ EMS Component	If **EMS Component**, complete the *P2PE Component Details* below.	

P2PE Component Details (*for EMS Component assessments ONLY*)				
P2PE Component Name:		Is the Component already (or was it previously) listed on the PCI SSC List of Validated P2PE Components?	☐ Yes (*If **Yes**, provide listing reference #*):	
			☐ No (*If **No,** the component has never been listed*)	

P2PE EMS Component Type for this assessment. Select **one** of the following: *(Do not check anything for Solution Assessments)*		
☐ Encryption Management Component Provider (EMCP)	☐ POI Deployment Component Provider (PDCP)	☐ POI Management Component Provider (PMCP)

2.2 Validated P2PE Component Providers

SOLUTION ASSESSMENTS: Only document Validated P2PE Component Providers here that are being used to partially satisfy applicable EMS requirements that are not being met by the Solution Provider. E.g., a full EMCP must be documented in the Solution P-ROV. Do **not** list P2PE Components used for non-EMS related requirements here.

EMS COMPONENT ASSESSMENTS: Complete this table if Validated P2PE Component Providers are being used to help satisfy applicable requirements for this EMS Component assessment.

For every PDCP and PMCP Component below, document the PTS Approval #s associated with their respective Validated P2PE Component listing that are being included in this assessment. The PTS approval #s here must also be present in Table 2.5. For non-EMS Component Types denote "**N/A**" in the PTS Approval # column.

Note 1: *It is not permissible to use a PCI-listed P2PE Component Provider of the same type as the entity under assessment. A PCI-listed EMCP cannot be used to satisfy the requirements of an EMCP under assessment. This applies to all Component type assessments.*

Note 2: *The use of PCI-listed P2PE Component Providers must be considered Validated. Refer to the P2PE Program Guide for additional details.*

Note 3: *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 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 requirements that were not covered under its associated Component Type assessment. Reference the "P2PE Applicability of Requirements" in the P2PE Program Guide.*

Are Validated P2PE Component Providers being used to help satisfy requirements of this assessment?	☐ Yes (*If **Yes,** document below accordingly. Ensure all remaining applicable requirements are assessed and satisfied as they relate to the full scope of the assessment.)*
	☐ No (*If **No,** leave the remainder of this table blank. Ensure all applicable requirements are assessed and satisfied as they relate to the full scope of the assessment.)*

Type of Validated P2PE Component (*select ONLY one Component Type per row*)						**P2PE Component Provider Name**	**P2PE Component Name**	**Validated Listing Reference #**	**PTS Approval #(s) (*comma delimited*)**
PDCP	**PMCP**	**KIF**	**KMCP**	**KLCP**	**CA/RA**				
☐	☐	☐	☐	☐	☐				
☐	☐	☐	☐	☐	☐				
☐	☐	☐	☐	☐	☐				
☐	☐	☐	☐	☐	☐				

Validated P2PE Component Providers Continued
Describe how the Validated P2PE Component Provider(s) are being used to satisfy applicable P2PE requirements for this Encryption Management Services assessment. If more than one Validated P2PE Component Provider is being used, clearly distinguish between them in the description. Provide more detail than simply, e.g., "*The KIF is satisfying Domain 5 for the EMCP*". Do **not** leave this blank unless ***No*** was checked above.
<Description>

2.3 Third-Party Entities Involved in the Encryption Management Services

Use Table 2.2 for the use of applicable 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 additional information.

SOLUTION ASSESSMENTS: Document the use of all Third Parties as they relate to (***only***) Encryption Management Services here. It is not necessary to duplicate this information in the Solution P-ROV.

EMS COMPONENT ASSESSMENTS: Document the use of all applicable Third Parties.

Are Third Party entities involved in the scope of Encryption Management Services for this assessment?	☐ Yes (*If **Yes**, provide details below - insert additional rows as necessary*)	☐ 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.

SOLUTION ASSESSMENTS: All non-payment software used by the Solution must be accounted for and satisfy requirement 1C-2.

EMS COMPONENT ASSESSMENTS: Complete this table as applicable. Note that non-payment software is not listed, and as such, any non-payment software, while it must be accounted for in the scope of the EMS assessment, cannot be used in another Component or Solution without being reassessed.

Non-payment software is any software/files that does **not** have the potential to access clear-text account data. (Refer to P2PE Glossary)

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.*

Insert additional rows as necessary.

Non-payment Software Name	Software Version #	Software Vendor Name	Does the software have the potential to access to clear-text account data? **Note:** An applicable "YES" response is **not** acceptable as this does not qualify as non-payment software. Refer to Table 2.4.b for P2PE Applications.
			☐ No
			☐ No
			☐ No

2.4.b Validated P2PE Applications

SOLUTION ASSESSMENTS: If the Solution is using its own application that has the potential to access clear-text account data, the Solution Provider can choose whether or not to pursue listing the application on the List of Validated P2PE Applications. Whether intended to list the application or not, 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.

EMS COMPONENT ASSESSMENTS: The use of any non-Validated applications that have the potential to access clear-text account data requires a P2PE Application P-ROV and associated Domain 2 assessment. P2PE Component assessments are not permitted to include non-Validated P2PE Applications (i.e., applications that can access clear-text account data must be listed on the List of Validated P2PE Applications). This table is only for Validated P2PE Applications.

ONLY list the PTS Approval #s from each Validated P2PE Application in use that are actually supported by the P2PE Component or 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:

- **SOLUTION ASSESSMENTS ONLY:** 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 assessment. **OR,**
- **SOLUTION AND COMPONENT ASSESSMENTS**: 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 P2PE Component or Solution assessment (this will be unique for each 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

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 – SOLUTION ASSESSMENTS ONLY

! DO NOT COMPLETE THIS TABLE FOR P2PE COMPONENT ASSESSEMENTS !

SOLUTION ASSESSMENTS: If the Solution is using its own application that has the potential to access clear-text account data, the Solution Provider can choose whether or not to pursue listing the application on the List of Validated P2PE Applications. Whether intended to list the application or not, 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 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 non-Validated P2PE Applications included in the scope of the Solution assessment where the Solution Provider is choosing not to separately list the application?	☐ No (*If **No**, leave remainder of this table blank*)
	☐ Yes (*If **Yes**, 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

SOLUTION ASSESSMENTS & EMS COMPONENT ASSESSMENTS: Complete this table as instructed.

- Only list each unique PTS Approval # **once**.
- List ALL associated hardware (HW) and firmware (FW) versions **supported** by the Encryption Management Services or 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 Component and Solution 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:*
  - ***SOLUTION ASSESSMENTS ONLY:*** *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****,*
  - ***SOLUTION AND COMPONENT ASSESSMENTS*** *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 P2PE Component or Solution 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 P2PE Component or Solution assessment (this will be unique for each assessment).*

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

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 (Only an option for Solution assessments)*" **OR** "*A combination of applicable Validated P2PE Components and an assessment to the remaining requirements in section 4 below*" **OR** "*A complete assessment to all applicable requirements in Domains 1 and 5 in section 4 below*"

2.6 Secure Cryptographic Devices (SCDs)

List the SCD types used as part of the Encryption Management Services

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.

SOLUTION ASSESSMENTS: Document the use of all SCDs as they relate to (***only***) Encryption Management Services here. It is not necessary to duplicate this information in the Solution P-ROV.

EMS COMPONENT ASSESSMENTS: Complete this table as applicable.

Note: *PTS-approved POI device information used for account-data capture and encryption must be entered in Table 2.5. Do* ***not*** *enter it here.*

Insert additional rows as necessary.

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 or multi-P2PE Solution 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 are involved in supporting additional encryption implementations.

Insert additional rows as necessary.

PTS Approval # ***(One unique # per row)***	**POI Device Firmware(s)** ***(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 / solution provider) managing it.

2.8 Summary of P2PE Assessment Compliance Status

Encryption Management Services

This table must correlate correctly with Table 2.1 for the assessment type.

*Mark **Yes** or **No**, as applicable to the assessment type and the overall findings, and mark **N/A** for all other assessment types.*

Type of P2PE Assessment	Compliant	Comments (*optional*)
Solution Provider (*or MMS as a Solution Provider)*	☐ Yes ☐ No ☐ N/A	
Encryption Management Component Provider (EMCP)	☐ Yes ☐ No ☐ N/A	
POI Deployment Component Provider (PDCP)	☐ Yes ☐ No ☐ N/A	
POI Management Component Provider (PMCP)	☐ Yes ☐ No ☐ N/A	

3. Details and Scope of P2PE Assessment

INSTRUCTIONS FOR SECTION 3
Solution Assessments: Complete the entirety of section 3 here as it pertains to the scope of Encryption Management Services of the Solution assessment. It is not necessary to duplicate information between this section here and section 3 in the Solution P-ROV. However, while there may be overlap in section 3 between the two P-ROVs, this section here must be completed and satisfied in its entirety within the scope of Encryption Management Services. **EMS Component Assessments:** Complete the entirety of Section 3.

3.1 Scoping Details
Describe how the accuracy of the scope for the P2PE assessment was validated, including:
• The methods or processes used to identify all elements in scope of the P2PE assessment:
• How the scope of the assessment was confirmed to be accurate and to cover all components and facilities for the Encryption Management Services:

3.2 Encryption Management Services Diagram

Provide one or more ***high-level*** diagrams to illustrate the function of the Encryption Management Services, including: ▪ Locations of critical facilities ▪ Location of systems performing encryption management functions ▪ Other necessary components, as applicable to the Encryption Management Services	
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 Encryption Management Services diagram(s) here>

3.3 (Table Not Currently Used)

3.4 Key-management Processes	
Provide one or more ***high-level*** diagrams showing all key-management processes, including: ▪ Key Generation ▪ Key Distribution / Loading / Injection into 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

Lab/Test environment(s) used by the P2PE Assessor for this assessment (*add rows as necessary*)		
Identify whether the lab/test environment was provided by the P2PE QSA Company and/or the Solution / Component Provider:	☐ P2PE QSA Company ***and/or*** ☐ Solution / Component Provider	
Address of the lab/test environment(s) used for this assessment:	P2PE QSA Company:	
	Solution/Component Provider:	
Describe the lab/test environment(s) used for this assessment. When more than one environment is used, be clear which environment you are describing.		

Facilities INCLUDED in the scope of this assessment (*insert additional rows as necessary*)		
Were any facilities **included** in the scope of the assessment?	☐ Yes (*If **Yes,** document below*)	☐ No (*If **No,** leave details blank*)
Description and purpose of facility included in the 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?		☐ 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. Insert additional rows to each section as necessary.

Note: *If the 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 P2PE Application, etc.*

P2PE Application Implementation Guide(s) (IG)

Reference # (*optional use*)	**Document Name (*Title of the IG*)**	**Version Number**	**Document Date (*latest version date*)**	**Which P2PE Application(s) 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 (*insert additional rows as necessary*)

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

3.8 Device Samples for P2PE Assessment

Complete for all sampled devices in the P2PE assessment, including for every POI Device Type at Table 2.5 and every SCD type at Table 2.6.

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

Sample Ref # (*optional*)	PTS and/or FIPS Approval #	Sample Size (*x of y*)	Serial Numbers of Tested Devices / Other Identifiers	Sampling Rationale

3.9 Key Matrix

List all cryptographic key types used in the Encryption Management Services
Reference Annex C in the P2PE Standard.

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

NOTE: *Entities only meeting a partial set of applicable requirements (where a Validated P2PE Component Provider is not being used to satisfy the remaining applicable requirements) are not eligible for PCI SSC's Validated P2PE Product listings.*

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

Encryption Management Services – Summary of Findings

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

Abbreviations:			
EMCP	Encryption Management Component Provider	**PDCP**	POI Deployment Component Provider
PMCP	POI Management Component Provider	**SP**	Solution Provider (*or MMS as a Solution Provider*)

Encryption Management Services: P2PE Validation Requirements					**Summary of Findings (check one for EVERY row)**		
EMCP	**PDCP**	**PMCP**	**SP**	**Requirements**	**In Place**	**N/A**	**Not in Place**
DOMAIN 1							
Applies to:				**1A Account data must be encrypted in equipment that is resistant to physical and logical compromise.**			
☑	☑		☑	***1A-1*** *PCI-approved POI devices with SRED are used for transaction acceptance.*	☐	☐	☐
☑	☑		☑	***1A-2*** *Applications on POI devices with access to clear-text account data are assessed per P2PE Application P-ROV before being deployed into a P2PE solution.*	☐	☐	☐
				1B Logically secure POI devices.			
☑	☑		☑	***1B-1*** *Solution/component provider ensures that logical access to POI devices deployed at merchant encryption environment(s) is restricted to authorized personnel.*	☐	☐	☐
☑		☑	☑	***1B-2*** *Solution/component provider secures any remote access to POI devices deployed at merchant encryption environments.*	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑		☑	☑	***1B-3*** *The solution/component provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	☐	☐	☐
☑		☑	☑	***1B-4*** *Solution/component provider implements procedures to secure account data when troubleshooting.*	☐	☐	☐
☑		☑	☑	***1B-5*** *The P2PE solution/component provides auditable logs of any changes to critical functions of the POI device(s).*	☐	☐	☐
				1C Use P2PE applications that protect PAN and SAD.			
☑		☑	☑	***1C-1*** *Applications are implemented securely, including when using shared resources and when updating applications and application functionality.*	☐	☐	☐
☑	☑	☑	☑	***1C-2*** *All applications/software without a business need do not have access to account data.*	☐	☐	☐
				1D Implement secure application-management processes.			
☑		☑	☑	***1D-1*** *Integrity of applications is maintained during installation and updates.*	☐	☐	☐
☑	☑	☑	☑	***1D-2*** *Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	☐	☐	☐
				1E Component providers ONLY: Report status to solution providers.			
☑	☑	☑		***1E-1*** *For component providers of encryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.*	☐	☐	☐
DOMAIN 5							
Not used in P2PE				***1-1***		☒	
Not used in EMS				***1-2***		☒	
☑	☑	☑	☑	***1-3***	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***1-4***	☐	☐	☐
Not used in EMS				***1-5***		☒	
Requirements 2, 3 and 4 are not used in P2PE.							
Applies to:				**Control Objective 2:** **Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys**			
☑	☑	☑	☑	***5-1***	☐	☐	☐
☑	☑	☑	☑	***6-1***	☐	☐	☐
☑	☑	☑	☑	***6-2***	☐	☐	☐
☑	☑	☑	☑	***6-3***	☐	☐	☐
☑	☑	☑	☑	***6-4***	☐	☐	☐
☑	☑	☑	☑	***6-5***	☐	☐	☐
☑	☑	☑	☑	***6-6***	☐	☐	☐
☑	☑	☑	☑	***7-1***	☐	☐	☐
☑	☑	☑	☑	***7-2***	☐	☐	☐
Applies to:				**Control Objective 3:** **Keys are conveyed or transmitted in a secure manner**			
☑	☑	☑	☑	***8-1***	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***8-2***	☐	☐	☐
☑	☑	☑	☑	***8-3***	☐	☐	☐
☑	☑	☑	☑	***8-4***	☐	☐	☐
☑	☑	☑	☑	***9-1***	☐	☐	☐
☑	☑	☑	☑	***9-2***	☐	☐	☐
☑	☑	☑	☑	***9-3***	☐	☐	☐
☑	☑	☑	☑	***9-4***	☐	☐	☐
☑	☑	☑	☑	***9-5***	☐	☐	☐
☑	☑	☑	☑	***9-6***	☐	☐	☐
☑	☑	☑	☑	***10-1***	☐	☐	☐
Not used in P2PE				***10-2***		☒	
Not used in P2PE				***10-3***		☒	
Not used in P2PE				***10-4***		☒	
Not used in P2PE				***10-5***		☒	
☑	☑	☑	☑	***11-1***	☐	☐	☐
☑	☑	☑	☑	***11-2***	☐	☐	☐
Applies to:				**Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner**			
☑	☑	☑	☑	**12-1**	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***12-2***	☐	☐	☐
☑	☑	☑	☑	***12-3***	☐	☐	☐
☑	☑	☑	☑	***12-4***	☐	☐	☐
☑	☑	☑	☑	***12-5***	☐	☐	☐
☑	☑	☑	☑	***12-6***	☐	☐	☐
☑	☑	☑	☑	***12-7***	☐	☐	☐
☑	☑	☑	☑	***12-8***	☐	☐	☐
Not used in EMS				***12-9***		☒	
☑	☑	☑	☑	***13-1***	☐	☐	☐
☑	☑	☑	☑	***13-2***	☐	☐	☐
☑	☑	☑	☑	***13-3***	☐	☐	☐
☑	☑	☑	☑	***13-4***	☐	☐	☐
☑	☑	☑	☑	***13-5***	☐	☐	☐
☑	☑	☑	☑	***13-6***	☐	☐	☐
☑	☑	☑	☑	***13-7***	☐	☐	☐
☑	☑	☑	☑	***13-8***	☐	☐	☐
Not used in EMS				***13-9***		☒	

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***14-1***	☐	☐	☐
☑	☑	☑	☑	**14-2**	☐	☐	☐
☑	☑	☑	☑	***14-3***	☐	☐	☐
☑	☑	☑	☑	***14-4***	☐	☐	☐
☑	☑	☑	☑	***14-5***	☐	☐	☐
☑	☑	☑	☑	***15-1***	☐	☐	☐
☑	☑	☑	☑	***15-2***	☐	☐	☐
Not used in EMS				***15-3***		☒	
Not used in EMS				***15-4***		☒	
Not used in EMS				***15-5***		☒	
☑	☑	☑	☑	***16-1***	☐	☐	☐
☑	☑	☑	☑	***16-2***	☐	☐	☐
				Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage			
☑	☑	☑	☑	***17-1***	☐	☐	☐
☑	☑	☑	☑	***18-1***	☐	☐	☐
☑	☑	☑	☑	***18-2***	☐	☐	☐
☑	☑	☑	☑	***18-3***	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
Not used in EMS				*18-4*		☒	
Not used in EMS				*18-5*		☒	
Not used in EMS				*18-6*		☒	
Not used in EMS				*18-7*		☒	
☑	☑	☑	☑	*19-1*	☐	☐	☐
☑	☑	☑	☑	*19-2*	☐	☐	☐
☑	☑	☑	☑	*19-3*	☐	☐	☐
☑	☑	☑	☑	*19-4*	☐	☐	☐
☑	☑	☑	☑	*19-5*	☐	☐	☐
Not used in EMS				*19-6*		☒	
Not used in EMS				*19-7*		☒	
Not used in EMS				*19-8*		☒	
Not used in EMS				*19-9*		☒	
Not used in EMS				*19-10*		☒	
Not used in EMS				*19-11*		☒	
Not used in EMS				*19-12*		☒	
☑	☑	☑	☑	*20-1*	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***20-2***	☐	☐	☐
☑	☑	☑	☑	***20-3***	☐	☐	☐
☑	☑	☑	☑	***20-4***	☐	☐	☐
Applies to:				**Control Objective 6: Keys are administered in a secure manner**			
☑	☑	☑	☑	***21-1***	☐	☐	☐
☑	☑	☑	☑	***21-2***	☐	☐	☐
☑	☑	☑	☑	***21-3***	☐	☐	☐
Not used in EMS				***21-4***		☒	
☑	☑	☑	☑	***22-1***			
☑	☑	☑	☑	***22-2***			
Not used in EMS				***22-3***		☒	
Not used in EMS				***22-4***		☒	
Not used in EMS				***22-5***		☒	
☑	☑	☑	☑	***23-1***	☐	☐	☐
☑	☑	☑	☑	***23-2***	☐	☐	☐
☑	☑	☑	☑	***23-3***	☐	☐	☐
☑	☑	☑	☑	***24-1***	☐	☐	☐

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
☑	☑	☑	☑	***24-2***	☐	☐	☐
☑	☑	☑	☑	***25-1***	☐	☐	☐
Not used in EMS				***25-2***		☒	
Not used in EMS				***25-3***		☒	
Not used in EMS				***25-4***		☒	
Not used in EMS				***25-6***		☒	
Not used in EMS				***25-7***		☒	
Not used in EMS				***25-8***		☒	
Not used in EMS				***25-9***		☒	
☑	☑	☑	☑	***26-1***	☐	☐	☐
☑	☑	☑	☑	***27-1***	☐	☐	☐
☑	☑	☑	☑	***27-2***	☐	☐	☐
☑	☑	☑	☑	***28-1***	☐	☐	☐
Not used in EMS				***28-2***		☒	
Not used in EMS				***28-3***		☒	
Not used in EMS				***28-4***		☒	
Not used in EMS				***28-5***		☒	

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
Applies to:				**Control Objective 7: Equipment used to process account data and keys is managed in a secure manner**			
☑	☑	☑	☑	***29-1***	☐	☐	☐
Not used in EMS				***29-2***		☒	
☑	☑	☑	☑	***29-3***	☐	☐	☐
☑	☑	☑	☑	***29-4***	☐	☐	☐
☑	☑	☑	☑	***29-5***	☐	☐	☐
Not used in P2PE				***30-1***		☒	
Not used in P2PE				***30-2***		☒	
☑	☑	☑	☑	***31-1***	☐	☐	☐
☑	☑	☑	☑	***32-1***	☐	☐	☐
Not used in EMS				***32-2***		☒	
Not used in EMS				***32-3***		☒	
Not used in EMS				***32-4***		☒	
Not used in EMS				***32-5***		☒	
Not used in EMS				***32-6***		☒	
Not used in EMS				***32-7***		☒	
Not used in EMS				***32-8***		☒	

Encryption Management Services: P2PE Validation Requirements					Summary of Findings (check one for EVERY row)		
EMCP	PDCP	PMCP	SP	Requirements	In Place	N/A	Not in Place
Not used in EMS				***32-9***		☒	
☑	☑	☑	☑	***33-1***	☐	☐	☐
Applies to:				***Requirement 5A: Account data is processed using algorithms and methodologies that ensure they are kept secure***			
☑	☑	☑	☑	***5A-1***	☐	☐	☐

Document All Requirements Determined to be 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.*

Every requirement denoted as 'N/A' in the reporting section below must be documented in this table and vice versa.

List requirements in the order as they appear in the reporting section below. Insert additional rows if needed.

Requirement	Document how it was determined that the requirement is Not Applicable to the P2PE Product under assessment

P2PE Encryption Management Services – Reporting

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
DOMAIN 1 **NOTE:** Within this domain, the term "solution provider" refers to whichever entity is undergoing the P2PE assessment. This may be a solution provider, a component provider, or a merchant as a solution provider (MMS). Refer to Domain 1 in the P2PE Standard for additional details.					
	1A-1.1 Account data encryption operations must be performed using a POI device approved per the PCI PTS program with SRED (secure reading and exchange of data). The PTS approval listing must match the deployed devices in the following characteristics: • Model name and number • Hardware version number • Firmware version number • SRED listed as a function provided		☐	☐	☐
PDCP **EMCP** **SP**	**1A-1.1** Account data encryption operations must be performed using a POI device approved per the PCI PTS program with SRED (secure reading and exchange of data). The PTS approval listing must match the deployed devices in the following characteristics: • Model name/number • Hardware version number • Firmware version number • SRED listed as a function provided	For each POI device type used in the solution, examine the POI device and review the PCI SSC list of Approved PTS Devices to verify that all of the following POI device characteristics match the PTS listing: <Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1A-1.1.1 The POI device's SRED capabilities must be enabled and active.			☐	☐	☐
PDCP EMCP SP	**1A-1.1.1.a** Examine documented procedures and interview personnel to verify that procedures are defined to ensure that SRED capabilities are enabled and active on all POI devices prior to devices being deployed to merchant encryption environments.	Documented procedures reviewed:	*<Report Findings Here>*		
		Personnel interviewed:	*<Report Findings Here>*		
PDCP EMCP SP	**1A-1.1.1.b** For all POI device types used in the solution, review POI device configurations to verify that all POI device types used in the solution have SRED capabilities enabled and active (that is, the POI devices are operating in "encrypting mode") prior to devices being deployed to merchant encryption environments.	For all POI device types used in the solution, review POI device configurations to verify that all POI device types used in the solution have SRED capabilities enabled and active (that is, the POI devices are operating in "encrypting mode") prior to devices being deployed to merchant encryption environments.			
		<Report Findings Here>			
1A-1.2 POI devices must be configured to use only SRED-validated account-data capture mechanisms.			☐	☐	☐
PDCP EMCP SP	**1A-1.2.a** For all POI device types intended for use in the P2PE solution, identify and document all account-data capture interfaces.	Refer to Section 2.5 "PTS Devices Supported" in the Summary Overview for this documentation. No further reporting required here.			
PDCP EMCP SP	**1A-1.2.b** For each POI device type used in the solution, examine the device configuration to verify that it is configured by default to use only SRED-validated account-data capture mechanisms for accepting and processing P2PE transactions.	For each POI device type used in the solution, examine the device configuration to verify that it is configured by default to use only SRED-validated account-data capture mechanisms for accepting and processing P2PE transactions.			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1A-1.2.1 All account data capture mechanisms on the POI device must be SRED-validated, or must be disabled or otherwise prevented from being used for P2PE transactions such that they cannot be enabled by the merchant.			☐	☐	☐
PDCP EMCP SP	**1A-1.2.1.a** Examine POI configuration and deployment procedures to verify they include either: • Disabling all capture mechanisms that are not SRED validated, or • Implementing configurations that prevent all non-SRED validated capture mechanisms from being used for P2PE transactions.	Documented POI configuration and deployment procedures reviewed:	*<Report Findings Here>*		
PDCP EMCP SP	**1A-1.2.1.b** Verify that the documented procedures include ensuring that all non-SRED-validated capture mechanisms are disabled or otherwise prevented from being used for P2PE transactions prior to devices being deployed to merchant encryption environments.	Documented procedures reviewed:	*<Report Findings Here>*		
PDCP EMCP SP	**1A-1.2.1.c** For all POI device types, verify: • All non-validated capture mechanisms are either disabled or configured to prevent their use for P2PE transactions prior to devices being deployed to merchant encryption environments. • Disabled capture mechanisms cannot be enabled by the merchant, and/or the configurations that prevent capture mechanisms from being used for P2PE transactions cannot be enabled by the merchant.	Describe the testing methods used to verify that for all POI device types, all non-validated capture mechanisms are either disabled or configured to prevent their use for P2PE transactions, prior to devices being deployed to merchant encryption environments:			
		<Report Findings Here>			
		Describe the testing methods used to verify that for all POI device types, disabled capture mechanisms cannot be enabled by the merchant, and/or the configurations that prevent capture mechanisms from being used for P2PE transactions cannot be enabled by the merchant.			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1A-1.3 If the POI device implements open protocols as part of the solution, the device must also be validated to the PCI PTS Open Protocols (OP) module. Open protocols include the following: • Link Layer Protocols • IP Protocols • Security Protocols • IP Services			☐	☐	☐
PDCP EMCP SP	**1A-1.3** For all POI device types that implement open protocols, examine device configurations and review the list of approved PTS devices at www.pcisecuritystandards.org, to verify that all POI devices that implement open protocols used in this solution are listed. Confirm each such device has a valid SSC listing number on the PCI SSC website under "Approved PCI PTS Devices" with "OP" listed as a "function provided".	Refer to Section 2.5 "PTS Devices Supported" in the Summary Overview for this documentation. No further reporting required here.			
1A-1.4 Clear-text account data must not be disclosed to any component or device outside of the PCI-approved POI device.			☐	☐	☐
PDCP EMCP SP	**1A-1.4.a** Examine documented transaction processes and data flows to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.	Documented transaction processes and data flows reviewed:	<Report Findings Here>		
PDCP EMCP SP	**1A-1.4.b** Using forensic tools and/or other data tracing methods, inspect a sample of transactions to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.	Identify the sample of transactions	*<Report Findings Here>*		
		Describe the forensic tools and/or other data tracing methods used to inspect the sample of transactions:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1A-2.1 All applications on POI devices with access to clear-text account data must be assessed according to Domain 2. The assessment must match the application in the following characteristics: • Application name • Version number			☐	☐	☐
PDCP **EMCP** **SP**	**1A-2.1.a** For applications on the PCI SSC list of Validated P2PE Applications, review the list and compare to applications used in the solution to verify that the applications match the P2PE application listing in the following characteristics: • Application name • Version number	Refer to Section 2.3 "Listed P2PE Applications used in the P2PE Solution" in the Summary Overview for this documentation. No further reporting required here.			
PDCP **EMCP** **SP**	**1A-2.1.b** For applications not on the PCI SSC list of Validated P2PE Applications, review the application P-ROV(s) and verify that the applications used in the solution match the application P-ROV in the following characteristics: • Application name • Version number	Identify application P-ROV(s) reviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1A-2.2.a. For applications on the PCI SSC list of Validated P2PE Applications, review the list and verify all POI device types the application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) • Explicitly included in that application's listing			☐	☐	☐
PDCP EMCP SP	**1A-2.2.a** For applications on the PCI SSC list of Validated P2PE Applications, review the list and verify all POI device types the application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) • Explicitly included in that application's listing	Refer to Section 2.3 "Listed P2PE Applications used in the P2PE Solution" and Section 2.5 "PTS Devices Supported" in the Summary Overview for this documentation. No further reporting required here.			
PDCP EMCP SP	**1A-2.2.b** For applications not on the PCI SSC list of Validated P2PE Applications, review the application P-ROV and verify the POI device types the application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) • Explicitly included in that P-ROV as assessed for that application.	Refer to Section 2.5 "PTS Devices Supported" in the Summary Overview for confirmation per 1A-1.1 of PTS-approval (if this testing procedure is applicable).			
		Identify application P-ROV(s) reviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-1.1 Solution/component provider must ensure merchant logical access to POI devices, if needed, is restricted as follows: • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear text PAN and/or SAD • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear text PAN • Cannot view or access SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms • Does not use any POI vendor default device passwords			☐	☐	☐
PDCP **EMCP** **SP**	**1B-1.1.a** Examine documented POI device configuration procedures and documented account privilege assignment rules to verify that merchant logical access to POI devices is restricted as follows: • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear text PAN and/or SAD • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear text PAN • Cannot view or access SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms • Does not use the POI vendor's default passwords	Documented procedures reviewed:	*<Report Findings Here>*		
		Describe how documented POI device configuration procedures and documented account privilege assignment rules verified that merchant logical access to POI devices is restricted as follows: • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear text PAN and/or SAD • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear text PAN • Cannot view or access SAD. • Cannot enable disabled device interfaces or disabled data-capture mechanisms • Does not use the POI vendor's default passwords			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **EMCP** **SP**	**1B-1.1.b** For a sample of all POI devices used in the solution, logon to the device using an authorized test merchant account. Verify that merchant-account logical access meets the following: • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear text PAN and/or SAD Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear text PAN • Cannot view or access SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms • Does not use the POI vendor's default passwords	Identify the sample of POI devices used:	<Report Findings Here>		
		Describe how logon to the device using an authorized test merchant account verified that merchant-account logical access meets the following: • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear text PAN and/or SAD Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear text PAN • Cannot view or access SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms • Does not use the POI vendor's default passwords			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-1.1.1 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 ONLY if the following are met: • The solution/component provider must document which payment application(s) facilitates printing of PANs for merchants. • The P2PE application that facilitates this is confirmed per **1A-2.1** as assessed to P2PE Application P-ROV and on PCI SSC's list of Validated P2PE Applications. ***Note:*** *P2PE Application P-ROV (at **2A-3.1.2**) and Solution P-ROV (at **3A-1.3**) also include requirements that must be met for any P2PE application and P2PE solution provider, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*			☐	☐	☐
PDCP **EMCP** **SP**	**1B-1.1.1.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 specifies the payment application(s) that facilitate printing of PANs for merchants.	Solution provider's documented procedures reviewed:	*<Report Findings Here>*		
	1B-1.1.1.b Review applications confirmed at 1A-2.1 to verify the application(s) that facilitates printing of full PANs on merchant receipts is on PCI SSC's list of Validated P2PE Applications.	Identify any P2PE Applications at 1A-2.1 that facilitate printing of full PANs on merchant receipts:	*<Report Findings Here>*		
		Refer to Section 2.3 "Listed P2PE Applications used in the P2PE Component" in the Summary Overview for documentation of the PCI SSC listing of the P2PE Application (if this testing procedure is applicable):			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-1.2 All solution/component-provider personnel with logical access to POI devices deployed in merchant encryption environments must be documented in a formal list and authorized by solution/component provider management. The list of authorized personnel is reviewed at least annually.			☐	☐	☐
PMCP **EMCP** **SP**	**1B-1.2.a** Examine documented authorizations to verify: All personnel with access to devices are documented in a formal list. • All personnel with access to devices are authorized by management. • The list of authorized personnel is reviewed at least annually.	Documented authorizations reviewed:	*<Report Findings Here>*		
PMCP **EMCP** **SP**	**1B-1.2.b** For a sample of all POI device types, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to POI devices.	Identify the sample of POI devices used:	*<Report Findings Here>*		
		Describe how account-access configurations for a sample of all POI device types verified that only personnel documented and authorized in the formal list have access to POI devices:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-1.2.1 Solution provider personnel with logical access to POI devices deployed in merchant encryption environments must be granted based on least privilege and need to know.			☐	☐	☐
PMCP **EMCP** **SP**	**1B-1.2.1a** Examine documented access-control policies and procedures to verify that solution provider personnel with logical access to POI devices deployed at merchant encryption environments is assigned according to least privilege and need to know.	Documented access-control policies and procedures reviewed:	*<Report Findings Here>*		
PMCP **EMCP** **SP**	**1B-1.2.1.b** For a sample of all POI devices and personnel, observe configured accounts and permissions, and interview responsible personnel to verify that the level of logical access granted is according to least privilege and need to know.	Identify the sample of POI devices used:	*<Report Findings Here>*		
		Identify the sample of personnel used:	*<Report Findings Here>*		
		Responsible personnel interviewed:	*<Report Findings Here>*		
		Describe how configured accounts and permissions for the sample of all POI devices and personnel verified that the level of logical access granted is according to least privilege and need to know:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-2.1 Solution provider's authorized personnel must use multi-factor or cryptographic authentication for all remote access to merchant POI devices. ***Note:*** *This includes personnel authenticating to a terminal management system (TMS) or other similar systems to gain remote access to POI devices*			☐	☐	☐
PMCP EMCP SP	**1B-2.1.a** Examine documented procedures to verify that either multi-factor or cryptographic authentication must be used for all remote access to POI devices.	Documented procedures reviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-2.1.b** Observe remote-access mechanisms and controls to verify that either multi-factor or cryptographic authentication is configured for all remote access to POI devices.	Describe how remote-access mechanisms and controls verified that either multi-factor or cryptographic authentication is configured for all remote access to POI devices:			
		<Report Findings Here>			
PMCP EMCP SP	**1B-2.1.c** Interview personnel and observe actual remote connection attempts to verify that either multi-factor or cryptographic authentication is used for all remote access to POI devices.	Personnel interviewed:	*<Report Findings Here>*		
		Describe how actual remote connection attempts verified that either multi-factor or cryptographic authentication is configured for all remote access to POI devices:			
		<Report Findings Here>			
1B-2.2 POI devices must be configured to ensure that remote access is only permitted from the solution provider's authorized systems (which might include a terminal management system (TMS) or similar system).			☐	☐	☐
PMCP EMCP SP	**1B-2.2.a** Examine documented device-configuration procedures and interview personnel to verify that devices must be configured to permit remote access only from the solution provider's authorized systems.	Documented device-configuration procedures reviewed:	*<Report Findings Here>*		
		Personnel interviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-2.2.b** For all devices used in the solution, observe a sample of device configurations to verify that remote access is permitted only from the solution provider's authorized systems.	Describe how sampled device configurations for all devices used in the solution verified that remote access is permitted only from the solution provider's authorized systems:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-2.3 POI devices must be configured such that merchants do not have remote access to the merchant POI devices.			☐	☐	☐
PMCP EMCP SP	**1B-2.3.a** Examine documented POI-configuration procedures and interview personnel to verify that devices must be configured to ensure merchants do not have remote access to the POI devices.	Documented POI-configuration procedures reviewed:	*<Report Findings Here>*		
		Personnel interviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-2.3.b** For all devices used in the solution, observe a sample of device configurations to verify that merchants do not have remote access to the POI devices.	Describe how sampled device configurations for all devices used in the solution verified that merchants do not have remote access to the POI devices:			
		<Report Findings Here>			
1B-2.4 Solution provider must implement secure identification and authentication procedures for remote access to POI devices deployed at merchant encryption environments:			☐	☐	☐
PMCP EMCP SP	**1B-2.4.a** Examine documentation to verify secure identification and authentication procedures are defined for remote access to POI devices deployed at merchant encryption environments.	Documented identification and authentication procedures reviewed:	*<Report Findings Here>*		
1B-2.5 Solution Provider must maintain individual authentication credentials for all authorized solution-provider personnel that are unique for each merchant. **Note**: If a centralized terminal-management system (TMS) is utilized to manage multiple merchant accounts, it is acceptable for the TMS system to only require unique access for each authorized solution-provider employee accessing the TMS instead of requiring unique access per merchant.			☐	☐	☐
PMCP EMCP SP	**1B-2.5.a** Examine documentation to verify that all authorized solution-provider personnel are required to have individual authentication credentials that are unique for each merchant (or if applicable, per centralized TMS).	Documented identification and authentication procedures reviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-2.5.1 Tracing all logical access to POI devices by solution-provider personnel to an individual user.			☐	☐	☐
PMCP EMCP SP	**1B-2.5.1.a** Examine POI device configurations and authentication mechanisms to verify that all logical access to POI devices by solution-provider personnel can be traced to an individual user.	Describe how the POI device configurations and authentication mechanisms examined, verified that all logical access to POI devices by solution-provider personnel can be traced to an individual user.	*<Report Findings Here>*		
PMCP EMCP SP	**1B-2.5.1.b** Observe a sample of authorized logical accesses and examine access records/logs to verify that all logical access is traced to an individual user.	Describe how sampled authorized logical accesses and access records/logs verified that all logical access is traced to an individual user.	*<Report Findings Here>*		
1B-2.5.2 Maintaining audit logs of all logical access to POI devices by solution-provider personnel and retaining access logs for at least one year.			☐	☐	☐
PMCP EMCP SP	**1B-2.5.2.a** Examine documentation to verify that access records/logs of all logical access to POI devices by solution-provider personnel are required to be retained for at least one year.	Documented device-configuration procedures reviewed:			
		<Report Findings Here>			
1B-3.1 The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.			☐	☐	☐
PMCP EMCP SP	**1B-3.1.a** Examine documented procedures to verify secure update processes are defined for all firmware and software updates, and include: • Integrity checks of update • Authentication of origin of the update	Documented procedures reviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-3.1.b** Observe a sample of firmware and software updates, and interview personnel to verify: • The integrity of the update is checked • The origin of the update is authenticated	Identify sample of firmware and software updates observed:	*<Report Findings Here>*		
		Personnel interviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-3.2 An up-to-date inventory of POI device system builds must be maintained and confirmed at least annually and upon any changes to the build. ***Note:*** *A POI system build includes at least the following information:* • *Model name and number* • *Hardware version number* • *Firmware version number(s)* • *P2PE Payment Applications* • *Non-payment Software*			☐	☐	☐
PMCP EMCP SP	**1B-3.2.a** Examine documented procedures to verify they include: • Procedures for maintaining an up-to-date inventory of POI device system builds • Procedures for confirming all builds at least annually and upon any changes to the build	Documented procedures reviewed:	<Report Findings Here>		
PMCP EMCP SP	**1B-3.2.b** Review documented inventory of devices, and examine the inventory of system builds to verify: • The inventory includes all POI device system builds. • The inventory of POI device system builds is up-to-date.	Describe how the documented inventory of devices and inventory of system builds verified that: • The inventory includes all POI device system builds. • The inventory of POI device system builds is up-to-date. *<Report Findings Here>*			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-3.3 Critical software security updates must be deployed to POI devices in the field within 30 days of receipt from device vendors or application vendors. ***Note:*** *A "critical software security update" is one that addresses an imminent risk to account data, either directly or indirectly.* ***Note:*** *These security patches can be deployed via "push" from the solution provider or vendor, or via "pull" from the POI device or merchant. In all cases, the solution provider is ultimately responsible to ensure security patches are installed in a timely manner.* • *Aligns with 2C-1.2*			☐	☐	☐
PMCP EMCP SP	**1B-3.3.a** Examine documented procedures to verify they include defined procedures for deploying critical software security updates to POI devices in the field within 30 days of receipt from device or application vendors.	Documented procedures reviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-3.3.b** Examine security update deployment records and device logs, and interview responsible solution provider personnel and to verify that critical security updates are deployed to devices and applications in the field within 30 days of receipt from device and application vendors.	Responsible solution provider personnel interviewed:	*<Report Findings Here>*		
		Describe how the security update deployment records and device logs verified that critical security updates are deployed to devices and applications in the field within 30 days of receipt from device and application vendors.			
		<Report Findings Here>			
1B-3.4 The integrity of patch and update code must be maintained during delivery and deployment, as defined by the vendor—e.g., in the POI device vendor's security guidance or in the P2PE application's Implementation Guide..			☐	☐	☐
PMCP EMCP SP	**1B-3.4.a** Examine documented procedures for device updates to verify they follow guidance from the device or application vendor to maintain the integrity of all patch and update code during delivery and deployment.	Documented procedures reviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-3.4.b** Observe processes for delivering updates and interview responsible personnel to verify that the integrity of patch and update code is maintained during delivery and deployment, and according to guidance from the device or application vendor.	Responsible personnel interviewed:	*<Report Findings Here>*		
		Describe how the processes for delivering updates verified that updates are delivered in a secure manner with a known chain-of-trust and following guidance from the device or application vendor:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-4 Solution/Component provider implements procedures to secure account data when troubleshooting			☐	☐	☐
1B-4.1 Any PAN and/or SAD used for debugging or troubleshooting purposes must be securely deleted. These data sources must be collected in limited amounts and collected only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.			☐	☐	☐
PMCP EMCP SP	**1B-4.1.a** Examine the Solution/Component provider's procedures for troubleshooting customer problems and verify the procedures include: • PAN and/or SAD is never output to merchant environments • Collection of PAN and/or SAD only when needed to solve a specific problem • Storage of such data in a specific, known location with limited access • Collection of only a limited amount of data needed to solve a specific problem • Encryption of PAN and/or SAD while stored • Secure deletion of such data immediately after use	Documented Solution/Component provider's procedures for troubleshooting customer problems reviewed:	*<Report Findings Here>*		
PMCP EMCP SP	**1B-4.1.b** For a sample of recent troubleshooting requests, observe data collection and storage locations, and interview responsible personnel to verify the procedures identified at 1B-4.1.a were followed.	Identify the sample of recent troubleshooting requests:	*<Report Findings Here>*		
		Responsible personnel interviewed:	*<Report Findings Here>*		
		Describe how the data collection and storage locations for the sample of recent troubleshooting requests verified that procedures identified at 1B-4.1.a were followed:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1B-5.1 Any changes to critical functions of POI devices must be logged—either on the device or within the remote-management systems of the P2PE solution provider. ***Note:*** *Critical functions include application and firmware updates as well as changes to security-sensitive configuration options, such as whitelists or debug modes.*			☐	☐	☐
PMCP **EMCP** **SP**	**1B-5.1.a** Examine device and/or system configurations to verify that any changes to the critical functions of the POI devices are logged, including: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)	Describe how the device and/or system configurations observed verified that any changes to the critical functions of the POI devices are logged, including: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)			
		<Report Findings Here>			
PMCP **EMCP** **SP**	**1B-5.1.b** Observe authorized personnel perform authorized changes on POI devices, as follows, and examine log files to verify that all such activities result in a correlating log file: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)	Describe how observation of authorized personnel performing authorized changes on POI devices, as follows, and examination of log files verified that all such activities result in a correlating log file: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)			
		<Report Findings Here>			
PMCP **EMCP** **SP**	**1B-5.1.c** Examine documented procedures and sample logs to ensure access to logs is limited to need-to-know personnel and integrity of logs is maintained and verified.	Documented procedures reviewed:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1C-1.1 Processes for any whitelisting functionality must include: • Implementing whitelisting functionality in accordance with the device vendor's security guidance or the application's Implementation Guide • Cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control • Cryptographic authentication by the POI device's firmware • Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data • Approval of functionality by authorized personnel prior to implementation • Documentation for all new installations or updates to whitelist functionality that includes the following: • Description and justification for the functionality • The identity of the authorized person who approved the new installation or updated functionality prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data			☐	☐	☐
PMCP **EMCP** **SP**	**1C-1.1.a** Review documented policies and procedures and interview personnel to verify that processes for implementing any whitelisting functionality include: • Following the device vendor's security guidance or the application's Implementation Guide • Cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control • Cryptographic authentication of whitelisting functionality by the POI device's firmware • Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data • Approval of functionality by authorized personnel prior to implementation • Documentation for all new installations and updates to whitelist functionality that includes the following: – Description and justification for the functionality – The identity of the authorized person who approved the new installation or updated functionality prior to release – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data	Personnel interviewed:	*<Report Findings Here>*		
		Documented procedures reviewed:			
		<Report Findings Here>			

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1C-1.1.1 Any whitelisting functionality must only allow the output of clear text account data for non-PCI payment brand account/card data.			☐	☐	☐
PMCP EMCP SP	**1C-1.1.1.a** Observe application and device configurations and interview personnel to verify that whitelisting functionality only allows for the output of non-PCI payment brand accounts/cards, by following guidance in either the device vendor's security guidance or the application's Implementation Guide.	Describe how the application and device configurations observed verified that whitelisting functionality only allows for the output of non-PCI payment brand accounts/cards.			
		<Report Findings Here>			
		Personnel interviewed			
		<Report Findings Here>			
PMCP EMCP SP	**1C-1.1.1.b** For all device types with whitelisting functionality, perform test transactions to verify output of clear text account data is only enabled for non-PCI payment brand account/card data.	Describe how the test transactions performed, verified that any output of clear text account data is only enabled for non-PCI payment brand account/card data.			
		<Report Findings Here>			
1C-1.1.2 Any new installations of, or updates, to whitelisting functionality must be: • Cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control. • Cryptographically authenticated by the POI device's firmware in accordance with the device vendor's security guidance or the application's Implementation Guide.			☐	☐	☐
PMCP EMCP SP	**1C-1.1.2.a** Observe the process for new installations of, or updates to, whitelisting functionality and interview personnel to verify they are performed as follows: • Cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control • Cryptographically authenticated by the POI device firmware, in accordance with the device vendor's security guidance or the application's Implementation Guide	Documented policies and procedures reviewed:	*<Report Findings Here>*		
		Personnel interviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1C-1.1.3 Any new installations of, or updates to, whitelisting functionality must follow change-control procedures that include: • Coverage for both new installations and updates to such functionality • Description and justification for the functionality • The identity of the person who approved the new installation or update prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data			☐	☐	☐
PMCP **EMCP** **SP**	**1C-1.1.3.a** Review records of both new installations and updated whitelisting functionality, and confirm they include the following: • Coverage for both new installations and updates to such functionality • Description and justification for the functionality. • The identity of the person who approved the new installation or update prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data	Identify sampled records of updated whitelisting functionality:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1C-2.1 Processes must be documented and implemented to ensure that, prior to new installations or updates, any non-payment software: • Does not have any logical interfaces (e.g., application programming interfaces (APIs)) that allow for the storing, processing, or transmitting of clear text account data • Is cryptographically authenticated by the POI device's firmware • Requires an SCD with dual control for the application-signing process			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1C-2.1** Review the solution provider's documented processes and interview responsible personnel to confirm the processes include: • Review of the non-payment software vendor's documentation to determine all logical interfaces used by the non-payment software do not allow for the storing, processing, or transmitting of clear text account data • Documenting how the Solution/Component provider confirmed that the non-payment software has no logical interfaces that allow for storing, processing, or transmitting clear text account data • Authentication of the non-payment software by the POI device's firmware • Requiring an SCD with dual control to sign the non-payment software • Following this process both for new installations and for updates	Responsible personnel interviewed:	*<Report Findings Here>*		
		Responsible personnel interviewed:	*<Report Findings Here>*		
1C-2.1.1 The non-payment software does not have any logical interfaces—e.g., application programming interfaces (APIs)—that allow for storing, processing, or transmitting clear text account data.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1C-2.1.1** For each POI device type and each non-payment software intended for that POI device type that does not have a business need to access clear text account data, review the non-payment software vendor's documentation to verify that the non-payment software has no logical interfaces that allow for storing, processing, or transmitting clear text account data.	Solution/Component provider's documentation reviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1C-2.1.2 The non-payment software is authenticated within the POI device using an approved security mechanism of the POI device.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1C-2.1.2** Interview Solution/Component-provider personnel and observe the process for new installations or updates of non-payment software to verify that it is authenticated to the POI device using an approved security mechanism of the POI device.	Describe how the process for new application installations or application updates verified that applications with no need to access clear-text account data are authenticated to the device using an approved security mechanism:	*<Report Findings Here>*		
1C-2.1.3 Requires an SCD with dual control for the application-signing process (i.e., signing non-payment software).			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1C-2.1.3** Interview Solution/Component-provider personnel and observe processes for new installations or updates of non-payment software to confirm that application signing process is performed under dual control using an SCD.	Personnel interviewed:	*<Report Findings Here>*		
		Describe how the process for new application installations or application updates verified that application signing is performed under dual control:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1D-1.1 Processes must be documented and implemented to manage all changes to applications, including: • Following vendor guidance in the application's Implementation Guide. • Documented approval for all changes by appropriate personnel. • Documented reason and impact for all changes. • Functionality testing of all changes on the intended device(s). • Documented back-out procedures for application installations/updates. *Note that adding a changed application or a changed POI device to a PCI-listed P2PE Component requires the Component Provider to undergo an assessment per PCI's "Delta-Change" process. See the P2PE Program Guide for more information.* *Aligns with **2C-2.1***			☐	☐	☐
PMCP **EMCP** **SP**	**1D-1.1.a** Review the Solution/Component provider's documented processes for implementing changes to applications, and interview Solution/Component-provider personnel, and confirm the following processes are in place: • Guidance in the Implementation Guide is followed. • All changes to applications include documented approval by appropriate authorized Solution/Component-provider personnel. • All changes to applications are documented as to reason and impact of the change. • Functionality testing of all changes on the intended devices is performed. • Documentation includes back-out procedures for application installations/updates.	Solution/Component provider personnel interviewed:	*<Report Findings Here>*		
		Solution/Component provider's documentation reviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PMCP EMCP SP	**1D-1.1.b** Review records of changes to applications and confirm the following: • All Implementation Guide requirements were followed. • Approval of the change by appropriate parties is documented. • The documentation includes reason and impact of the change. • The documentation describes functionality testing that was performed. • Documentation includes back-out procedures for application installations/updates.	Identify the sample of records of changes to applications:	*<Report Findings Here>*		
1D-1.2 All new installations and updates to applications must be authenticated as follows:			☐	☐	☐
PMCP EMCP SP	**1D-1.2.a** Review the Solution/Component provider's documentation and confirm their documented processes include using the guidance in the application's Implementation Guide for any application installations and updates.	Solution/Component provider's documentation reviewed:	*<Report Findings Here>*		
1D-1.2.1 All applications must be cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control.			☐	☐	☐
PMCP EMCP SP	**1D-1.2.1.a** Confirm the following through interviews with responsible Solution/Component provider personnel and by observing an installation/update: • Cryptographic signing processes for applications are followed as specified in the Implementation Guide. • Cryptographic signing (or similar) is performed prior to installation only by authorized personnel using dual control. • All new installations and updates to applications are signed prior to installation on the device. • Cryptographic signing for new installations and updates to applications is done under dual control..	Responsible Personnel interviewed:	*<Report Findings Here>*		
		Describe how the installation and update processes observed verified that new application installations and updates are cryptographically authenticated by the POI device's firmware:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1D-1.3 Processes must be in place to implement application developer guidance on key and certificate usage from the application's Implementation Guide. *Aligns with 2B-3.1.1*			☐	☐	☐
PMCP **EMCP** **SP**	**1D-1.3.a** Review the Solution/Component provider's documentation and confirm their documented processes include application developer key-management security guidance.	Documentation reviewed:	*<Report Findings Here>*		
PMCP **EMCP** **SP**	**1D-1.3.b** Interview Solution/Component-provider personnel to confirm that they follow key-management security guidance in accordance with the Implementation Guide.	Responsible Personnel interviewed: *<Report Findings Here>*			
1D-2.1 Upon receipt from the application vendor, a current copy of the application vendor's Implementation Guide must be retained and distributed to any outsourced integrators/resellers used for the P2PE Solution/Component. *Aligns with 2C-3.1.3*			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1D-2.1** Interview Solution/Component-provider personnel and examine documentation (including a current copy of the Implementation Guide from the application vendor) to confirm the following: • The Solution/Component provider retains a current copy of the Implementation Guide. • The Solution/Component provider distributes the Implementation Guide to any outsourced integrators/resellers the Solution/Component provider uses for the P2PE Solution/Component upon obtaining updates from the application vendor.	Documentation reviewed, in addition to the current copy of the Implementation Guide from the application vendor:	*<Report Findings Here>*		
		Current Application Vendor Implementation Guide(s) reviewed:	*<Report Findings Here>*		
		Current Application Vendor Implementation Guide(s) reviewed:	*<Report Findings Here>*		
Note: *This section (**1E-1**) is ONLY applicable for **P2PE component providers** undergoing an assessment for subsequent PCI listing of the component provider's Encryption-Management Services. This section is not applicable to, and does not need to be completed by, P2PE solution providers (or merchants as solution providers) that include encryption-management functions in their P2PE solution assessment (whether those functions are performed by the solution provider or are outsourced to non-PCI listed third parties).*					

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1E-1.1 Track status of the encryption-management services and provide reports to solution provider annually and upon significant changes, including at least the following: • Types/models of POI devices • Number of devices deployed and any change in numbers since last report • Date of last inventory of POI device system builds • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated			☐	☐	☐
PDCP **PMCP** **EMCP**	**1E-1.1.a** Review component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel, and to confirm that the following processes are documented and implemented: • Types/models of POI devices • Number of devices deployed and change since last report • Date of last inventory of POI device system builds • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated	Responsible component provider personnel interviewed:	*<Report Findings Here>*		
		Reports reviewed for this testing procedure:	*<Report Findings Here>*		
PDCP **PMCP** **EMCP**	**1E-1.1.b** Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of POI devices • Number of devices deployed and changed since last report • Date of last inventory of POI device system builds • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated	Reports reviewed for this testing procedure:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1E-1.2 Manage and monitor changes to encryption-management services and notify the solution provider upon occurrence of any of the following: • Critical software security updates deployed to POI devices • Addition and/or removal of POI device types • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change • Adding, changing, and/or removing P2PE non-payment software on POI devices (without access to clear-text account data), including description of change • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software Note that adding, changing, or removing POI device types, P2PE applications, and/or P2PE non-payment software may require adherence to PCI SSC's process for making changes. Please refer to the P2PE Program Guide for details about obligations when adding, changing, or removing elements of a P2PE solution.			☐	☐	☐
PDCP **PMCP** **EMCP**	**1E-1.2.a** Review component provider's documented procedures and interview responsible component-provider personnel, and confirm that processes include notifying the solution provider upon occurrence of the following: • Critical software security updates deployed to POI devices • Addition and/or removal of POI device types • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change • Adding, changing, and/or removing P2PE non-payment software on POI devices (without access to clear-text account data), including description of change • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software	Documented component provider's procedures reviewed:	*<Report Findings Here>*		
		Responsible component provider personnel interviewed:	*<Report Findings Here>*		

Encryption Management Services – Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP**	**1E-1.2.b** Observe reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical software security updates deployed to POI devices • Addition and/or removal of POI device types • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change • Adding, changing, and/or removing P2PE non-payment software (without access to clear-text account data), including description of change • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software	Reports reviewed for this testing procedure:	*<Report Findings Here>*		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
DOMAIN 5					
1-1 Not used in P2PE					
1-2 Not used in EMS					
1-3 All hardware security modules (HSMs) must be either: • FIPS 140-2 or FIPS 140-3 Level 3 or higher certified, or • PCI approved ***Note:*** *HSM approval listings must be current—HSMs must have a non-expired PCI PTS HSM approval or a non-expired FIPS 140-2 or FIPS 140-3 certificate (i.e., the FIPS 140 HSM certificates must not be listed as historical or revoked).* ***Note:*** *PCI-approved HSMs may have their approvals restricted whereby the approval is valid only when the HSM is deployed in controlled environments or more robust (e.g., secure) environments as defined in ISO 13491-2 and in the device's PCI HSM Security Policy. This information is noted in the Additional Information column of approved PTS devices.* ***Note:*** *Key-injection platforms and systems must include hardware devices for managing (e.g., generating and storing) the keys that conform to the requirements for SCDs. This includes SCDs used in key-injection facilities (e.g., modified PEDs). A PED used for key injection must be validated and approved to the KLD approval class, or it must be managed in accordance with Requirement 13-9.*			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1-3.a** For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval), and examine the list of approved devices to verify that all HSMs are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 or FIPS 140-3 Level 3, or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.	Approval documentation examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
1-4 The approval listing must match the deployed devices in the following characteristics: • Vendor name • Model name and number • Hardware version number • Firmware version number • The PCI PTS HSM or FIPS 140 Approval Number • For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**1-4.a** For all PCI-approved HSMs used, examine HSM devices and examine the PCI SSC list of Approved PCI PTS Devices to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The PCI PTS HSM number • Any applications, including application version number, resident within the device which were included in the PTS assessment	For each PCI-approved HSM used, describe how the observed HSM device configurations verified that all of the device characteristics at 6A-1.4.a match the PTS listing: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**1-4.b** For all FIPS-approved HSMs used, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 or 140-3 Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The FIPS 140 Approval Number	For each FIPS-approved HSM used, describe how the observed HSM device configurations verified that all of the device characteristics at 6A-1.4.b match the FIPS140-2 Level 3 (or higher) approval listing: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
1-5 Not used in EMS					
Requirements 2, 3 and 4 are not used in P2PE.					
	5-1 Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Generation of cryptographic keys or key components must occur within an SCD. They must be generated by one of the following: • An approved key-generation function of a PCI–approved HSM or POI device • An approved key-generation function of a FIPS 140-2 or FIPS 140-3 Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent laboratory to comply with NIST SP800-22 **Note:** Random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key generation relies upon good quality, randomly generated values.		☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5-1.a** Examine key-management policy documentation to verify that it requires that all devices used to generate cryptographic keys meet one of the following: • An approved key-generation function of a PCI–approved HSM or POI device • An approved key-generation function of a FIPS 140-2 or FIPS 140-3 Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to NIST SP 800-22	Documented POI configuration and deployment procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**5-1.b** Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: • An approved key-generation function of a PCI–approved HSM or POI device • An approved key-generation function of a FIPS 140-2 or FIPS 140-3 Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to NIST SP 800-22	Certification Letters/technical documentation examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**5-1.c** Examine procedures to be used for future generations and/or logs of past key generation to verify devices used for key-generation are those as noted above, including validation of firmware used.	Identify the P2PE Assessor who confirms that devices used for key-generation are those noted above, including validation of firmware used.	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-1 Implement security controls, including dual control and tamper detection, to prevent the unauthorized disclosure of keys or key components.			☐	☐	☐
6-1.1 Any clear-text output of the key-generation process must be managed under dual control. Only the assigned custodian can have direct access to the clear text of any key component/share. Each custodian's access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian, and not to the entire key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-1.1.a** Examine documented procedures to verify the following. • Any key-generation process with clear-text output is performed under dual control • Any output of a clear-text component or share is overseen by only the assigned key custodian(s) for that component/share • Each custodian's access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian, and not the entire key	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**6-1.1.b** Observe key-generation process demonstration and interview responsible personnel to verify: • Any key-generation process with clear-text output is performed under dual control. • Any output of clear-text component or share is overseen by only the assigned key custodian(s) for the component/share. • Each custodian's access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian and not the entire key	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the key generation processes observed verified that any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-1.2 There must be no point in the key-generation process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key. Note: Key shares derived using a recognized secret-sharing algorithm or full-length key components are not considered key parts and do not provide any information regarding the actual cryptographic key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-1.2.a** Examine documented procedures for all key-generation methods and observe demonstrations of the key-generation process from end-to-end to verify there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.	Describe how the end-to-end process observed verified that there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-1.2.b** Examine key-generation logs to verify that: • The documented procedures were followed, and • At least two individuals performed the key-generation processes.	Key-generation logs reviewed: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-1.3 Devices used for the generation of clear-text key components that are output in the clear must either be powered off when not in use or require re-authentication whenever key generation is invoked. Logically partitioned devices used concurrently for other processes—e.g., providing services simultaneously to host systems, such as for transaction processing—must have key-generation capabilities disabled when not in use and other activities are continuing.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-1.3.a** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate clear-text key components are powered off when not in use or require re-authentication whenever key generation is invoked; or • If the device used for key generation is logically partitioned for concurrent use in other processes, the key-generation capabilities are enabled for execution of the procedure and disabled when the procedure is complete.	Documented key-generation procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-1.4 Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (e.g., unknown cables) and must be inspected prior to the initialization of key-generation activities. Ensure there isn't any mechanism that might disclose a clear-text key or key component (e.g., a tapping device) between the key-generation device and the device or medium receiving the key or key component. **Note:** This does not apply to logically partitioned devices located in data centers that are concurrently used for other purposes, such as transaction processing.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-1.4.a** Examine documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering prior to use. Verify procedures include a validation step to ensure no unauthorized mechanism exists that might disclose a clear-text key or key component (e.g., a tapping device).	Documented key-generation procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**6-1.4.b** Observe key-generation set-up processes for all key types to verify that key-generation equipment is inspected prior to use, to ensure equipment does not show any signs of tampering. Verify procedures include a validation step to ensure no unauthorized mechanism exists that might disclose a clear-text key or key component (e.g., a tapping device).	Describe how the key-generation set-up processes observed verified that key-generation equipment is inspected prior to use to ensure equipment does not show any signs of tampering:			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the area during key-generation processes where clear-text keying material is in use. It must not be feasible to observe any clear-text keying material either directly or via camera monitoring.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-1.5.a** Examine documentation to verify that physical security controls (e.g., partitions or barriers) are defined to ensure the key component cannot be observed or accessed by unauthorized personnel.	Documentation examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**6-1.5.b** During the demonstration for 6-1.1.b, observe the physical security controls (e.g., partitions or barriers) used, and validate that they ensure the key-generation process cannot be observed or accessed by unauthorized personnel directory or via camera monitoring (including those on cellular devices).	Describe how the physical security controls observed verified that key-component/key-generation process cannot be observed or accessed by unauthorized personnel: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
6-2 Multi-use/purpose computing systems must not be used for key generation where any clear-text secret key or private key, or key component thereof, appears in memory outside the tamper-protected boundary of an SCD. For example, it is not permitted for the cryptographic key to be passed through the memory of a computer unless it has been specifically tasked for the sole purpose of key generation/loading. Computers that have been specifically purposed and used solely for key generation/loading are permitted for use if all other requirements can be met, including those of Requirement 5 and the controls defined in Requirement 13. Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices that do not have the ability to access clear-text cryptographic keys or components. Single-purpose computers with an installed SCD or a modified PED where clear keying material is injected directly from a secure port on the key-generating SCD to the target (e.g., a POI device) meet this requirement. Where the components pass through memory of the PC, Requirement 13 must be met. SCDs used for key generation must meet Requirement 5-1. **Note:** See Requirement 5 and Requirement 13.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-2.a** Examine documented procedures to verify that multi-purpose computing systems are not permitted for key generation where any clear-text secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**6-2.b** Observe the generation process and examine documentation for each type of key to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD except where Requirement 5 and Requirement 13 are met.	Vendor documentation reviewed for each type of key:	<Report Findings Here>		
		Describe how the generation process observed for each type of key verified that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**6-2.c** Where single-purpose computers with an installed SCD or a modified PED are used, verify that either: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) or • Where clear keying material passes through memory of the PC, the PC requirements of **Requirement 13** are met.	Describe how the single-purpose computers with an installed SCD verified that either: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device), or • Where clear keying material passes through unprotected memory of the PC, the PC requirements of **Requirement 13** are met. <Report Findings Here>			
6-3 Printed key components must be printed within blind mailers or sealed in tamper-evident and authenticable packaging immediately after printing or transcription to ensure that: • Only approved key custodians can observe the key component. • Tampering can be visually detected. Printers used for this purpose must not be used for other purposes, must not be networked (i.e., locally connected only), and must be managed under dual control. Location must be a secure room that meets the following requirements: **Note:** Printed key components includes manual (handwritten) capture.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.a** Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed in tamper-evident and authenticable packaging immediately after printing such that: • Only approved key custodians can observe the key component. • Tampering can be visually detected.	Documented procedures for printed key components examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**6-3.b** Observe blind mailers, tamper-evident and authenticable packaging, or other sealed containers used for key components to verify that components cannot be read from within and that tampering can be visually detected.	Describe how the blind mailers or other sealed containers used for key components observed verified that tampering can be visually detected: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-3.c** Observe processes for printing key components to verify that : • Key components are printed within blind mailers or sealed in tamper-evident and authenticable packaging (that is able to be authenticated) immediately after printing, such that no one but the authorized custodian ever has physical access to the output; • Printers are not networked; and • Printers used for this purpose are not used for other purposes and are used only under dual control.	Describe how processes observed for printing key components verified the criteria in the test procedure: <Report Findings Here>			
6-3.1 The room must have walls made of solid materials. The walls do not have to extend from true floor to true ceiling but do need to extend from floor to ceiling.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.1** Inspect the secure room designated for printing clear-text key components to verify that the walls are made of solid materials and extend from floor to ceiling.	Identify the P2PE Assessor who confirms the walls are made of solid materials and extend from floor to ceiling in the secure room designated for printing clear-text key components: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-3.2 Any windows into the secure room must be: • Locked and protected by alarmed sensors. • Covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.2.a** Observe all windows in the secure room to verify they are: • Locked and protected by alarmed sensors. • Covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	Identify the P2PE Assessor who confirms all windows in the secure room are: • Locked and protected by alarmed sensors. • Covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-3.2.b** Examine configuration of window sensors to verify that the alarm mechanism is active.	Identify the P2PE Assessor who confirms the alarm mechanism is active for the window sensors:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
6-3.3 An electronic access control system (for example, badge and/or biometrics) must be in place that: • Enforces dual-access requirements for entry into the secure room, and anti-pass-back requirements. • Supports generation of an alarm when one person remains alone in the secure room for more than 30 seconds.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.3.a** Observe authorized personnel entering the secure room to verify that a badge-control system is in place that enforces the following requirements: • Dual access for entry to the secure room • Anti-pass-back	Identify the P2PE Assessor who confirms that a badge-control system is in place that enforces the following requirements for authorized personnel entering the secure room: • Dual access for entry to the secure room • Anti-pass-back			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-3.3.b** Examine alarm mechanisms and interview alarm-response personnel to verify that the badge-control system supports generation of an alarm when one person remains alone in the secure room for more than 30 seconds.	Identify the P2PE Assessor who confirms through observation and interview of personnel that the badge-control system supports an alarm being generated when one person remains alone in the secure room for more than 30 seconds.			
		<Report Findings Here>			
6-3.4 CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be motion-activated, in which case the recording must continue for at least a minute after the last pixel of activity subsides.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.4** Inspect CCTV configuration and examine a sample of recordings to verify that CCTV monitoring includes the ability to record events during dark periods, and verify that, if motion-activated, recording continues for at least a minute after the last pixel of activity subsides.	Identify the P2PE Assessor who confirms through observation and examination of sample recordings that a CCTV monitoring includes the ability to record events during dark periods, and verify that, if motion-activated, recording continues for at least a minute after the last pixel of activity subsides.			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-3.5 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.5** Inspect configuration of monitoring systems and interview monitoring personnel to verify that monitoring is supported on a continuous (24/7) basis and alarms can be resolved by authorized personnel.	Identify the P2PE Assessor who confirms through observation and interview of personnel that monitoring is supported on a continuous (24/7) basis and alarms can be resolved by authorized personnel.			
		<Report Findings Here>			
6-3.6 The CCTV server and digital storage must be secured in a separate secure location that is not accessible to personnel who have access to the secure room.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.6.a** Inspect location of the CCTV server and digital storage to verify they are located in a secure location that is separate from the secure room.	Identify the P2PE Assessor who confirms the CCTV server and digital storage are located in a secure location that is separate from the secure room.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-3.6.b** Inspect access-control configurations for the CCTV server/storage secure location and the key-injection secure room to identify all personnel who have access to each area. Compare access lists to verify that personnel with access to the secure room do not have access to the CCTV server/storage secure location.	Identify the P2PE Assessor who confirms all personnel who have access to the access-control configurations for the CCTV server/storage secure location and the key-injection secure room do not have access to the CCTV server/storage secure location.			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-3.7 The CCTV cameras must be positioned to monitor: • The entrance door, • Any safes that are present, and • Any equipment that is used.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.7** Inspect CCTV positioning and examine a sample of recordings to verify that CCTV cameras are positioned to monitor: • The entrance door, • Any safes that are present, and • Any equipment that is used.	Identify the P2PE Assessor who confirms through observation and examination of sample recordings that CCTV cameras are positioned to monitor: • The entrance door, • Any safes that are present, and • Any equipment that is used.			
		<Report Findings Here>			
6-3.8 CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.8** Inspect CCTV positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.	Identify the P2PE Assessor who confirms through observation and examination of sample recordings that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-3.9 Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-3.9.a** If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	Identify the P2PE Assessor who confirms digital-recording system configurations have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**6-3.9.b** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.	Identify the P2PE Assessor who confirms at least the most recent 45 days of images are securely archived from captured recordings.			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
6-4 Any residue that may contain clear-text keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual. Examples of where such key residue may exist include (but are not limited to): • Printing material, including ribbons and paper waste • Memory storage of a key-loading device, after loading the key to a different device or system • Other types of displaying or recording (e.g., printer memory, printer drum)			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures ensure the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • Specific direction as to the method of destruction is included in the procedure. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device(s) that will use the key. Examine logs of past destructions and deletions to verify that procedures are followed.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**6-4.b** Observe the destruction process of each identified type of key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • The method of destruction is consistent with Requirement 24. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device(s) that will use the key.	Describe how the destruction process of the identified key residue observed verified that any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation:			
		<Report Findings Here>			
		Identify the P2PE Assessor who confirms that the method of destruction is consistent with Requirement 24.	<Report Findings Here>		
		If a key is generated in a separate device before being exported into the end-use device, describe how the destruction process of the identified key residue observed verified that the key and all related critical security parameters are deleted from the generation and/or injection device immediately after the transfer to the device that will use the key:			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
6-5 Asymmetric-key pairs must either be: • Generated by the device that will use the key pair; or • If generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (zeroized) immediately after the transfer to the device that will use the key pair.	Documented procedures for asymmetric-key generation examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**6-5.b** Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (e.g., zeroized) immediately after the transfer to the device that will use the key pair.	Describe how the key-generation processes observed verified that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted immediately after the transfer to the device that will use the key pair. <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
6-6 Policy and procedures must exist to ensure that clear-text private or secret keys or their components/shares are not transmitted across insecure channels. Preclusions include but are not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying clear-text private or secret keys or components • Conveying clear-text private key shares or secret key components/shares without containing them within tamper-evident and authenticable packaging • Writing key or component values into startup instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manuals			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**6-6.a** Examine documented policy and procedures to verify that they include language that prohibits transmitting clear-text private or secret keys or their components/shares across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying clear-text keys or components • Conveying clear-text private key shares or secret key components/shares without containing them within tamper-evident and authenticable packaging • Writing key or component values into startup instructions • Affixing key or component values to or inside devices • Writing key or component values in procedure manual	Documented policy and procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**6-6.b** From observation of key-management processes verify that clear-text private or secret keys or their components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying clear-text keys or components • Conveying clear-text private or secret key components without containing them within tamper-evident, authenticable packaging • Writing key or component values into startup instructions • Affixing key or component values to or inside devices • Writing key or component values in procedure manual	Describe how the key-management processes observed verified that key components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Conveying clear-text private or secret key components without containing them within tamper-evident, authenticable packaging • Writing key or component values into startup instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manual			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
7-1 Written key-generation policies and procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of these procedures. Procedures for creating all keys must be documented.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**7-1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations and address all keys in scope.	Documented key-generation procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**7-1.b** Interview those responsible for the key-generation processes (including key custodians, supervisory staff, technical management, etc.) to verify that the documented procedures are known and understood by all affected parties.	Responsible personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**7-1.c** Observe key-generation ceremonies, whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.	Describe how the observation of actual or demonstrative key-generation ceremonies verified that the documented procedures are demonstrably in use: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
7-2 Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs. The minimum log contents include date and time, object name/identifier, purpose, name and signature of individual(s) involved, and tamper-evident package number(s) and serial number(s) of device(s) involved.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**7-2.a** Examine documented key-generation procedures to verify that key-generation events for higher-level keys (e.g., KEKs shared with other organizations or otherwise manually loaded as components and MFKs and BDKs) are logged.	Documented key-generation procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**7-2.b** Observe demonstrations for the generation of higher-level keys to verify that all key-generation events are logged.	Describe how the demonstrations for all types of key-generation events observed verified that all key-generation events are logged: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**7-2.c** Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded and that all required elements were captured.	Key generation logs examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
8-1 Keys must be transferred either encrypted, as two or more full-length clear-text components, key shares, or within an SCD. Clear-text key components/shares must be conveyed in SCDs or using tamper-evident, authenticable packaging. Where key components are transmitted in clear text using pre-numbered, tamper-evident, authenticable mailers: Components/shares must be conveyed using at least two separate communication channels, such as different courier services. Components/shares sufficient to form the key must not be conveyed using the same communication channel. Details of the serial number of the package are conveyed separately from the package itself. Documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material. Where SCDs are used for conveying components/shares, the mechanisms or data (e.g., PIN) to obtain the key component/share from the SCD must be conveyed using a separate communication from the SCD channel, or it must be conveyed in the same manner as a paper component. SCDs must be inspected for signs of tampering. Where an SCD (i.e., HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering. ***Note:*** *Components/shares of encryption keys must be conveyed using different communication channels, such as different courier services. It is not sufficient to send key components/shares for a specific key on different days using the same communication channel.*		☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**8-1.a** Determine whether keys are transmitted encrypted, as clear-text components/shares, or within an SCD.	Identify the P2PE Assessor who determined whether keys are transmitted encrypted, or as clear-text components, or within an SCD:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**8-1.b** If key components are transmitted in clear text using pre-numbered, tamper-evident, authenticable packaging, perform the following: Examine documented procedures for sending components in tamper-evident, authenticable packaging to verify that • They define how the details of the package serial number are to be transmitted. • There is a requirement that the package serial number is to be sent separately from the package itself. • Each component is to be sent to/from only the custodian(s) authorized for the component. • At least two communication channels are used to send the components of a given key (not just separation by sending on different days). • Prior to the use of the components, the serial numbers are to be confirmed. Confirm through observation, interview, and inspection of the records of past key transfers that the process used to transport clear-text key components using pre-	Documented procedures reviewed:	<Report Findings Here>		
		Records of key conveyances examined:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the observed method to transport clear-text key components using tamper-evident mailers verified that details of the serial number of the package are transmitted separately from the package itself:			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
	numbered, tamper-evident, authenticable packaging, is sufficient to ensure: • The package serial number was transmitted as prescribed. • The details of the serial number of the package were transmitted separately from the package itself. • At least two communication channels were used to send the components of a given key (not just separation by sending on different days). • Each component was sent to/from only the custodian(s) authorized for the component. • Prior to the use of the component, the serial number was confirmed.	<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**8-1.c** Where SCDs are used to convey components/shares: • Examine documented procedures to verify that the mechanism to obtain the keying material (e.g., PIN) is conveyed using a separate communication channel from the associated SCD. • Examine documented procedures to verify that each SCD is inspected to ensure that there are not any signs of tampering. • Examine the chain-of-custody document for the SCDs and any transport logs to ensure the movement of each device is tracked and that there is evidence that the SCDs and dual-control mechanisms were separated sufficiently to ensure that no one person gained access to the SCDs and both SCD enablers.	Documented procedures examined:	<Report Findings Here>		
		Records of key conveyances examined:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**8-1.d** Where an SCD is conveyed with pre-loaded secret and/or private keys, perform the following: • Examine documented procedures to verify that the SCD requires dual-control mechanisms to become operational. • Examine the documented procedures to ensure the method of shipment of the SCD and dual-control mechanisms (e.g., smart cards or passphrases) are separated in a way that ensures there is no opportunity for one person to gain access to the SCD and both authorization mechanisms (e.g., both smartcards, etc.). • Examine documented procedures to verify that the SCD is inspected to ensure there are no signs of tampering. • Examine records of key transfers and interview responsible personnel to verify the mechanisms that make the SCD operational are conveyed using separate communication channels.	Documented procedures examined:	<Report Findings Here>		
		Records of key conveyances examined:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
8-2 A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. ***Note:*** *An m-of-n scheme is a component- or share-allocation scheme where m is the number of shares or components necessary to form the key, and n is the number of the total set of shares or components related to the key. Management of the shares or components must be sufficient to ensure that no one person can gain access to enough of the item to form the key alone* E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**8-2.a** Examine documented procedures to verify they include controls to ensure that no single person can gain access to components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. Verify procedures include: • Designation of person(s) permitted to convey/receive keys. • Reminder that any person with access to one component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component or shares sufficient to form the necessary threshold to derive the key. • Steps to ensure any person with access to the media conveying a component/share of a key could not have access to other components/shares of this key, or to any other medium conveying any other component of this key that is sufficient to form the necessary threshold to derive the key, without detection.	Documented device-configuration procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**8-2.b** Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can gain access to components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. Verify the implemented controls ensure the following: • Only designated custodians can send/receive the component or share • There is a clear understanding that an individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key • There is sufficient evidence to show that a person with access to the media conveying a key component or key share could not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key without detection	Personnel interviewed:	<Report Findings Here>		
		Describe how the observed key-transfer processes verified that: • An individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying other components or shares of this key that are sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a key component or key share must not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**8-2.c** Examine records of past key transfers to verify that the method used did not allow for any personnel to have access to components or shares sufficient to form the key.	Logs examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
8-3 E-mail must not be used for the conveyance of secret or private keys or their components/shares, even if encrypted, unless the key (or component/share) has already been encrypted in accordance with these requirements—i.e., in an SCD. This is due to the existence of these key values in memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear text of any encrypted text or files conveyed through those systems. Other similar mechanisms, such as SMS, fax, or telephone must not be used to convey clear-text key values.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**8-3.a** Validate through interviews, observation, and log inspection that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components/shares.	Personnel interviewed:	<Report Findings Here>		
		Logs reviewed:	<Report Findings Here>		
		Describe the observations that confirmed that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
8-4 Public keys must be conveyed in a manner that protects their integrity and authenticity. • Examples of acceptable methods include: • Use of public-key certificates as defined in within this Domain that are created by a trusted CA that meets the applicable requirements of this Domain • Validating a hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 • Conveyance within an SCD • Encrypted ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.* Self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data. The authenticity of the root certificate is based on the use of secure procedures to distribute them. Specifically, they must be directly installed into the PIN pad of the ATM or POS device and not remotely loaded to the device subsequent to manufacture. For all methods used to convey public keys, perform the following:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**8-4.a** Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity, such as: • Use of public-key certificates created by a trusted CA that meets the applicable requirements of this Domain • Validation of a hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 • Conveyance within an SCD • Encrypted	Documented procedures examined: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**8-4.b** Validate that procedures dictate that self-signed certificates must not be used as the sole method of authentication.	Identify the P2PE Assessor who attests that self-signed certificates must not be used as the sole method of authentication:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**8-4.c** Observe the process for conveying public keys, associated logs, and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the observed process for conveying public keys verified that all methods ensure public keys are conveyed in a manner that protects their integrity and authenticity:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
9-1 During the process to convey it, any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • Sealed in a security container or courier mailer (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it and unauthorized access would be detected, or • Contained within a physically secure SCD. **Note**: No single person must be able to access or use all components or a quorum of shares of a single secret or private cryptographic key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, • Sealed in a security container or courier mailer (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or • Contained within a physically secure SCD.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**9-1.b** Observe key-management processes, examine associated logs, and interview responsible personnel to verify processes implemented ensure that any single clear-text secret or private key component/share is at all times either: • Under the continuous supervision of a person with authorized access to this component • Sealed in a security container or courier mailer (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, or contained within a physically secure SCD.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the key-management processes observed verified that processes are implemented to ensure that any single clear-text secret or private key component/share is at all times either: • Under the continuous supervision of a person with authorized access to this component • Locked in a security container (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or • Contained within a physically secure SCD.			
		<Report Findings Here>			
9-2 Packaging or mailers (i.e., pre-numbered, tamper-evident packaging) containing clear-text key components are examined for evidence of tampering before being opened. Any sign of package tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the destruction and replacement of: • The set of components • Any keys encrypted under this (combined) key			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-2.a** Verify documented procedures include requirements for all packaging or mailers containing clear-text key components to be examined for evidence of tampering before being opened.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**9-2.b** Interview responsible personnel and observe processes to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being opened.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the processes observed verified that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being opened:			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**9-2.c** Verify documented procedures require that any sign of package tampering is identified, reported, and, if compromise is confirmed, ultimately results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**9-2.d** Interview responsible personnel and observe processes to verify that if a package shows signs of tampering indicating a component was potentially compromised, processes are implemented to identify the tampering, report/escalate it, and, if compromise is confirmed, ultimately result in the destruction and replacement of both: • The set of components, and • Any keys encrypted under this (combined) key	Responsible personnel interviewed :	<Report Findings Here>		
		Describe how the process observed verified that if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**9-2.e** Examine records related to any escalated transmittal events. Verify that if compromise is confirmed it resulted in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key	Documented records examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
9-3 Only an authorized key custodian and designated backup(s) must have physical access to a key component prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-3.a** Verify the existence of a list(s) of key custodians and designated backup(s) authorized to have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.	Documented reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**9-3.b** Observe implemented access controls and processes to verify that only those authorized key custodians and designated backup(s) have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.	Describe the implemented access controls and processes observed that verified that only those authorized key custodians (and designated backup(s)) have physical access to key components prior to being secured in transmittal packaging: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**9-3.c** Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each component.	Physical access logs examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
9-4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal. • Check tamper-evident packaging upon receipt for signs of tampering prior to opening tamper-evident authenticable packaging containing key components. • Check the serial number of the tamper-evident packaging upon receipt of a component package. **Note**: See Requirement 26 for logging.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-4.a** Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.	Documented reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**9-4.b** Observe implemented mechanisms and processes and examine logs to verify that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.	Describe how the implemented mechanisms and processes observed verified that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package. <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
9-5 Pre-numbered, tamper-evident, authenticable bags must be used for the conveyance of clear-text key components not in an SCD. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers. **Note**: Numbered courier bags are not sufficient for this purpose.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-5** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. • Examine logs to verify that procedures are followed.	Documented procedures reviewed:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the observed method used to transport clear-text key components using tamper-evident mailers verified that details of the serial number of the package are transmitted separately from the package itself:			
		Documented procedures reviewed:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
9-6 If components or shares of multiple keys are being sent simultaneously between the same sending and receiving custodians, the component/shares for a specific custodian or custodian group can be shipped in the same TEA bag provided that: • The components inside the tamper-evident and authenticable package are in separate opaque and identifiable packaging (e.g., individually sealed within labeled, opaque envelopes or PIN mailers) to prevent confusion and/or inadvertent observation when the package is opened. • The components are repackaged at receipt into separate tamper-evident and authenticable packages for storage at the receiving location. Records reflect the receipt of the shipped bag and association with subsequent individual bags.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**9-6.a** If components or shares of multiple keys are being sent simultaneously between the same sending and receiving custodians, the component/shares for a specific custodian or custodian group can be shipped in the same TEA bag provided that: • The components inside the tamper-evident and authenticable package are in separate opaque and identifiable packaging (e.g., individually sealed within labeled, opaque envelopes or within PIN mailers) to prevent confusion and/or inadvertent observation when the package is opened. • The components are repackaged at receipt into separate tamper-evident and authenticable packages for storage at the receiving location. • Records reflect the receipt of the shipped bag and association with subsequent individual bags.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**9-6.b** Examine logs to verify that procedures are followed.	Logs reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
10-1 All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be at least as strong as the key being sent, as delineated in Annex C., except as noted below for RSA keys used for key transport. • TDEA keys used for encrypting keys must be at least triple-length keys (have bit strength of 112 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. • A triple-length TDEA key must not be encrypted with a TDEA key of lesser strength. • TDEA keys must not be used to protect AES keys. • TDEA keys must not be used to encrypt keys greater in strength than 112 bits. • RSA keys encrypting keys greater in strength than 80 bits shall must have a bit strength of at least 112 bits.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**10-1.a** Examine documented procedures to verify there is a requirement that all keys used to transmit or convey other cryptographic keys must be at least as strong as any key transmitted or conveyed, as delineated in Annex C. (except as noted for RSA keys).	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**10-1.b** Using the network schematic and the summary listing of cryptographic keys and through interview of personnel, identify keys that protect other keys for transmission. Consider keys manually transferred (e.g., cryptograms sent to an ESO) as well as those that are system-generated and transferred (e.g., KEK or TMK encrypting working keys).	Appropriate Personnel interviewed:	<Report Findings Here>		
		Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**10-1.c** Observe key-generation processes for the key types identified above. Verify that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed, except as noted for RSA keys. To verify that: • Interview appropriate personnel and examine documented procedures for the creation of these keys. • Using the table in Annex C, validate the respective key sizes relative to the algorithms used for key encryption. • Verify that: • TDEA keys used for encrypting keys must be at least triple-length keys (have an effective bit strength of 112 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. • A triple-length TDEA key must not be encrypted with a TDEA key of lesser strength. • TDEA keys are not used to protect AES keys. • TDEA keys are not be used to encrypt keys greater in strength than 112 bits. • RSA keys encrypting keys greater in strength than 80 bits have a bit strength at least 112 bits.	Describe how the key-generation processes observed verified that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed, as delineated in Annex C. <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**10-1.d** Examine system documentation and configuration files to validate the above, including HSM settings.	System documentation examined: <Report Findings Here>			
10-2 to 10-5 Not used in P2PE					

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
11-1 Written procedures must exist and be known to all affected parties.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**11-1.a** Verify documented procedures exist for all key transmission and conveyance processing.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**11-1.b** Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.	Responsible personnel interviewed:	<Report Findings Here>		
11-2 Methods used for the conveyance or receipt of keys must be documented.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**11-2.a** Verify documented procedures include all methods used for the conveyance or receipt of keys.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
12-1 The loading of secret or private keys, when from the individual key components or shares, must be performed using the principles of dual control and split knowledge. **Note**: Manual key loading may involve the use of media such as paper, smart cards, or other physical tokens.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-1.a** Using the summary of cryptographic keys, identify keys that are loaded from components and examine documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-1.b** Interview appropriate personnel to determine the number of key components for each manually loaded key.	Appropriate personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-1.c** Witness a structured walk-through/demonstration of various key-loading processes for all key types (MFKs, AWKs, TMKs, PEKs, etc.). Verify the number and length of the key components against information provided through verbal discussion and written documentation.	Describe how the structured walk-through/demonstration verified that the number and length of the key components is consistent with information provided through verbal discussion and written documentation: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**12-1.d** Verify that the process includes the entry of individual key components by the designated key custodians.	Describe how the structured walk-through/demonstration verified that the process includes the entry of individual key components by the designated key custodians: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**12-1.e** Ensure key-loading devices can only be accessed and used under dual control.	Describe how the structured walk-through/demonstration verified that key-loading devices can only be accessed and used under dual control: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**12-1.f** Examine locations where keys may have been recorded that don't meet this requirement. As applicable, examine HSM startup documentation (including Disaster Recovery or Business Continuity Planning documentation) and procedure manuals to ensure that there are no key or component values recorded.	Describe how the review of locations where keys may have been recorded verified there are no key or component values recorded. <Report Findings Here>			
12-2 Procedures must be established that will prohibit any one person from having access to components sufficient to form an encryption key when components are removed from and returned to storage for key loading.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-2.a**. Examine logs of access to security containers for key components/shares to verify that only the authorized custodian(s) have accessed them. Compare the number on the current tamper-evident and authenticable package for each component to the last log entry for that component. Trace historical movement of higher-order keys (MFK, KEK, and BDK) in and out of secure storage to ensure there is no break in the package-number chain that would call into question authorized handling and sufficient storage of the component or share. This must address at a minimum the time frame from the date of the prior audit.	Access logs examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
12-3 The loading of clear-text cryptographic keys using a key-loading device requires dual control to authorize any key-loading session. It must not be possible for a single person to use the key-loading device to load clear keys alone. • Dual control must be implemented using one or more of, but not limited to, the following techniques: • Two or more passwords/authentication codes of five characters or more (vendor default values must be changed) • Multiple cryptographic tokens (such as smartcards), or physical keys • Physical access controls • Separate key-loading devices for each component/share ***Note**: For devices that do not support two or more passwords/authentication codes, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian. Each half must be a minimum of five characters.* ***Note:** Passwords/authentication codes to the same object may be assigned to a custodian group team e.g., custodian team for component A.* ***Note:** The addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS POI Security Requirements and listed as such in the approval listings. If a PED that has been modified to perform these functions has not been validated and approved to the KLD approval class, the PED must be managed in accordance with Requirement 13-9.*			☐	☐	☐

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**12-3.a** Identify instances where a key-loading device is used to load clear-text keys. Examine documented procedures for loading of clear-text cryptographic keys to verify that: • Procedures require dual control to authorize any key-loading session. • The techniques to be used to achieve dual control are identified. • There is a requirement to change any default passwords/authentication codes and set passwords/authentication codes that have at least five characters. • There is a requirement that if passwords/authentication codes or tokens are used, they be maintained separately.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-3.b** For each type of production SCDs loaded using a key-loading device, observe for the process (e.g., a demonstration) of loading clear-text cryptographic keys and interview personnel. Verify that: • Dual control is necessary to authorize the key-loading session. • Expected techniques are used. • Default passwords/authentications codes are reset. • Any passwords/authentication codes used are a minimum of five characters. • Any passwords/authentication codes or tokens are maintained separately.	Describe how the observed processes for loading clear-text cryptographic keys for all types of production SCDs verified that dual control is required to authorized any key-loading sessions, expected techniques are used, any passwords used are a minimum of five characters (default passwords/authentication codes are reset) and any passwords/authentication codes or tokens are maintained separately: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**12-3.c** Examine documented records of key-loading to verify the presence of two authorized persons during each type of key-loading activity.	Documented records of key-loading processes reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-3.d** Ensure that any default dual-control mechanisms (e.g., default passwords/authentication codes—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.	Describe how default dual-control mechanisms were verified to have been disabled or changed: <Report Findings Here>			
12-4 Key components for symmetric keys must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components e.g., via XOR'ing of full-length components. The resulting key must only exist within the SCD. **Note**: Concatenation of key components together to form the key is unacceptable; e.g., concatenating two 8-hexadecimal character halves to form a 16-hexadecimal secret key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-4.a** Examine documented procedures for combining symmetric-key components and observe processes to verify that key components are combined using a process such that no active bit of the key can be determined without knowledge of the remaining components e.g., only within an SCD.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-4.b** Confirm key-component lengths through interview and examination of blank component forms and documented procedures. Examine device configuration settings and interview personnel to verify that key components used to create a key are the same length as the resultant key.	Describe how the key-component lengths or device configuration settings observed verified that key components used to create a key are the same length as the resultant key: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
12-5 Hardware security module (HSM) Master File Keys (MFK), including those generated internal to the HSM and never exported, must use AES with a key size of at least 128 bits.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-5.a** Examine vendor documentation describing options for how the HSM MFK is created and verify the current MFK was created using AES (or triple-length TDEA for existing P2PE implementations only). Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.	Vendor documentation reviewed:	<Report Findings Here>		
		Identify the P2PE Assessor who corroborated how the HSM MFK is created:	<Report Findings Here>		
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-6.a** Thorough examination of documented procedures, interviews, and observation, confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key.	Documented procedures reviewed:	<Report Findings Here>		
		Personnel interviewed:	<Report Findings Here>		
		Describe how it was confirmed that any devices that are loaded with the same key components use the same mathematical process to derive the final key:			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
12-7 The initial terminal master key (TMK) or initial DUKPT key must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key or an initial DUKPT key may use techniques described in this document such as: • Asymmetric techniques • Manual techniques • The existing TMK to encrypt the replacement TMK for download • For AES DUKPT, using the option to derive a key-encryption key called the DUKPT Update Key so that the host can send a device a new initial key encrypted under that key. Note this also requires that a new initial key ID is also sent. • Keys must not be reloaded by any methodology in the event of a compromised device and must be withdrawn from use.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-7.a** Examine documented procedures for the loading of TMKs and initial DUKPT keys to verify that they require asymmetric key-loading techniques or manual techniques for initial loading and allowed methods for replacement TMK or initial DUKPT key loading.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-7.b** Examine documented procedures to verify that keys are withdrawn from use if they were loaded to a device that has been compromised or gone missing.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
12-8 If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, these must meet the applicable requirements detailed in this document. For example: • A public-key technique for the distribution of symmetric secret keys must: • Use public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Provide for mutual device authentication for both the host and the POI device or host-to-host if applicable, including assurance to the host that the POI device has (or can compute) the session key, and that no entity other than the POI device specifically identified can possibly compute the session key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**12-8.a** For techniques involving public-key cryptography, examine documentation to illustrate the process, including the size and sources of the parameters involved, and the mechanisms utilized for mutual device authentication for both the host and the POI device.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**12-8.b** If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, verify that the applicable requirements detailed in this Domain are met, including: • Use of public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.	Identify the P2PE Assessor who confirms that requirements detailed in this document are met where key-establishment protocols using public-key cryptography are used to remotely distribute secret keys:	<Report Findings Here>		
12.9 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
13-1 Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that: • Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of clear-text key components. • There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys. • The sending and receiving SCDs must be inspected prior to key loading to ensure that they have not been subject to any prior tampering or unauthorized modification that could lead to the disclosure of clear-text keying material. • SCDs must be inspected to detect evidence of monitoring and to ensure dual control procedures are not circumvented during key loading. • An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are uniquely identified by the device.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-1.a** Observe key-loading environments, processes, and mechanisms (e.g., terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Ensure cameras are positioned to ensure they cannot monitor the entering of clear-text key components. • Examine documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that:	Documented procedures reviewed:	<Report Findings Here>		
		Describe how the demonstration verified that: • SCDs must be inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. • An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are identified by the device. • There is not any mechanism (including cabling) at the interface between the conveyance medium and the SCD device that might disclose the transferred keys. • The SCD is inspected to ensure it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying material.			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
	• SCDs are inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. • An SCD transfers a plaintext secret or private key only when at least two authorized individuals are identified by the device. • There is not any mechanism at the interface (including cabling) between the conveyance medium and the SCD that might disclose the transferred keys. • The SCD is inspected to ensure it has not been subject to any prior tampering or unauthorized modification, which could lead to the disclosure of clear-text keying material.	<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
13-2 Only SCDs must be used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility, as delineated in the requirements contained in this Domain. For example, computer keyboards or those attached to an HSM must never be used for the loading of clear-text secret or private keys or their components. **Note**: The addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS POI Security Requirements and listed as such in the approval listings. If a PED that has been modified to perform these functions has not been validated and approved to the KLD approval class, they must be managed in accordance with Requirement 13-9.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-2.a** Examine documentation to verify that only SCDs are used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility, as delineated in this requirement. For example, computer keyboards or keyboards attached to an HSM must never be used for the loading of clear-text secret or private keys or their components.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**13-2.b** Observe a demonstration of key loading to verify that only SCDs are used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility.	Describe how the observed demonstration verified that only SCDs are used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility.			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
13-3 The loading of clear-text secret or private key components or shares from an electronic medium—e.g., smart card, thumb drive, fob, or other device used for data transport—directly into a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following: • The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium in accordance with Requirement 24.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-3.a** Examine documented procedures for the loading of secret or private key components from electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key injection, including: • Instructions for the medium to be placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium, including the method to use.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**13-3.b** Observe key-loading processes to verify that the injection process results in one of the following: • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.	Describe how the observed key-loading processes verified that the injection process results in one of the following: • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions		Assessor's Findings		
				In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**13-3.c** Examine records/logs of erasures to confirm that: • The documented procedure was followed. • The method used was in accordance with Requirement 24.	Logs examined:	<Report Findings Here>			
13-4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:				☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-4** Examine documented procedures and observe processes for the use of key-loading devices. Perform the following:					
13-4.1 The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected. **Note**: A PCI-approved KLD meets this requirement for an SCD.				☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-4.1** Verify the key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.	Documented procedures reviewed:	<Report Findings Here>			
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected:				
		<Report Findings Here>				

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions		Assessor's Findings		
				In Place	N/A	Not In Place
13-4.2 The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it. **Note:** Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.				☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-4.2** Verify the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.	Documented procedures reviewed:	<Report Findings Here>			
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it:				
		<Report Findings Here>				
13-4.3 The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.				☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-4.3.a** Verify the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD.	Documented procedures reviewed:	<Report Findings Here>			
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD:				
		<Report Findings Here>				
PDCP **PMCP** **EMCP** **SP**	**13-4.3.b** Verify that both authorized personnel involved in key-loading activity inspect the key-loading device prior to use to ensure that a key-recording device has not been inserted between the SCDs.	Documented procedures reviewed:	<Report Findings Here>			
		Describe how the observed processes for the use of key-loading devices verified that authorized personnel inspect the key-loading device prior to use to ensure that a key-recording device has not been inserted between the SCDs:				
		<Report Findings Here>				

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
13-4.4 The key-loading device must not retain any information that might disclose the key (e.g., allow replay of the key for injection into a non-SCD) that was installed in the device or a key that it has successfully transferred.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-4.4** Verify the key-loading device does not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred. For example, attempt to output the same value more than one time from the device or cause the device to display check values for its contents both before and after injection and compare.	Documented procedures reviewed:	<Report Findings Here>		
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device does not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
13-5 Any media (electronic or otherwise) containing secret or private key components or shares used for loading cryptographic keys must be maintained in a secure location and accessible only to authorized custodian(s). When removed from the secure storage location, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process. The media upon which a component resides must be physically safeguarded at all times when removed from secure storage. Key components that can be read (e.g., those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are never used in a manner that would result in the component being displayed in clear text to anyone who is not a designated custodian for that component.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-5.a** Interview personnel and observe media locations to verify that the media is maintained in a secure location accessible only to custodian(s) authorized to access the key components.	Personnel interviewed:	<Report Findings Here>		
		Media locations observed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**13-5.b** Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices be in the physical possession of only the designated component holder(s). • The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions		Assessor's Findings		
				In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**13-5.c** Interview designated component holder(s) and examine key-management logs to verify that media or devices removed from secure storage are in the physical possession of only the designated component holder(s).	Designated component holder(s) interviewed:	<Report Findings Here>			
		Key-management logs examined:	<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**13-5.d** Interview key-injection personnel and examine logs for the removal of media/devices from secure storage to verify they are removed only for the minimum practical time necessary to complete the key-loading process.	Key-injection personnel interviewed:	<Report Findings Here>			
		Logs examined:	<Report Findings Here>			
13-6 If the component is in human-readable form it must be visible only to the designated component custodian and only for the duration of time required for this person to privately enter the key component into an SCD.				☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-6** Validate through interview and observation that if components are in human-readable form, they are visible only to designated component custodians and only for the duration of time required for this person to privately enter the key component into an SCD.	Personnel interviewed:	<Report Findings Here>			
		Describe how it was verified that if components are in human-readable form, they are visible only to designated component custodians and only for the duration of time required for this person to privately enter the key component into an SCD:				
		<Report Findings Here>				

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
13-7 Written or printed key component documents must not be opened until immediately prior to use.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-7.a** Examine documented procedures and confirm that printed/written key component documents are not opened until immediately prior to use.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**13-7.b** Observe key-loading processes and verify that printed/written key component documents are not opened until immediately prior to use.	Describe how the observed key-loading processes verified that printed/written key-component documents are not opened until immediately prior to use: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
13-8 A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**13-8.a** Examine documented procedures for the use of key components to verify that procedures ensure that any individual custodian only has access to their assigned components and never has access to sufficient key components to reconstruct a cryptographic key.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**13-8.b** Examine key-component access controls and access logs to verify that any single authorized custodian can and has only had access to their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.	Describe how the observed key-component access controls and access logs verified that any single authorized custodian can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key: <Report Findings Here>			
13-9 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
14-1 Any hardware and passwords/authentication codes used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. Resources (e.g., passwords/authentication codes and associated hardware) must be managed such that no single individual has the capability to enable key loading of clear-text keys or their components. This is not to imply that individual access authentication mechanisms must be managed under dual control. **Note**: Where key-loading is performed for POI devices, the secure environment as defined in Requirement 32-9 must additionally be met.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**14-1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords/authentication codes and associated hardware) used in the key-loading function or for the signing of authenticated applications must be controlled and managed such that no single individual has the capability to enable key loading of clear-text keys or their components.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-1.b** Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function or for the signing of authenticated applications is controlled and maintained in a secure environment under dual control.	Describe how the observation of key-loading environments and controls verified that: • All hardware used in the key-loading function is controlled and maintained in a secure environment under dual control. • All resources (e.g., passwords and associated hardware) used for key-loading functions are controlled and managed such that no single individual has the capability to enable key loading.			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
	• All resources (e.g., passwords/authentication codes and associated hardware) used for key-loading functions and for the signing of authenticated applications are controlled and managed such that no single individual has the capability to enable key loading.	<Report Findings Here>			
14-2 All cable attachments over which clear-text keying material traverses must be examined at the beginning of an entity's key activity operations (system power on/authorization) or application signing operations to ensure they have not been tampered with or compromised.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**14-2.a** Examine documented procedures to ensure they require that cable attachments are examined at the beginning of an entity's key-activity operations (system power on/authorization) or application signing operations.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-2.b** Observe key-loading processes to verify that all cable attachments are properly examined at the beginning of an entity's key-activity operations (system power on/authorization) or application-signing operations.	Describe how the key-loading processes observed verified that all cable attachments are properly examined prior to key-loading functions: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
14-3 Key-loading equipment usage must be monitored, and a log of all key-loading and application-signing activities maintained for audit purposes must contain, at a minimum, date, time, personnel involved, and number of devices keys are loaded to.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**14-3.a** Observe key-loading and application-signing activities to verify that key-loading equipment usage is monitored.	Describe how the key-loading activities observed verified that key-loading equipment usage is monitored: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**14-3.b** Verify logs of all key-loading and application-signing activities are maintained and contain all required information.	Logs of key-loading activities reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
14-4 Any physical tokens (e.g., brass keys or chip cards) used to enable key loading or the signing of authenticated applications must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control. These tokens must be secured in a manner similar to key components, including tamper-evident, authenticable packaging and the use of access-control logs for when removed or placed into secure storage.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**14-4.a** Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key loading or the signing of authenticated applications. Verify procedures require that physical tokens must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-4.b** Inspect locations and controls for physical tokens to verify that tokens used to enable key loading or the signing of authenticated applications are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control.	Identify the P2PE Assessor who inspected locations and controls for physical tokens and confirms that tokens used to enable key loading are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-4.c** Examine storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.	Identify the P2PE Assessor who confirms adequacy of reviewed storage locations for physical tokens to ensure that only the authorized custodian(s) can access their specific tokens:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**14-4.d** Verify that access-control logs exist and are in use including notation of tamper-evident, authenticable bag numbers.	Access-control logs reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-4.e** Reconcile storage contents to access-control logs.	Identify the P2PE Assessor who reconciled storage contents to access-control logs:	<Report Findings Here>		
14-5 Default passwords/authentication codes used to enforce dual-control mechanisms must be changed, and documented procedures must exist to require that these password/PINs be changed, when assigned personnel change.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**14-5.a** Verify that documented procedures require default passwords/authentication codes used to enforce dual-control mechanisms are changed.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**14-5.b** Verify that documented procedures exist to require that these passwords/authentication codes be changed when assigned personnel change.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
15-1 A cryptographic-based validation mechanism must be in place to ensure the authenticity and integrity of keys and/or their components (e.g., testing key-check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See ISO 11568. Where check values are used, recorded, or displayed key-component check values and key-check values must be generated by a cryptographic process such that all portions of the key or key component are involved in generating the check value. The check value must be in accordance with the following **note**. **Note**: Check values may be computed by two methods. TDEA may use either method. AES must only use the CMAC method. In the first method, check values are computed by encrypting an all binary zeros block using the key or component as the encryption key, using the leftmost n-bits of the result; where n is at most 24 bits (6 hexadecimal digits/3 bytes). In the second method the KCV is calculated by MACing an all binary zeros block using the CMAC algorithm as specified in ISO 9797-1 (see also NIST SP 800-38B). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MACed using the TDEA block cipher, while a 128-bit AES key or component will be MACed using the AES-128 block cipher.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**15-1.a** Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and/or components.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**15-1.b** Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and is verified by the applicable key custodians.	Describe how the key-loading processes observed verified that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and is verified by the applicable key custodians:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**15-1.c** Verify that the methods used for key validation are consistent with ISO 11568—e.g., when check values are used, they are in accordance with this requirement.	Describe how the key-loading processes observed verified that the methods used for key validation are consistent with ISO 11568:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
15-2 The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted in accordance with Annex C, or if in plaintext form, must: • Be within a certificate as defined in applicable requirements within this Domain; or • Be within a PKCS#10 (authentication and integrity occurs via other mechanisms); or • Be within an SCD; or • Have a MAC (message authentication code) created using the algorithm defined in ISO 16609.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**15-2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.	Personnel interviewed:	<Report Findings Here>		
		Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**15-2.b** Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.	Describe how the observed public-key stores and mechanisms verified that public keys exist only in an approved form:			
		<Report Findings Here>			
15-3 not used in EMS					
15-4 not used in EMS					
15-5 not used in EMS					

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
16-1 Documented key-loading procedures must exist for all devices (e.g., HSMs and POI devices), and all parties involved in cryptographic key loading must be aware of those procedures.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**16-1.a** Verify documented procedures exist for all key-loading operations.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**16-1.b** Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.	Responsible personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**16-1.c** Observe the key-loading process for keys loaded as components and verify that the documented procedures are demonstrably in use. This may be done as necessary on test equipment—e.g., for HSMs.	Identify the P2PE Assessor who confirms that the documented procedures for keys loaded as components are demonstrably in use:	<Report Findings Here>		
16-2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**16-2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.	Log files examined:	<Report Findings Here>		
		Describe how the logging processes observed verified that audit trails are in place for all key-loading events:			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
17-1 Where two organizations or logically separate systems share a key to encrypt account data (including a key-encipherment key used to encrypt a data-encryption key) communicated between them, that key must: • Be unique to those two entities or logically separate systems, and • Not be given to any other entity or logically separate systems. **Note**: This requirement does not apply after the decryption environment.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**17-1.a** Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations or logically separate systems.	Documented key matrix reviewed:	<Report Findings Here>		
		Documented operational procedures reviewed:	<Report Findings Here>		
		Personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**17-1.b** For all keys shared between two organizations or logically separate systems for encrypting account data (including key-encryption keys used to encrypt a data-encryption key), perform the following: Generate or otherwise obtain key check values for any key-encipherment keys (KEKs) to verify key uniqueness between the two organizations. A random sample may be used where more than 10 zone connections are in use. This is not intended to be based on values retained on paper or otherwise sent as part of the original conveyance of the keying material, but rather on values generated from stored zone production keys from the production host database. Cryptograms may be used for this purpose if it is verified that the same MFK variant is used to encrypt the KEKs. If a remote key-establishment and distribution scheme is implemented between networks, examine public keys and/or hash values and/or fingerprints of the keys to verify key uniqueness of the asymmetric-key pairs. Compare key check values against those for known or default keys to verify that known or default key values are not used.	Describe how the generation of (or otherwise obtaining) key check values for any key-encipherment keys (KEKs), public keys, and/or hash values and/or fingerprints (where a remote key-establishment and distribution scheme is implemented) verified key uniqueness between the two organizations: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
18-1 Synchronization errors must be monitored to help reduce the risk of an adversary's substituting a key known only to them. Procedures must exist and be followed for investigating repeated synchronization errors for online processes such as online key exchanges or transmission or processing of transactions. **Note**: Multiple synchronization errors may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**18-1.a** Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**18-1.b** Verify that implemented procedures include: • Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) • Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
18-2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of the component and the associated key at all locations where they exist.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**18-2.a** Verify that documented procedures require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**18-2.b** Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it results in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.	Personnel interviewed:	<Report Findings Here>		
		Describe how the processes observed verified that procedures are implemented to require that key-component packaging/containers showing signs of tampering result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
18-3 Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods The phased implementation dates are as follows: • **Phase 1** – Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to hardware security modules (HSM). Effective date: **1 June 2019 (past)**. • **Phase 2** – Implement Key Blocks for external connections to Associations and Networks. Effective date: **1 January 2023**. • **Phase 3** – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Effective date: **1 January 2025**. Acceptable methods of implementing the integrity requirements include, but are not limited to: • A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself e.g. TR-31; • A digital signature computed over that same data, e.g., TR-34; • An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**18-3** Using the cryptographic-key summary to identify secret keys conveyed or stored, examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of the acceptable methods or an equivalent. Where key blocks are not implemented, identify and examine project plans to implement in accordance with the prescribed timeline.	Describe how the documented procedures examined and the key operations observed verified that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of the acceptable methods or an equivalent.			
		<Report Findings Here>			
		Where key blocks are not implemented, describe how the examined project plans verified that key block implementation is in accordance with the prescribed timeline(s).			
		<Report Findings Here>			
18-4 Not used in EMS					
18-5 Not used in EMS					

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
18-6 Not used in EMS					
18-7 Not used in EMS					
19-1 Encryption keys must only be used for the purpose they were intended i.e., key-encryption keys must not be used as PIN-encryption keys, PIN-encryption keys must not be used for account-data, etc. Derivation Keys may be derived into multiple keys, each with its own purpose. For example, a DUKPT Initial Key may be used to derive both a PIN encryption key and a data encryption key. The derivation key would only be used for its own purpose—key derivation. This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**19-1.a** Examine key-management documentation (e.g., the cryptographic-key inventory) and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are defined for a specific purpose.	Key-management documentation examined:	<Report Findings Here>		
		Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**19-1.b** Using a sample of device types, validate via examination of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.	Sample of device types reviewed:	<Report Findings Here>		
		Describe how review of check values, terminal definition files, etc. verified that keys used for key encipherment or PIN encipherment are not used for any other purpose:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
19-2 Private keys: • Must be used only for a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating POI devices). • Must never be used to encrypt other keys. • When used for remote key distribution, must not be used in connection with any other purpose. **Note**: The restriction does not apply to certificate signing requests e.g., PKCS #10.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**19-2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are : • Used only to create digital signatures or to perform decryption operations. • Used only for a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both. • Never used to encrypt other keys. • Not used in connection with any other purpose when used for remote key distribution.	Key-management documentation examined:	<Report Findings Here>		
		Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		
19-3 Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**19-3** Examine key-management documentation and interview key custodian and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for POI devices).	Key-management documentation examined:	<Report Findings Here>		
		Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
19-4 Keys must never be shared or substituted between production and test/development systems. Keys used for production must y present or used in a production system. **Note**: For logically partitioned HSMs and computing platforms, if one or more logical partitions of a physical device are used for production and one or more other logical partitions are used for testing, including QA or similar, the entire configuration that is impacted—computing platform(s) and networking equipment—must be managed and controlled as production.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**19-4.a** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and test/development systems.	Key-management documentation examined:	<Report Findings Here>		
		Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**19-4.b** Observe processes for generating and loading keys into production systems to ensure that they are in no way associated with test or development keys.	Describe how the observed processes for generating and loading keys into production systems verified that they are in no way associated with test or development keys:			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**19-4.c** Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.	Describe how the observed processes for generating and loading keys into test systems verified that they are in no way associated with production keys:			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**19-4.d** Compare check, hash, cryptogram, or fingerprint values for production and test/development keys with higher-level keys (MFKs, KEKs shared with other network nodes, and BDKs) to verify that development and test keys have different key values.	Describe how the observed compared check, hash, cryptogram, or fingerprint values for production and test/development keys with higher-level keys (MFKs, KEKs shared with other network nodes, and BDKs) verified that development and test keys have different key values:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
19-5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements. At all times, the HSMs and servers/computers must be physically and logically secured in accordance with these requirements. **Note**: This does not apply to HSMs that are never intended to be used for production.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**19-5** Interview personnel to determine whether production platforms are ever temporarily used for test purposes. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes, the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.	Personnel interviewed:	<Report Findings Here>		
		Documented procedures examined:	<Report Findings Here>		
19-6 Not used in EMS					
19-7 Not used in EMS					
19-8 Not used in EMS					
19-9 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
19-10 Not used in EMS					
19-11 Not used in EMS					
19-12 Not used in EMS					
	20-1 POI devices must each implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device. This means not only the account-data-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device. POI device private keys must not exist anywhere but the specific POI device they belong to, except where generated external to the POI device and prior to the injection into the POI device.		☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**20-1.a** Examine documented procedures for the loading and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**20-1.b** Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POI devices to verify that unique keys are generated and used for each POI device.	Describe how the observed HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POI devices verified that unique keys are generated and used for each POI device: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**20-1.c** Examine check values, hash, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI device vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.	Describe how the examined check values, hash, or fingerprint values for a sample of cryptographic keys from different POI devices verified that private and secret keys are unique for each POI device: <Report Findings Here>			
20-2 If a POI device directly interfaces with more than one entity for decryption of account data (e.g., different acquiring organizations), the POI device must have a completely different and unique key or set of keys for each acquirer. These different keys, or sets of keys, must be totally independent and not variants of one another.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**20-2.a** Examine documented procedures for generating all types of keys and verify procedures exist to ensure that unique keys or sets of keys are used for each acquiring organization and totally independent and are not variants of one another.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**20-2.b** Interview personnel and observe key-generation processes to verify that unique keys or sets of keys will be generated for each acquiring organization when required.	Personnel interviewed:	<Report Findings Here>		
		Describe how the key-generation processes observed verified that unique keys or sets of keys are generated for each acquiring organization: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
20-3 Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device. This requirement refers to the use of a single "base" key to derive initial keys for many different POI devices, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys once loaded—e.g., as done with DUKPT.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**20-3.a** Examine documented procedures and observe processes for generating initial keys. Verify the following is implemented where initial keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI device. • Examine key-generation/injection logs to ensure that sequential values included in unique key derivation are not repeated.	Documented procedures examined:	<Report Findings Here>		
		Key generation logs examined:	<Report Findings Here>		
		Describe how the processes observed for generating master keys verified that the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**20-3.b** Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.	Describe how the processes observed for generating master keys verified that derivation keys used to generate keys for multiple devices are never loaded into a POI device:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
20-4 Entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring organizations must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques: • Different BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model • Different BDKs by geographic region, market segment, processing platform, or sales unit COMPONENT PROVIDERS ONLY: Must use at least one unique Base Derivation Key (BDK) per acquiring organization and must be able to support segmentation of multiple BDKS of acquiring organizations.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**20-4** Examine documented key-generation and injection procedures to verify that entities processing or injecting DUKPT or other key-derivation methodologies incorporate a segmentation strategy in their environments using one or more of the following techniques: • Different BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model • Different BDKs by geographic region, market segment, processing platform, or sales unit FOR COMPONENT PROVIDERS ONLY: Examine documented key-generation and injection procedures to verify that key-injection vendors use at least one unique Base Derivation Key (BDK) per acquiring organization and are able to support segmentation of multiple BDKs of acquiring organizations.	Documented procedures examined:	<Report Findings Here>		
20-5 Not used in EMS					
20-6 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
21-1 Secret or private keys must only exist in one or more of the following forms: • At least two separate key shares (secret or private) or full-length components (secret) • Encrypted with a key of equal or greater strength as delineated in Annex C • Contained within a secure cryptographic device ***Note**: Key-injection facilities may have clear-text keying material outside of a SCD when used within a secure room in accordance with Requirement 32.* **Note for hybrid decryption solutions:** Clear-text Data Decryption Keys (DDKs) may temporarily be retained by the Host System in volatile memory for the purpose of decrypting account data.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-1.a** Examine documented procedures for key storage and usage to verify that secret or private keys only exist in one or more approved forms at all times when stored (with the exception of DDKs used on the Host System for hybrid decryption solutions).	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**21-1.b** Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored (with the exception of DDKs used on the Host System for hybrid decryption solutions).	Describe how the key stores observed verified that secret or private keys only exist in one or more approved forms at all times when stored: <Report Findings Here>			
21-2.2 Construction of the cryptographic key must require the use of at least two key components/shares.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-2.2** Observe processes for constructing cryptographic keys to verify that at least two key components/shares are required for each key construction.	Describe how the processes observed for constructing keys verified that at least two key components are required for each key construction: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
21-2.3 Each key component/share must have one or more specified authorized custodians.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-2.3.a** Examine documented procedures for the use of key components/shares and interview key custodians and key-management supervisory personnel to verify that each key component/share is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component/share.	Key-management documentation examined:	<Report Findings Here>		
		Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**21-2.3.b** Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components or shares are designated as key custodians for those particular components/shares.	Describe how the key-component access controls and key-custodian authorizations/assignments observed verified that all individuals with access to key components are designated as key custodians for those particular components:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
21-2.4 Procedures must exist to ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private key cryptographic key. For example, in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three shares are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one share. If a custodian was previously assigned share A, which was then reassigned, the custodian must not then be assigned share B or C, as this would give them knowledge of two shares, which gives them ability to recreate the key. In an m-of-n scheme where n=5, where three shares are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key shares (e.g., share A and share B); and a second custodian (with, in this example, share C) would be required to reconstruct the final key, ensuring that dual control is maintained.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-2.4.a** Examine documented procedures for the use of key components/shares to verify that procedures ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private cryptographic key.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**21-2.4.b** Examine key-component/share access controls and access logs to verify that authorized custodians cannot access sufficient key components or shares to reconstruct a secret or private cryptographic key.	Describe how the key-component access controls and access logs observed verified that authorized custodians cannot access sufficient key components or shares to reconstruct a secret or private cryptographic key: <Report Findings Here>			
21-3 Key components/shares must be stored as follows:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-3** Examine documented procedures, interview responsible personnel and inspect key-component/share storage locations to verify that key components/shares are stored as outlined in Requirements 21-3.1 through 21-3.3 below:	Documented procedures examined:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
21-3.1 Key components that exist in clear text outside of an SCD must be sealed in individual opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging. **Note**: Tamper-evident authenticable packaging—opacity may be envelopes within tamper-evident packaging— used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-3.1.a** Examine key components and storage locations to verify that components are stored in individual opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging.	Describe how the key components and storage locations observed verified that components are stored in opaque, pre-numbered tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging: <Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**21-3.1.b** Inspect any tamper-evident packaging used to secure key components—e.g., is the package sufficiently opaque to prevent reading of a component—and ensure that it prevents the determination of the key component without visible damage to the packaging.	Identify the P2PE Assessor who confirms that tamper-evident packaging prevents the determination of the key component without visible damage to the packaging:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**21-3.1.c** Ensure clear-text key components do not exist in non-secure containers, such as databases or in software programs.	Responsible personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**21-3.1.d** Confirm that start-up instructions and other notes used by service technicians do not contain initialization-key values written in the clear (e.g., at the point in the checklist where the keys are entered).	Identify the P2PE Assessor who confirms that start-up instructions and other notes used by service technicians do not contain initialization-key values written in the clear:	<Report Findings Here>		
21-3.2 Key components/shares for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.* Components/shares for a specific key that are stored in separate envelopes, but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-3.2** Inspect each key component/share storage container and verify the following: • Key components/shares for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s).	Identify the P2PE Assessor who confirms that for each key component storage container: • Key components for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s).	<Report Findings Here>		
21-3.3 If a key component/share is stored on a token, and an access code (e.g., a PIN or similar access-control mechanism) is used to access the token, only that token's owner or designated backup(s) must have possession of both the token and its access code.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**21-3.3** Interview responsible personnel and observe implemented processes to verify that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its access code.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its access code:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
21-4 Not used in EMS					
22-1 Procedures for known or suspected compromised keys must include the following:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1** Verify documented procedures exist for replacing known or suspected compromised keys that includes all of the following (22-1.1 through 22-1.5 below):	Documented procedures examined:	<Report Findings Here>		
22-1.1 Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1.1** Interview responsible personnel and observe implemented processes to verify key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised:			
		<Report Findings Here>			
22-1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1.2** Interview responsible personnel and observe implemented processes to verify that if unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that if unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
22-1.3. A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s). ***Note**: The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.* Known or suspected substitution of a secret key must result in the replacement of that key and based on an analysis of how the key was substituted, any associated key-encipherment keys that may have been compromised			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, and all the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
22-1.4 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1.4.a** Interview responsible personnel and examine documented processes to verify key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s).	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s):			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**22-1.4.b** A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	Identify the P2PE Assessor who confirms that notifications include a damage assessment including, where necessary, the engagement of outside consultants and details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
22-1.5 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: • Missing secure cryptographic devices • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • Host System tamper-detection mechanism has been activated, for hybrid decryption solutions			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-1.5** Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, at a minimum, the following events: • Missing SCDs • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • Host System tamper-detection mechanism has been activated, for hybrid decryption solutions	Responsible personnel interviewed:	<Report Findings Here>		
		Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
22-2 If attempts to load a secret key or key component into an KLD or POI device (or a Host System, for hybrid decryption solutions) fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (or Host System).			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**22-2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an KLD or POI device (or a Host System, for hybrid decryption solutions) fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (or Host System).	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the implemented processes observed verified that if attempts to load a secret key or key component into an KLD or POI device fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (or Host System):			
		<Report Findings Here>			
22-3 Not used in EMS					
22-4 Not used in EMS					
22-5 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
23-1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from account-data keys. **Note**: Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**23-1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.	Documented procedures reviewed:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**23-1.b** Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.	Describe how the processes observed verified that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
23-2 An MFK used by host processing systems for encipherment of keys for local storage—and variants of the MFK—must not be used external to the (logical) configuration that houses the MFK itself. For example, MFKs and their variants used by host processing systems for encipherment of keys for local storage must not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration. A logical configuration is defined as one where all the components form a system used to undertake a particular task and are managed and controlled under a single operational and security policy.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**23-2.a** Interview responsible personnel to determine which host MFKs keys exist as variants. ***Note**: Some HSMs may automatically generate variants or control vectors for specific keys, but it is still up to the entity to specify exact usage.*	Responsible personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**23-2.b** Examine vendor documentation to determine support for key variants.	Vendor documentation examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**23-2.c** Via examination of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used, determine that variants of the MFK are not used external to the logical configuration that houses the MFK.	Describe how the review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used verified that variants of the MFK are not used external to the logical configuration that houses the MFK: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
23-3 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys e.g., DEKs from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or working keys with different purposes from another working key. ***Note**: Using transformations of keys across different levels of a key hierarchy—e.g., generating a DEK from a key-encrypting key—increases the risk of exposure of each of those keys.* It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**23-3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys • Variants of working keys must only be calculated from other working keys.	Documented procedures examined:	<Report Findings Here>		
		Describe how the implemented processes observed verified that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys • Variants of working keys must only be calculated from other working keys.			
		<Report Findings Here>			
24-1 Instances of secret or private keys, and their key components, that are no longer used or that have been replaced by a new key must be destroyed.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**24-1.a** Verify documented procedures are in place for destroying secret or private keys, and their key components that are no longer used or that have been replaced by a new key.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**24-1.b** Identify a sample of keys and key components that are no longer used or have been replaced. For each item in the sample, interview responsible personnel and examine key-history logs and key-destruction logs to verify that all keys have been destroyed.	Sample of keys and key components that are no longer used or have been replaced reviewed:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		
		Key-history logs examined:	<Report Findings Here>		
		Key-destruction logs examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**24-1.c** Examine storage locations for the sample of destroyed keys to verify they are no longer kept.	Describe how the storage locations observed verified that the sample of destroyed keys are no longer kept:			
		<Report Findings Here>			
24-2 The procedures for destroying key components or shares that are no longer used or have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered. For written components, this must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient. **Note**: Key destruction for keys installed in HSMs and POI devices is addressed in Requirement 31.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**24-2.a** Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**24-2.b** Observe key-destruction processes to verify that no part of the key or component can be recovered.	Describe how the key-destruction processes observed verified that no part of the key or component can be recovered:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
24-2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic database backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568. For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**24-2.1.a** Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**24-2.1.b** Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or component—are destroyed following the procedures outlined in ISO–9564 or ISO–11568.	Describe how the key-destruction processes observed verified that keys on all other storage media types in all permissible forms—physically secured, enciphered, or component—are destroyed following the procedures outlined in ISO–9564 or ISO–11568: <Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
24-2.2 The key-destruction process must be observed by a third party other than the custodians of any component of that key—i.e., the third party must not be a key custodian for any part of the key being destroyed. The third-party witness must sign an affidavit of destruction, and this affidavit is retained for a minimum of two years.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**24-2.2.a** Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian for any component of that key.	Identify the P2PE Assessor who confirms the key-destruction process is witnessed by a third party other than a key custodian for any component of that key:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**24-2.2.b** Inspect key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key destruction process.	Key-destruction logs inspected:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
24-2.3 Key components for keys other than the HSM or KLD MFKs that have been successfully loaded and confirmed as operational must also be destroyed, unless the HSM does not store the encrypted values on a database but only stores the subordinate keys internal to the HSM. BDKs used in KLDs may also be stored as components where necessary to reload the KLD.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**24-2.3.a** Verify documented procedures exist for destroying key components of keys once the keys are successfully loaded and validated as operational.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**24-2.3.b** Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.	Describe how the key-conveyance/loading processes observed verified that any key components are destroyed once the keys are successfully loaded and validated as operational:			
		<Report Findings Here>			
25-1 To reduce the opportunity for key compromise, the number of key custodians must be limited to the minimum required for operational efficiency. Controls must include:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**25-1** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:	Key custodians interviewed:	<Report Findings Here>		
		Key-management supervisory personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
25-1.1 Designate key custodian(s) for each component, such that the fewest number (e.g., a primary and a backup) of key custodians are assigned as necessary to enable effective key management. Key custodians must be employees or contracted personnel.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**25-1.1.a** Examine key-custodian assignments for each component to verify that: • Key custodian(s) are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel.	Describe how the key-custodian assignments reviewed for each component verified that: • Key custodian(s) are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel. <Report Findings Here>			
25-1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**25-1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form.	Completed key-custodian forms examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**25-1.2.b** Examine completed key-custodian forms to verify that backup custodians sign the form.	Completed key-custodian forms examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
25-1.3 Each key-custodian form provides the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**25-1.3** Examine all key-custodian forms to verify that they include the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access	Completed key-custodian forms examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
25-1.4 In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual except as noted below for organizations of insufficient size. For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual. The components collectively held by an individual and his or her direct reports must not constitute a quorum (or must not provide any information about the value of the key that is not derivable from a single component). Custodians must not become a custodian for a component/share of a key where the custodian has previously been or is currently a custodian for another component/share of that key if that would collectively constitute a quorum to form the actual key. When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented. Organizations that are of insufficient size that they cannot support the reporting-structure requirement must: Ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian); Receive explicit training to instruct them from sharing key components with their direct manager; Sign key-custodian agreements that include an attestation to the requirement; and Receive training that includes procedures to report any violations.		☐	☐	☐

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**25-1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisors possess the necessary threshold of key components sufficient to form any given key. • Key custodians are not and have not been a custodian for another component/share of a key where that collectively would constitute a quorum to form the actual key.	Documented key-custodian assignments examined:	<Report Findings Here>		
		Documented organization charts examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**25-1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, ensure that documented procedures exist and are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes procedures to report any violations.	Documented procedures examined:	<Report Findings Here>		
25-2 Not used in EMS					
25-3 Not used in EMS					
25-4 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
25-5 Not used in EMS					
25-6 Not used in EMS					
25-7 Not used in EMS					
25-8 Not used in EMS					
25-9 Not used in EMS					
	26-1 Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. The logs must be securely stored, for example, in a secure container with the associated key components. These logs must be archived for a minimum of two years subsequent to key destruction. At a minimum, logs must include the following: • Date and time in/out • Key-component identifier • Purpose of access • Name and signature of custodian accessing the component • Name and signature of a non-custodian (for that component/share) witness • Tamper-evident and authenticable package number (if applicable)		☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**26-1.a** Interview responsible personnel and examine documented procedures to determine the following: • Logs are kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. • Logs are securely stored, for example, in a secure container with the associated key components. • Logs must be archived for a minimum of two years subsequent to key destruction	Personnel interviewed:	<Report Findings Here>		
		Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**26-1.b** Examine log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD	Log files examined:	<Report Findings Here>		
		Describe how log files and audit log settings verified that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**26-1.c** Examine log files to verify they are: • Archived for a minimum of two years subsequent to key destruction. • Securely stored	Log files examined:	<Report Findings Here>		
		Describe how the log files examined verified that they are archived for a minimum of two years subsequent to key destruction.			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**26-1.d** Examine log files and audit log settings to verify that logs include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Name and signature of a non-custodian (for that component/share) witness • Tamper-evident and authenticable package number (if applicable)	Log files examined:	<Report Findings Here>		
		Describe how log files and audit log settings verified that logs include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
27-1 If backup copies of secret and/or private keys exist, they must be maintained in accordance with the same requirements as are followed for the primary keys.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**27-1.a** Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following:	Responsible personnel interviewed:	<Report Findings Here>		
		Documented procedures examined:	<Report Findings Here>		
		Backup records examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**27-1.b** Observe backup processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys.	Describe how the backup processes observed verified that backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys:			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**27-1.c** Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: • Securely stored with proper access controls • Under at least dual control • Subject to at least the same level of security control as operational keys as specified in this document	Documented procedures examined:	<Report Findings Here>		
		Personnel interviewed:	<Report Findings Here>		
		OR Describe how backup storage locations verified that backups are maintained as follows: • Securely stored with proper access controls • Under at least dual control • Subject to at least the same level of security control as operational keys as specified in this document			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
27-2 If backup copies are created, the following must be in place: • Creation (including cloning) of top-level keys—e.g., MFKs—must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**27-2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the backup processes observed verified that: • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process • All requirements applicable for the original keys also apply to any backup copies of keys and their components.			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
28-1 Written procedures must exist and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as: • Training of all key custodians regarding their responsibilities, and forming part of their annual security training • Role definition—nominated individual with overall responsibility • Background checks for personnel (within the constraints of local laws) • Management of personnel changes, including revocation of access control and other privileges when personnel move			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**28-1.a** Examine documented procedures for key-administration operations to verify they cover all activities related to key administration, and include: • Training of all key custodians regarding their responsibilities, and forming part of their annual security training • Role definition—nominated individual with overall responsibility • Background checks for personnel (within the constraints of local laws) • Management of personnel changes, including revocation of access control and other privileges when personnel move	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**28-1.b** Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.	Responsible personnel interviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**28-1.c** Interview personnel to verify that security-awareness training is provided for the appropriate personnel.	Personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**28-1.d** Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).	Responsible HR personnel interviewed:	<Report Findings Here>		
28-2 Not used in EMS					
28-3 Not used in EMS					
28-4 Not used in EMS					
28-5 Not used in EMS					

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
29-1 Secure cryptographic devices—such as HSMs and POI devices—must be placed into service only if there is assurance that the equipment has not been subjected to unauthorized modifications, substitution, or tampering and has not otherwise been subject to misuse prior to deployment. **Note**: This applies to SCDs used for key injection or code signing, including display prompts.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-1.a** Examine documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-1.b** Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.	Personnel interviewed:	<Report Findings Here>		
		Identify the P2PE Assessor who confirms that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-1.1 All POI devices and other SCDs must be protected against compromise. Any compromise must be detected. Loading and use of any financial keys after the compromise must be prevented. Controls must include the following:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-1.1** Examine documented procedures to verify controls are defined to protect POI devices, and other SCDs from unauthorized access up to point of deployment.	Documented procedures reviewed:	<Report Findings Here>		
29-1.1.1 Access to all POI devices, and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection. The minimum log contents include date and time, object name/identifier, purpose, name of individual(s) involved, signature or electronic capture (e.g., badge) of individual involved, and if applicable, tamper-evident package number(s) and serial number(s) of device(s) involved. Electronic logging e.g., using bar codes is acceptable for device tracking.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-1.1.1.a** Examine access-control documentation and device configurations to verify that access to all POI devices and key injection/loading devices is defined and documented.	Access-control documentation reviewed:	<Report Findings Here>		
		Describe how access-control documentation and device configurations observed verified that access to all POI devices and key injection/loading devices is defined and documented:			
		<Report Findings Here>			
PDCP **PMCP** **EMCP** **SP**	**29-1.1.1.b** For a sample of POI device types and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POI devices and other SCDs is logged.	Sample of POI device types and other SCDs:	<Report Findings Here>		
		Access logs reviewed:	<Report Findings Here>		
		Describe how observation of authorized personnel accessing devices and access logs verified that access to all POI devices and other SCDs is logged:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**29-1.1.1.c** Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD.	Describe how the implemented access controls examined verified that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD: <Report Findings Here>			
29-1.1.2 All personnel with access to POI devices and other SCDs prior to deployment are documented in a formal list and authorized by management. A documented security policy must exist that requires the specification of personnel with authorized access to all secure cryptographic devices. This includes documentation of all personnel with access to POI devices and other SCDs as authorized by management. The list of authorized personnel is reviewed at least annually. **Note**: "Prior to deployment" for this requirement means prior to the solution provider (or component provider) sending POI devices to either a distribution channel or the end merchant who will use the POI device to process payment transactions.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-1.1.2.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POI devices and other SCDs are documented in a formal list authorized by management in an auditable manner. • The authorizations are reviewed annually.	Documented authorizations reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-1.1.2.b** For a sample of POI device types and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in an auditable manner have access to devices.	Sample of POI device types and other SCDs reviewed: Describe how the implemented access controls for the sample of POI device types and other SCDs examined verified that only personnel documented and authorized in an auditable manner have access to devices: <Report Findings Here>	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-1.2 POI devices and other SCDs must not use default keys or data (such as keys that are pre-installed for testing purposes) or passwords/authentication codes.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-1.2.a** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-1.2.b** Observe implemented processes and interview personnel to verify that default keys or passwords are not used.	Responsible personnel interviewed:	<Report Findings Here>		
29-2 Not used in EMS					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-3 Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the following: • Transportation uses a trusted courier service (e.g., via bonded carrier). The devices are then securely stored until key-insertion occurs. • Physically secure and trackable packaging (e.g., pre-serialized, counterfeit-resistant, tamper-evident packaging) is used. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs. • A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. The SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key, and the device is further protected until deployment. • Upon tamper of the device it becomes infeasible to load any keying material. • Shipped and stored containing a secret that: o Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and o Can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel. • Each cryptographic device is carefully inspected and tested immediately prior to key-insertion and deployment using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized access or modifications. ***Note**: Unauthorized access includes that by customs officials.* o Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised. *(**Note**: this control must be used in conjunction with one of the other methods.)* o Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-3.a** Examine documented procedures to verify they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**29-3.b** Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion and deployment.	Responsible personnel interviewed:	<Report Findings Here>		
29-4 Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or backup devices—throughout their lifecycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs, but cannot supplant the implementation of dual-control mechanisms.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.a** Examine documented procedures to verify that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-4.b** Interview responsible personnel and physically verify the dual-control mechanism used to prevent substitution or tampering of HSMs—both in service and spare or back-up devices—throughout their life cycle.	Identify the P2PE Assessor who physically verified the dual-control mechanism used to prevent substitution or tampering of HSMs—both in service and spare or back-up devices—throughout their life cycle:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
29-4.1 HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. **Note**: Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-4.1.b** For a sample of received devices, examine sender documentation sent by a different communication channel than the device's shipment (e.g., the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.	Sample of received devices:	<Report Findings Here>		
		Sender documentation/record of serial number validations reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-4.2 The security policy enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required to support specified functionality must be disabled before the equipment is commissioned. Documentation (e.g., a checklist or similar suitable to use as a log) of configuration settings must exist and be signed and dated by personnel responsible for the implementation. This documentation must include identifying information for the HSM, such as serial number and/or asset identifiers. This documentation must be retained and updated for each affected HSM any time changes to configuration settings would impact security.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.2.a** Obtain and examine the defined security policy to be enforced by the HSM.	Documented security policy examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-4.2.b** Examine documentation of the HSM configuration settings from past commissioning events to determine that the functions and commands enabled are in accordance with the security policy.	HSM configuration settings documentation examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-4.2.c** For a sample of HSMs, examine the configuration settings to determine that only authorized functions are enabled.	Sample of HSMs reviewed:	<Report Findings Here>		
		Describe how the HSM configuration settings observed verified that only authorized functions are enabled:			
		<Report Findings Here>			
29-4.2.d Not used in P2PE					
29-4.2.e Not used in P2PE					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
PDCP **PMCP** **EMCP** **SP**	**29-4.2.f** Examine documentation to verify: • Configuration settings are defined, signed and dated by personnel responsible for implementation. • It includes identifying information for the HSM, such as serial number and/or asset identifiers. • The documentation is retained and updated anytime configuration setting impacting security occur for each affected HSM.	Documentation examined:	<Report Findings Here>		
29-4.3 When HSMs are connected to online systems, controls are in place to prevent the use of an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. **Note**: Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.3** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.	Describe how the HSM configurations examined and processes observed verified that HSMs are not enabled in a sensitive state when connected to online systems: <Report Findings Here>			
29-4.4 Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised. Processes must include :			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.4.**Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify the integrity of the device and include requirements specified at 29-4.4.1 through 29-4.4.4 below.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-4.4.1 Running self-tests to ensure the correct operation of the device.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-.4.4.1** Examine records of device inspections and test results to verify that self-tests are run on devices to ensure the correct operation of the device.	Records of device inspections examined:	<Report Findings Here>		
		Describe how the records of device inspections and test results examined verified that self-tests are run on devices to ensure the correct operation of the device:			
		<Report Findings Here>			
29-4.4.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.4.2** Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the inspection processes observed verified that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised:			
		<Report Findings Here>			
29-4.4.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.4.3** Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how the inspection processes observed verified that processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
29-4.4.4 Maintaining records of the tests and inspections, and retaining records for at least one year.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-4.4.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.	Records of inspections examined:	<Report Findings Here>		
		Responsible personnel interviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-4.4.4.b** Examine records of inspections to verify records are retained for at least one year.	Records of inspections examined:	<Report Findings Here>		
29-5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**29-5.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**29-5.b** Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.	Sample of received devices reviewed:	<Report Findings Here>		
30-1 Not used in P2PE					
30-2 Not used in P2PE					

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
30-3 Not used in EMS					
31-1 Procedures must be in place to ensure that any SCDs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private keys, key material, and account data stored within the device irrecoverable. Processes must include the following: • Procedures require that all secret and private keys, key material, and all account data stored within the device be securely destroyed. • Procedures cover all devices removed from service permanently or for repair. • Procedures cover requirements at 31-1.1 through 31-1.6 below. **Note**: Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1** Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all secret and private keys, key material, and all account data stored within the device be securely destroyed. • Procedures cover all devices removed from service permanently or for repair. • Procedures cover requirements at 31-1.1 through 31-1.6 below.	Documented procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.1.a** Examine documented procedures for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**31-1.1.b** Interview personnel and observe demonstration (if HSM is available) of processes for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.	Personnel interviewed:	<Report Findings Here>		
		Describe how the demonstration observed verified that dual control is implemented for all critical decommissioning processes.			
		<Report Findings Here>			
31-1.2 Keys and account data are rendered irrecoverable (e.g., zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.2** Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material and account data are rendered irrecoverable (e.g., zeroized), or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.	Personnel interviewed:	<Report Findings Here>		
		Describe how the demonstration verified that all keying material and account data are rendered irrecoverable, or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
31-1.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.3** Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable.	Personnel interviewed:	<Report Findings Here>		
		Describe how the processes observed verified that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable or the devices are physically destroyed:			
		<Report Findings Here>			
31-1.4 Affected entities are notified before devices are returned.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.	Responsible personnel interviewed:	<Report Findings Here>		
		Device-return records examined:	<Report Findings Here>		
31-1.5 Devices are tracked during the return process.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.	Responsible personnel interviewed:	<Report Findings Here>		
		Device-return records examined:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
31-1.6 Records of the tests and inspections are maintained for at least one year.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**31-1.6** Interview personnel and observe records to verify that records of the tests and inspections are maintained for at least one year.	Personnel interviewed:	<Report Findings Here>		
		Records of testing examined:	<Report Findings Here>		
32-1 For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into POI devices, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.a** Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into POI devices.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**32-1.b** Verify that documented procedures cover requirements 32-1.1 through 32-1.5 below.	Documented procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
32-1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. ***Note:*** *Dual control consists of logical and/or physical characteristics.* ***For example****, dual control may be implemented for logical access via two individuals with two different passwords/authentication codes (at least five characters in length), or for physical access via a physical lock that requires two individuals each with a different high-security key.* *For devices that do not support two or more passwords/authentication codes, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian. Each half must be a minimum of five characters.* *Physical keys, authorization codes, passwords/authentication codes, or other enablers must be managed so that no one person can use both the enabler(s) and the device, which can create cryptograms of known keys or key components under a key-encipherment key used in production.*			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.1** Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.	Describe how the dual-control mechanisms and device-authorization processes observed verified that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people:			
		<Report Findings Here>			
32-1.2 Passwords/authentication codes used for dual control must each be of at least five numeric and/or alphabetic characters.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.2** Observe password policies and configuration settings to confirm that passwords/authentication codes used for dual control must be at least five numeric and/or alphabetic characters.	Password policies reviewed:	<Report Findings Here>		
		Describe how the configuration settings observed verified that passwords used for dual control must be at least five numeric and/or alphabetic characters:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
32-1.3 Dual control must be implemented for the following: • To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of clear-text key components; • For all access to key-loading devices (KLDs) and authenticated application-signing devices.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.3** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing • To enable application-signing functions • To place the device into a state that allows for the input or output of clear-text key components • For all access to KLDs and authenticated application-signing devices	Dual-control mechanisms examined:	<Report Findings Here>		
		Describe how the observation of authorized personnel performing the defined activities verified that dual control is implemented for the following: • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing • To enable application-signing functions • To place the device into a state that allows for the input or output of clear-text key components • For all access to KLDs and authenticated application-signing devices			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
32-1.4 Devices must not use default passwords.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.4.a** Examine password policies and documented procedures to confirm default passwords/authentication codes must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists.	Documented procedures and password policies reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**32-1.4.b** Observe device configurations and interview device administrators to verify that HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords /authentication codes.	Device administrators interviewed:	<Report Findings Here>		
		Describe how the device configurations observed verified that HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords:			
		<Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
32-1.5 To detect any unauthorized use, devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected. **Note**: For key-injection facilities, or applicable entities providing key-management services, POI devices may be secured by storage in the dual-control access key injection room.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**32-1.5.a** Examine and confirm documented procedures require devices are within a secure room and are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.	Documented procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**32-1.5.b** Interview responsible personnel and observe devices and processes to confirm that devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.	Responsible personnel interviewed:	<Report Findings Here>		
		Describe how devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.			
		<Report Findings Here>			
32-2 Not used in EMS					
32-3 Not used in EMS					
32-4 Not used in EMS					
32-5 Not used in EMS					
32-6 Not used in EMS					
32-7 Not used in EMS					

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
32-8 Not used in EMS					
32-9 Not used in EMS					
33-1 Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed on account-data processing devices before they are placed into service, as well as devices being decommissioned.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**33-1.a** Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for account-data processing devices placed into service, initialized, deployed, used, and decommissioned.	Documented procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**33-1.b** Verify that written records exist for the tests and inspections performed on devices before they are placed into service, as well as devices being decommissioned.	Documented records reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
5A-1.1 Only approved encryption algorithms and key sizes must be used to protect account data and cryptographic keys, as listed in Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5A-1.1.a** Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms and key sizes that are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	Documented key-management policies and procedures examined:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**5A-1.1.b** Observe key-management operations and devices to verify that all cryptographic algorithms and key sizes are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	Describe how observed key-management operations and devices verified that all cryptographic algorithms and key sizes are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
5A-1.2 Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (e.g., after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (e.g., NIST Special Publication 800-57). See Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5A-1.2.a** Examine documented key-management procedures to verify: • Crypto-periods are defined for every type of key in use. • Crypto-periods are based on industry best practices and guidelines (e.g., NIST Special Publication 800-57). • A process/methodology is in place to determine when the crypto-period is reached for each cryptographic key. • Cryptographic key changes are implemented whenever a key reaches the end of its defined crypto-period.	Documented key-management procedures reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**5A-1.2.b** Through observation of key-management operations and inspection of SCDs, verify that crypto-periods are defined for every type of key in use.	SCDs inspected:	<Report Findings Here>		
		Describe how the observed key-management operations and the inspected SCDs verified that crypto-periods are defined for every type of key in use:			
		<Report Findings Here>			

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
5A-1.3 Documentation describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution must exist and must be demonstrably in use for all key-management processes.			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.a** Verify documentation exists describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution.	Documentation reviewed:	<Report Findings Here>		
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.b** Observe architecture and key-management operations to verify that the documentation reviewed in 5A-1.3.a is demonstrably in use for all key-management processes.	Describe how architecture and key-management operations verified that the documentation reviewed in 5A-1.3.a is demonstrably in use for all key-management processes: <Report Findings Here>			

Encryption Management Services - Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions	Assessor's Findings		
			In Place	N/A	Not In Place
5A-1.3.1 Maintain documentation of all cryptographic keys managed as part of the P2PE solution, including: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.1.a** Examine key-management policies and procedures and verify documentation of all cryptographic keys managed as part of the P2PE solution is required, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method	Documented key-management policies and procedures examined:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.1.b** Observe documentation and interview personnel and confirm that documentation of all cryptographic keys managed as part of the P2PE solution exists, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method	Documentation reviewed:	<Report Findings Here>		
		Personnel interviewed:	<Report Findings Here>		
5A-1.3.2 Maintain a list of all devices used to generate keys or key components managed as part of the P2PE solution, including: • Device name/identifier • Device manufacturer/model • Type of keys generated (per 5A-1.3.1) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)			☐	☐	☐
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.2.a** Examine key-management policies and procedures and verify a list of all devices used to generate keys managed as part of the P2PE solution is required, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per 5A-1.3.1) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)	Documented key-management policies and procedures reviewed:	<Report Findings Here>		

Encryption Management Services - Reporting					
Applies to	**Requirements and Testing Procedures**	**Reporting Instructions**	**Assessor's Findings**		
			In Place	**N/A**	**Not In Place**
PDCP **PMCP** **EMCP** **SP**	**5A-1.3.2.b** Observe documentation and interview personnel and confirm that a list of all devices used to generate keys managed as part of the P2PE solution exists, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per 5A-1.3.1) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)	Documentation reviewed:	<Report Findings Here>		
		Personnel interviewed:	<Report Findings Here>		
5H-1 Not used in EMS					
5I-1 Not used in EMS					