Payment Card Industry (PCI)

Point-to-Point Encryption Decryption Management Services

Template for Report on Validation for use with P2PE v3.1 for P2PE Decryption 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 Decryption 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 DMS 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 3.10 to capture truncation information relative to requirement 4B-1.8. - 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 Decryption Management Services

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

DMS Component Assessments: Use of this Reporting Template is mandatory for all P2PE v3.1 Decryption Management Services Component Provider assessments (i.e., for a DMCP assessment).

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 Decryption Management Services requirements (i.e., when they have not completely satisfied the full scope of their decryption management services via the use of Validated Decryption 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 the submitted P-ROV(s) 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 applicable Validated P2PE 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 the 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) with 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 if any other relevant key management service that has not already been assessed as part of the inclusion of a Validated P2PE Component Provider and/or as part of the Domain 1 and Domain 4 assessment scope of the 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 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 Decryption Management Services Template for the P2PE v3.1 Standard

The 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 a DMS Component assessment?	☐ Solution	If **Solution**, enter the Solution Name: (*Complete this P-ROV with the Solution P-ROV*)	
	☐ DMS Component	If **DMS Component**, complete the *P2PE Component Details* below.	
P2PE Component Details (*for DMS Component assessments ONLY*)			
P2PE Component Name:		Is the Component currently (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 Component Type for this assessment:	☐ Decryption Management Component Provider (DMCP)		

2.2 Validated P2PE Component Providers

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

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

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 DMCP cannot be used to satisfy the requirements of a DMCP 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.*

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

Are Validated P2PE Component Providers being used to help satisfy requirements in scope for 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 #**
DMCP	**KIF**	**KMCP**	**KLCP**	**CA/RA**			
N/A	☐	☐	☐	☐			
N/A	☐	☐	☐	☐			
N/A	☐	☐	☐	☐			
N/A	☐	☐	☐	☐			

Validated P2PE Component Providers Continued
Describe how the Validated P2PE Component Provider(s) are being used to satisfy applicable P2PE requirements for this Decryption 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 DMCP*". Do **not** leave this blank unless ***No*** was checked above.
<Description>

2.3 Third-Party Entities Involved in the Decryption 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***) Decryption Management Services here. It is not necessary to duplicate this information in the Solution P-ROV.

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

Are Third Party entities involved in the scope of Decryption 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 (Table not currently used)

2.5 (Table not currently used)

2.6 Secure Cryptographic Devices (SCDs)

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

This includes all SCDs that apply to the P2PE requirements relative to this assessment. E.g., SCDs used in the decryption environment to decrypt account data, to generate, load, encrypt, or transfer cryptographic keys. Examples include HSMs, key-injection/loading devices (KLDs), etc.

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

DMS COMPONENT ASSESSMENTS: Complete this table as applicable.

Insert additional rows as necessary.

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

2.7 (Table not currently used)

2.8 Summary of P2PE Assessment Compliance Status		
Type of P2PE Assessment	**Compliant**	**Comments (*optional*)**
Decryption Management Services ***Note:*** *This table must correlate correctly with Table 2.1 for the assessment type. Refer to the "P2PE Applicability of Requirements" in the P2PE Program Guide.* Mark **Yes** or **No**, as applicable to the assessment type and the overall findings, and mark **N/A** for all other assessment types.		
Solution Provider (*or MMS as a Solution Provider*)	☐ Yes ☐ No ☐ N/A	
Decryption Management Component Provider (DMCP)	☐ 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 Decryption 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 Decryption Management Services. **DMS 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 Decryption Management Services:

3.2 Decryption Management Services Diagram

Provide one or more ***high-level*** diagrams to illustrate the function of the Decryption Management Services, including:

- Locations of critical facilities
- Location of systems performing decryption management functions
- Other necessary components, as applicable to the Decryption 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 Decryption Management Services diagram(s) here>

3.3 Overview of P2PE Decryption Management Services Data Flow

Provide a ***high-level*** data-flow diagram of the Decryption Management Services that illustrates:

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

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

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

<Insert Decryption Management Services Data Flow diagram(s) here>

3.4 Key-management Processes

Provide one or more ***high-level*** diagrams showing all key-management processes, including:

- Key Generation
- Key Distribution / Loading / Injection activities
- Key Storage
- Key Usage
- Key Archiving (if applicable)
- Any other relevant information

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

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

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

3.5 Facilities

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

All documentation reviewed for this P2PE Assessment (*insert additional rows as necessary*)

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 Devices Sampled for P2PE Assessment

Complete for all sampled devices in the P2PE assessment, including every SCD type at Section 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.

Note: *All HSMs (or Host Systems used in hybrid decryption) used for account-data decryption in the decryption environment must be reviewed to verify their secure configuration and therefore cannot be sampled. Refer to the P2PE Standard for additional information.*

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 Decryption 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, ECC, 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:	

3.10 Truncation Formats

List each truncation format supported by the Application

This table must align with the findings for requirement 4B-1.8.

PAN Length *(e.g., 16* **digits***)*	**BIN Length** *(e.g., 8 digits)*	**Which digits are retained?** *(e.g., First 6, Last 4)*	**Payment Brand**	**Is the truncated PAN created by the Application or received via an input to the Application (e.g., from the POI device's firmware)?**

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 listings.*

Decryption Management Services – Summary of Findings

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

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
DOMAIN 4				
4A	**Use approved decryption devices.**			
4A-1	*Use approved decryption devices.*	☐	☐	☐
4B	**Secure the decryption environment.**			
4B-1	*Maintain processes for securely managing the decryption environment.*	☐	☐	☐
4C	**Monitor the decryption environment and respond to incidents.**			
4C-1	*Perform logging and monitor the decryption environment for suspicious activity and implement notification processes.*	☐	☐	☐
4D	**Implement secure, hybrid decryption processes. (*Applicable to Hybrid Decryption Environments ONLY*)**			
4D-1	*Configure the Host System securely.*	☐	☐	☐
4D-2	*Access controls for the Host System are configured securely.*	☐	☐	☐
4D-3	*Non-console access to the Host System is configured securely.*	☐	☐	☐
4D-4	*The physical environment of the Host System is secured.*	☐	☐	☐
4E-1	**For component providers of decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.**			

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
4E-1	*For component providers of decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.*	☐	☐	☐
DOMAIN 5				
1	**Account data is processed using equipment and methodologies that ensure they are kept secure**			
1	*Account data is processed in equipment that conforms to requirements for secure cryptographic devices (SCDs). Account data never appears in the clear outside of an SCD.*	☐	☐	☐
Requirements 2, 3 and 4 are not used in P2PE.				
	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	*All keys, key components, and key shares are generated using an approved random or pseudo-random function.*	☐	☐	☐
6	*Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*	☐	☐	☐
7	*Documented procedures must exist and must be demonstrably in use for all key-generation processes.*	☐	☐	☐
	Keys are conveyed or transmitted in a secure manner			
8	*Secret or private keys must be transferred by:* *a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or* *b. Transmitting the key in ciphertext form.* *Public keys must be conveyed in a manner that protects their integrity and authenticity.* *It is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport.*	☐	☐	☐

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
9	*During its transmission, conveyance, or movement between any two locations or organizational entities, any single unencrypted secret or private key component or share must at all times be protected.* *Sending and receiving locations/entities are equally responsible for the physical protection of the materials involved.* *These requirements also apply to keys moved between locations of the same organization.*	☐	☐	☐
10	*All key-encryption keys used to transmit or convey other cryptographic keys must be at least as strong as any key transmitted or conveyed.*	☐	☐	☐
11	*Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.*	☐	☐	☐
	Key loading to HSMs and POI devices is handled in a secure manner			
12	*Secret and private keys must be input into hardware (host) security modules (HSMs) and Point of Interaction (POI) devices in a secure manner:* *a. Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.* *b. Key-establishment techniques using public-key cryptography must be implemented securely.*	☐	☐	☐
13	*The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	☐	☐	☐
14	*All hardware and access/authentication mechanisms (e.g., passwords/authentication codes) used for key loading or the signing of authenticated applications (e.g., for "whitelists") must be managed under dual control.*	☐	☐	☐
15	*The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	☐	☐	☐
16	*Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*	☐	☐	☐
	Keys are used in a manner that prevents or detects their unauthorized usage			
17	*Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems of two organizations or logically separate systems within the same organization.*	☐	☐	☐

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
18	*Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	☐	☐	☐
19	*Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	☐	☐	☐
20	*All secret and private cryptographic keys ever present and used for any function (e.g., key encipherment or account-data encipherment) by a POI device that processes account data must be unique (except by chance) to that device.*	☐	☐	☐
21	*Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	☐	☐	☐
22	*Procedures must exist and must be demonstrably in use to replace any key determined to be compromised, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to values not feasibly related to the original keys.*	☐	☐	☐
23	*Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.* *Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.* *Keys generated with a non-reversible process, such as key derivation or transformation process with a base key using an encipherment process, are not subject to these requirements*	☐	☐	☐
24	*Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*	☐	☐	☐
25	*Access to secret and private cryptographic keys and key material must be:* *a. Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and* *b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*	☐	☐	☐
26	*Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.*			

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
27	*Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.* *Note: It is not a requirement to have backup copies of key components or keys.*	☐	☐	☐
28	*Documented procedures must exist and must be demonstrably in use for all key-administration operations.*	☐	☐	☐
	Equipment used to process account data and keys is managed in a secure manner			
29	*Equipment used to protect account data (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*	☐	☐	☐
Requirements 30-1 and 30-2 are not used in P2PE **Requirement 30-3 is not used in DMS**			☒	
31	*Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*	☐	☐	☐
Requirements 32-1 – 32-9 are not used in DMS.			☒	
33	*Documented procedures must exist and be demonstrably in use to ensure the security and integrity of account-data processing equipment (e.g., POI devices and HSMs) placed into service, initialized, deployed, used, and decommissioned.*	☐	☐	☐
5A-1	**Account data is processed using algorithms and methodologies that ensure they are kept secure**			
5A-1	*Account data is protected with appropriate cryptographic algorithms, key sizes and strengths, and key-management processes.*	☐	☐	☐
5H	**For hybrid decryption solutions: Implement secure hybrid-key management. (*Applicable to Hybrid Decryption Environments ONLY*)**			

Decryption Management Services: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
5H-1	*Hybrid decryption solutions securely manage the Data decryption Keys (DDKs) that decrypt account data in software on a Host System.*	☐	☐	☐
5I	**Component providers *ONLY*: Report status to solution providers.**			
5I-1	*For component providers performing key management in conjunction with device-management or decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.*	☐	☐	☐

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

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
DOMAIN 4				
4A-1.1 All hardware security modules (*HSMs*) must be either: • FIPS140-2 or 140-3 Level 3 (overall) or higher certified, or • PCI PTS HSM approved.		☐	☐	☐
4A-1.1.a For all HSMs used in the decryption environment, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all *HSMs* used in the solution are either: • Listed on the *NIST Cryptographic Module Validation Program (CMVP)* list, with a valid listing number, and approved to FIPS 140-2 or 140-3 Level 3 (overall), or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid PCI SSC listing number, as Approved PCI PTS Devices under the approval class "HSM."	Approval documentation reviewed:	*<Report Findings Here>*		
4A-1.1.b Examine documented procedures and interview personnel to verify that all account-data decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified in 4A-1.1.a.	Documented procedures reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4A-1.1.1 The approval listing must match the deployed devices in the following characteristics: • Vendor name • Model name and number • Hardware version number • Device firmware version number • For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment ***Note:*** *If the solution provider has applied a vendor security patch resulting in an updated HSM firmware version, and the PCI SSC or NIST validation of that updated firmware version has not yet been completed (resulting in a mismatch between the HSM firmware version in use and the listed, validated one), the solution provider must obtain documentation from the vendor regarding the update that includes confirmation the update has been submitted for evaluation per the process specified by either PCI SSC or NIST (as applicable to the HSM).*		☐	☐	☐
4A-1.1.1.a For all PCI-approved HSMs used in the solution, examine HSM devices and review the PCI SSC list of Approved 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 • Device firmware version number • Any applications, including application version number, resident within the device which were included in the PTS assessment	For each PCI-approved HSM used in the solution, describe how the HSM device configurations observed verified that all of the device characteristics at 4A-1.1.1.a match the PTS listing: *<Report Findings Here>*			
4A-1.1.1.b For all FIPS-approved HSMs used in the solution, 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	For each FIPS-approved HSM used in the solution, describe how the HSM device configurations observed verified that all of the device characteristics at 4A-1.1.1.b match the FIPS140-2 or 140-3 Level 3 (or higher) approval listing: *<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4A-1.1.1.c If the solution provider has applied a vendor security patch that resulted in an updated HSM firmware version, and the PCI SSC or NIST validation of that updated firmware version has not yet been completed, obtain the vendor documentation and verify it includes confirmation that the update has been submitted for evaluation per the process specified by PCI SSC or NIST (as applicable to the HSM).	Vendor documentation reviewed:	*<Report Findings Here>*		
4A-1.1.2 If FIPS-approved HSMs are used, the HSM must use the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes. Note: Solution providers operating HSMs in non-FIPS mode or adding non-FIPS validated software must complete a written confirmation that includes the following: • *Description of why the HSM is operated in non-FIPS mode* • *Purpose and description of any non-FIPS validated software added to the HSM* • *A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements* • Note that adding any software may invalidate the FIPS approval.		☐	☐	☐
4A-1.1.2.a Examine FIPS approval documentation (security policy) and HSM operational procedures to verify that the FIPS approval covers the cryptographic primitives, data-protection mechanisms, and key-management used for account data decryption and related processes.	FIPS approval documentation reviewed:	*<Report Findings Here>*		
	HSM operational procedures reviewed:	*<Report Findings Here>*		
4A-1.1.2.b If the HSM is operated in non-FIPS mode or non-FIPS validated software has been added to the HSM, review the solution provider's written confirmation and confirm that it includes the following: • Description of why the HSM is operated in non-FIPS mode • Purpose and description of any non-FIPs validated software added to the HSM • A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements	Solution provider's written confirmation reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4A-1.1.3 If PCI PTS-approved HSMs are used, the HSM must be configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all P2PE operations (including algorithms, data protection, key management, etc.). ***Note:*** *PCI HSMs require that the decryption-device manufacturer make available a security policy document to end users, providing information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.*		☐	☐	☐
4A-1.1.3 Examine HSM configurations for all P2PE solution functions to verify that HSMs are configured to operate according to the security policy that was included as part of the PTS approval.	Describe how HSM configurations for all P2PE security functions verified that HSMs are configured to operate according to the security policy that was included as part of the PTS approval:			
	<Report Findings Here>			
4B-1.1 Current documentation must be maintained that describes or illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.		☐	☐	☐
4B-1.1.a Review documentation to verify that a procedure exists to maintain a document that describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.	Documented procedure reviewed:	*<Report Findings Here>*		
4B-1.1.b Interview responsible personnel and review solution-provider documentation to verify that it describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Solution-provider documentation reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.2 Procedures must be implemented to provide secure administration of decryption devices by authorized personnel, including but not limited to: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of user interface • Password/smart card management • Console and non-console administration • Access to physical keys • Use of HSM commands		☐	☐	☐
4B-1.2.a Examine documented procedures to verify secure administration by authorized personnel is defined for decryption devices including: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands	Documented procedures reviewed:	*<Report Findings Here>*		
4B-1.2.b Observe authorized personnel performing device-administration operations to verify secure administration procedures are implemented for the following: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands	Describe how the observation verified that secure administration procedures are implemented for the following: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands			
	<Report Findings Here>			
4B-1.2.c Observe personnel performing decryption-device administration and examine files/records that assign administrative roles and responsibilities to verify that only authorized and assigned personnel perform decryption-device administration operations.	Files/records examined:	*<Report Findings Here>*		
	Describe how the observation verified that only authorized and assigned personnel perform decryption-device administration operations:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.3 Only authorized users/processes have the ability to make function calls to the HSM—e.g., via the HSM's application program interfaces (APIs). *For example, require authentication for use of the HSMs APIs and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate use of the API, limit the exposure of the HSM to a trusted host via a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (e.g., high-speed serial or dedicated Ethernet).*		☐	☐	☐
4B-1.3.a Examine documented procedures and processes to verify that only authorized users/processes have the ability to make functions calls to the HSM—e.g., via the HSM's application program interfaces (APIs).	Documented procedures and processes reviewed:	*<Report Findings Here>*		
4B-1.3.b Interview responsible personnel and observe HSM system configurations and processes to verify that only authorized users/processes have the ability to make function calls to the HSM (e.g., via the HSM's application program interfaces (APIs)).	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe how the observed HSM configurations and processes verified that only authorized users/processes have the ability to make function calls to the HSM:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.4 POI devices must be authenticated by the decryption environment and upon request by the solution provider. ***Note:*** *This authentication can occur via use of cryptographic keys or certificates, uniquely associated with each POI device and decryption system. The intent is to ensure the decryption environment can authenticate each unique POI device within a P2PE solution communicating with it.*		☐	☐	☐
4B-1.4.a Examine documented policies and procedures to verify they require POI devices be authenticated upon connection to the decryption environment and upon request by the solution provider.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4B-1.4.b Verify documented procedures are defined for the following: • Procedures and/or mechanisms for authenticating POI devices upon connection to the decryption environment • Procedures and/or mechanisms for authenticating POI devices upon request by the solution provider	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4B-1.4.c Interview responsible personnel and observe a sample of device authentications to verify the following: • POI devices are authenticated upon connection to the decryption environment. • POI devices are authenticated upon request by the solution provider.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe how sample device authentications verified that POI devices are authenticated upon connection to the decryption environment and upon request by the solution provider:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.5 Inspections of decryption devices by authorized personnel must be performed at least quarterly to detect tampering or modification of devices. Inspections to include: • The device itself • Cabling/connection points • Physically connected devices		☐	☐	☐
4B-1.5.a Examine documented procedure to verify that inspection of devices is required at least quarterly to detect signs of tampering or modification, and that inspection procedures include: • The device itself • Cabling/connection points • Physically connected devices	Documented procedures reviewed:	*<Report Findings Here>*		
4B-1.5.b Interview personnel performing inspections and observe inspection processes to verify that inspections include: • The device itself • Cabling/connection points • Physically connected devices	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the inspection processes observed verified that inspections include the device itself, cabling/connection points, and physically connected devices:			
	<Report Findings Here>			
4B-1.5.c Interview personnel performing inspections and review supporting documentation to verify that inspections are performed at least quarterly.	Personnel performing inspections interviewed:	*<Report Findings Here>*		
	Supporting documentation reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.6 Decryption environment must be secured according to PCI DSS. ***Note:*** *For merchant-managed solutions, PCI DSS validation of the decryption environment is managed by the merchant in accordance with their acquirer and/or payment brand. This requirement is therefore not applicable to P2PE assessments where merchants are the P2PE solution provider.* ***Note:*** *The QSA (P2PE) should NOT challenge or re-evaluate the PCI DSS environment (or its compliance) where a completed and current ROC exists.*		☐	☐	☐
4B-1.6.a Review the "Description of Scope of Work and Approach Taken" section of the solution provider's current PCI DSS Report on Compliance (ROC) to verify the PCI DSS assessment scope fully covers the P2PE decryption environment.	PCI DSS Report on Compliance (ROC) reviewed:	*<Report Findings Here>*		
4B-1.6.b Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that all applicable PCI DSS requirements are "in place" for the P2PE decryption environment.	PCI DSS Report on Compliance (ROC) and/or Attestation of Compliance (AOC) reviewed:	*<Report Findings Here>*		
4B-1.6.c Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that the PCI DSS assessment of the P2PE decryption environment was: • Performed by a QSA • Performed within the previous 12 months	PCI DSS Report on Compliance (ROC) and/or Attestation of Compliance (AOC) reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.7 Processes are implemented to ensure that clear-text account data is never sent back to the encryption environment. ***Note:*** *Output of clear-text data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process when it occurs from the decryption environment is assessed at Requirement 4B-1.9.*		☐	☐	☐
4B-1.7.a Review documented processes and interview personnel to confirm that clear-text account data is never sent back to the encryption environment.	Documented processes reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
4B-1.7.b Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends clear-text account data back into the encryption environment.	Describe how process flows and data flows verified that there is no process, application, or other mechanism that sends clear-text account data back into the encryption environment:			
	<Report Findings Here>			
4B-1.8 Any truncated PANs sent back to the encryption environment must adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs that specify allowable digits.		☐	☐	☐
4B-1.8.a Review documented processes and interview personnel to confirm that any truncated PANs sent back to the encryption environment adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs.	Documented processes reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
4B-1.8.b Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends more digits of truncated PANs back to the encryption environment than is specified in PCI DSS and/or related FAQs.	Describe how process flows and data flows verified that there is no process, application, or other mechanism that sends more digits of truncated PANs back to the encryption environment than is specified in PCI DSS and/or related FAQs:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.9 Any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must ensure that the ONLY allowed output of clear-text account data is for non-PCI payment brand account/card data, and includes the following: • Cryptographic signing (or similar) prior to installation by authorized personnel using dual control • Cryptographic authentication by the HSM • 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** – **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		☐	☐	☐
4B-1.9 Any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must ensure that the ONLY allowed output of clear-text account data is for non-PCI payment brand account/card data.	Indicate whether any whitelisting functionality has been implemented within the decryption environment (yes/no).	*<Report Findings Here>*		
If "no", describe how it was verified that no whitelisting functionality has been implemented within the decryption environment. (Leave 4B-1.9.1a to 4B-1.9.3 blank)		*<Report Findings Here>*		
If "yes", complete 4B-1.9.1.a to 4B-1.9.3:				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.9 Review documented policies and procedures to verify that that any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment ensures that the ONLY allowed output of clear-text account data is for non-PCI payment brand account/card data, and includes the following: • Cryptographic signing (or similar) prior to installation by authorized personnel using dual control. • Cryptographic authentication by the HSM • 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 – 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	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4B-1.9.1 Any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must allow ONLY the output of clear-text account data for non-PCI payment brand account/card data.		☐	☐	☐
4B-1.9.1.a Observe application and system configurations and interview personnel to verify that whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment only allows the output of clear-text account data for non-PCI payment brand account/card data.	Personnel interviewed	*<Report Findings Here>*		
	Describe how application and system configurations observed verified that whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment only allows the output of clear-text account data for non-PCI payment brand account/card data:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.9.1.b Perform test transactions to verify that any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment only allows output clear-text account for non-PCI payment brand account/card data.	Describe how test transactions verified that any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment only allows output clear-text account for non-PCI payment brand account/card data:			
	<Report Findings Here>			
4B-1.9.2 Any new installations of, or updates to, whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must be: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM		☐	☐	☐
4B-1.9.2 Observe the process for new installations or updates to whitelisting functionality and interview personnel to verify that additions or updates to whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment are performed as follows: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the observed process verified that additions or updates to whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment are performed as follows: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4B-1.9.3 Any new installations of, or updates to, whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must follow change-control procedures that include: • Coverage for both new installations and updates to such functionality • Description and justification for the functionality • 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.		☐	☐	☐
4B-1.9.3 Review records of both new and updated whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment, and confirm the following: • Both new installations and updates to whitelisting functionality are documented. • The documentation includes description and justification. • The documentation includes who approved it prior to implementation. • The documentation includes confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.	Records of new whitelisting functionality reviewed:	*<Report Findings Here>*		
	Records of updated whitelisting functionality reviewed:	*<Report Findings Here>*		
4C-1.1 Changes to the critical functions of the decryption devices must be logged. Logs must be kept, at a minimum, for a year. ***Note:*** *Critical functions include but are not limited to application and firmware updates, key-injection, as well as changes to security-sensitive configurations.*		☐	☐	☐
4C-1.1 Examine system configurations and correlating log files to verify that any changes to the critical functions of decryption devices are logged, including: • Changes to the applications • Changes to the firmware • Changes to any security-sensitive configurations	Describe how system configurations and correlating log files verified that any changes to the critical functions of decryption devices are logged, including: • Changes to the applications • Changes to the firmware • Changes to any security-sensitive configurations			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.2 Mechanisms must be implemented to detect and respond to suspicious activity, including but not limited to: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API		☐	☐	☐
4C-1.2.a Examine documented procedures to verify mechanisms are defined to detect and respond to potential security incidents, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.2.b Interview personnel and observe implemented mechanisms to verify mechanisms are implemented to detect and respond to suspicious activity, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (configuration, access controls) • Unauthorized use of sensitive functions (e.g., key management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API	Personnel interviewed:	*<Report Findings Here>*		
	Describe the implemented mechanisms that were observed to be implemented to detect and respond to suspicious activity:			
	<Report Findings Here>			
4C-1.3 Mechanisms must be implemented to detect encryption failures, including at least the following: ***Note:*** *Although Domain 4 is concerned with the decryption environment, not the encryption environment, all traffic received into the decryption environment must be actively monitored to confirm that the POI devices in the merchant's encryption environment is not outputting clear-text account data through some error or misconfiguration.*		☐	☐	☐
4C-1.3 Examine documented procedures to verify controls are defined for the following: • Procedures are defined to detect encryption failures, and include 4C-1.3.1 through 4C-1.3.4 below. • Procedures include immediate notification upon detection of a cryptographic failure, for each 4C-1.3.1 through 4C-1.3.4 below.	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.3.1 Checking for incoming clear-text account data.		☐	☐	☐
4C-1.3.1.a Observe implemented processes to verify controls are in place to check for incoming clear-text account data.	Describe how the implemented processes observed verified that controls are in place to check for incoming clear-text account data:			
	<Report Findings Here>			
4C-1.3.1.b Observe implemented controls and notification mechanisms to verify mechanisms detect and provide immediate notification upon detection of incoming clear-text account data.	Describe the implemented controls and notification mechanisms observed that detect and provide immediate notification upon detection of incoming clear-text account data:			
	<Report Findings Here>			
4C-1.3.1.c Interview personnel to verify that designated personnel are immediately notified upon detection of incoming clear-text account data.	Personnel interviewed:	*<Report Findings Here>*		
4C-1.3.2 Detecting and reviewing any cryptographic errors reported by the HSM		☐	☐	☐
4C-1.3.2.a Observe implemented processes to verify controls are in place to detect and review any cryptographic errors reported by the HSM.	Describe how the implemented processes observed verified that controls are in place to detect and review and cryptographic errors reported by the HSM:			
	<Report Findings Here>			
4C-1.3.2.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification of cryptographic errors reported by the HSM.	Describe the implemented controls and notification mechanisms observed that detect and provide immediate notification of cryptographic errors reported by the HSM:			
	<Report Findings Here>			
4C-1.3.2.c Interview personnel to verify that designated personnel are immediately notified upon detection of cryptographic errors reported by the HSM.	Personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.3.3 Detecting and reviewing any unexpected transaction data received. *For example, transaction data received without an expected authentication data block (such as a MAC or signature, or a malformed message).*		☐	☐	☐
4C-1.3.3.a Observe implemented processes to verify controls are in place to detect and review any unexpected transaction data received.	Describe how the implemented processes observed verified that controls are in place to detect and review any unexpected transaction data received: *<Report Findings Here>*			
4C-1.3.3.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification for any unexpected transaction data received.	Describe the implemented controls and notification mechanisms observed that detect and provide immediate notification for any unexpected transaction data received: *<Report Findings Here>*			
4C-1.3.3.c Interview personnel to verify that designated personnel are immediately notified upon detection of any unexpected transaction data received.	Personnel interviewed:	*<Report Findings Here>*		
4C-1.3.4 Reviewing data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.		☐	☐	☐
4C-1.3.4.a Observe implemented processes to verify controls are in place to review data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.	Describe how the implemented processes observed verified that controls are in place to review data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections: *<Report Findings Here>*			
4C-1.3.4.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification upon detection of POI devices that are causing an unusually high rate of transaction authorization rejections.	Describe the implemented controls and notification mechanisms observed that detect and provide immediate notification upon detection of POI devices that are causing an unusually high rate of transaction authorization rejections: *<Report Findings Here>*			
4C-1.3.4.c Interview personnel to verify that designated personnel are immediately notified upon detection of POI devices that are causing an unusually high rate of transaction authorization rejections.	Personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.4 All suspicious activity must be identified and a record maintained, at a minimum, for a year, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during any identified time that encryption was malfunctioning or disabled		☐	☐	☐
4C-1.4.a Examine documented procedures to verify they include procedures for identifying the source and maintaining a record, of all suspicious activity, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.4.b Observe implemented controls and interview responsible personnel to verify that the source of any suspicious activity is identified, and records are maintained to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, and specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe how the implemented controls verified that the source of any suspicious activity is identified, and records are maintained to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, and specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4C-1.5 Implement mechanisms to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).		☐	☐	☐
4C-1.5.a Examine documented procedures to verify mechanisms are defined to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).	Documented procedures reviewed:	*<Report Findings Here>*		
4C-1.5.b Interview personnel and observe implemented mechanisms to verify that immediate notification of suspicious activity is provided to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the implemented mechanisms observed verified that immediate notification of suspicious activity is provided to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers):			
	<Report Findings Here>			
Hybrid Decryption Environments (where HSMs are required for cryptographic key-management functions but allow for non-SCD "Host Systems" to be used for account-data decryption) must meet the additional requirements specified in 4D and 5H. Refer to the P2PE Standard, P2PE Program Guide, and the P2PE Glossary for additional details.				
Does this assessment meet the definition of a Hybrid Decryption Environment and therefore include the use of a Host System(s), Yes or No?	☐ **Yes**, *this **IS** a Hybrid Decryption Environment (**Complete all of 4D and 5H**)* ☐ **No**, *this is **NOT** a Hybrid Decryption Environment (Either leave 4D and 5H blank, or denote something commensurate with "N/A – No Host Systems in Use".*			
Document how you determined whether or not non-SCD Host-System(s) are being used for the decryption of account data.	*<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1 Configure the Host System securely.				
4D-1.1 The solution provider must maintain current documentation that describes, or illustrates, the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.		☐	☐	☐
4D-1.1.a Interview responsible personnel and review documentation to verify that a procedure exists to maintain a document that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Documented procedure reviewed:	*<Report Findings Here>*		
4D-1.1.b Interview responsible personnel and review solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems within that environment, to verify that the document is current.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Solution provider documentation reviewed:	*<Report Findings Here>*		
4D-1.1.c Review the solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems, to verify that it accurately represents the decryption environment.	Solution provider documentation reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.2 The Host System must be isolated, or dedicated, to processing payment transactions, with only necessary services, protocols, daemons etc. enabled: • The necessary services, protocols, daemons etc. must be documented and justified, including description of the enabled security features for these services etc. • Functions not related to transaction processing must be disabled, or isolated (e.g., using logical partitions), from transaction processing. ***Note:*** *"Isolated" means that the Host System must not be accessed, modified or intercepted by other processes.*		☐	☐	☐
4D-1.2.a Inspect network and system configuration settings to verify the host processing system is isolated, or dedicated, to processing payment transactions, with only necessary services, protocols, daemons, etc. enabled.	Describe how network and system configuration settings verified that the host processing system is isolated, or dedicated, to processing payment transactions, with only necessary services, protocols, daemons, etc. enabled: *<Report Findings Here>*			
4D-1.2.b Review the documented record of services, protocols, daemons etc. that are required by the Host System and verify that each service includes justification and a description of the enabled security feature.	Documented record of services, protocols, daemons required by the Host System reviewed:	*<Report Findings Here>*		
4D-1.3 The Host System and HSM must reside on a network that is dedicated to decryption operations and transaction processing and must be segmented from any other network, or system, that is not performing or supporting decryption operations or transaction processing.		☐	☐	☐
4D-1.3.a Examine network diagram(s) to verify the Host System(s) and HSM(s) are located on a network that is segmented from other networks that are not required for decryption operations or transaction processing.	Network diagram(s) reviewed:	*<Report Findings Here>*		
4D-1.3.b Inspect network and system configurations to verify the Host System(s) and HSM(s) are located on a network that is segmented from other networks not required for decryption operations or transaction processing.	Describe how network and system configuration settings verified that the Host System(s) and HSM(s) are located on a network that is segmented from other networks not required for decryption operations or transaction processing: *<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.4 All application software installed on the Host System must be authorized and have a business justification.		☐	☐	☐
4D-1.4.a Examine documented policies and procedures to verify that all application software installed on the Host System must have a business justification and be duly authorized.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-1.4.b Examine change control and system configuration records to verify that all application software installed on the Host System is authorized.	Change control and system configuration records reviewed:	*<Report Findings Here>*		
4D-1.4.c Inspect Host System and compare with system configuration standards to verify that all software installed on the Host System has a defined business justification.	Describe how the Host System and system configuration standards verified that all software installed on the Host System has a defined business justification:			
	<Report Findings Here>			
4D-1.5 A process, either automated or manual, must be in place to prevent and/or detect and alert, any unauthorized changes to applications/software on the Host System.		☐	☐	☐
4D-1.5.a Examine documented policies and procedures to verify that a process is defined to prevent and/or detect and alert, any unauthorized changes to applications/software.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-1.5.b Interview personnel and observe system configurations to verify that controls are implemented to prevent and/or detect and alert personnel, upon any unauthorized changes to applications/software.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the system configurations observed verified that controls are implemented to prevent and/or detect and alert personnel, upon any unauthorized changes to applications/software:			
	<Report Findings Here>			
4D-1.5.c Examine output from the implemented process to verify that any unauthorized changes to applications/software are either prevented or detected with an alert generated that is immediately investigated.	Describe how the output from the implemented process verified that any unauthorized changes to applications/software are either prevented or detected with an alert generated that is immediately investigated:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.6 The Host System must perform a self-test when it is powered up to ensure its integrity before use. The self-test must include: • Testing integrity of cryptographic functions. • Testing integrity of firmware. • Testing integrity of any security functions critical to the secure operation of the Host System.		☐	☐	☐
4D-1.6.a Inspect Host System configuration settings, and examine vendor/solution provider documentation to verify that the Host System performs a self-test when it is powered up to ensure its integrity before use. Verify the self-test includes the following: • Testing integrity of cryptographic functions • Testing integrity of software/firmware • Testing integrity of any security functions critical to the secure operation of the Host System	Vendor/solution provider documentation reviewed:	*<Report Findings Here>*		
	Describe how Host System configuration settings and vendor/solution provider documentation verified that the Host System performs a self-test when it is powered up to ensure its integrity before use, and that the self-test includes the following: • Testing integrity of cryptographic functions • Testing integrity of software/firmware • Testing integrity of any security functions critical to the secure operation of the Host System			
	<Report Findings Here>			
4D-1.6.b Review logs/audit trails from when the Host System has previously been powered-up and interview personnel to verify that the Host System performs a self-test to ensure its integrity before use. Verify the self-tests included the tests described in 4D-1.6.a.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how logs/audit trails verified that the Host System performs a self-test to ensure its integrity before use and that the self-tests included the tests described in 4D-1.6.a:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.7 The Host System must perform a self-test when a security-impacting function or operation is modified (e.g., an integrity check of the software/firmware must be performed upon loading of a software/firmware update).		☐	☐	☐
4D-1.7.a Inspect Host System configuration settings and examine vendor/solution provider documentation to verify that the Host system performs a self-test when a security-impacting function or operation is modified.	Vendor/solution provider documentation reviewed:	*<Report Findings Here>*		
	Describe how Host System configuration settings and vendor/solution provider documentation verified that the Host system performs a self-test when a security-impacting function or operation is modified:			
	<Report Findings Here>			
4D-1.7.b Interview personnel and examine logs/records for when a security-impacting function, or operation, has been modified to verify that the Host System performs a self-test.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how logs/records verified that the Host System performs a self-test when a security-impacting function or operation is modified:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.8 The Host System must enter an error state and generate an alert upon any of the following events: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements 4D-1.6 and 4D-1.7 • Failure of a security function or mechanism ***Note:*** *An "error state" identifies the Host System has encountered an issue that requires a response action. To prevent potential damage or compromise, the system must cease cryptographic operations until the issue is resolved and the host is returned to a normal processing state.*		☐	☐	☐
4D-1.8.a Inspect Host System configuration settings and examine vendor/solution provider documentation to verify that the host enters an error state and generates an alert in the event of the following: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements 4D-1.6 and 4D-1.7 • Failure of a security function or mechanism	Vendor/solution provider documentation reviewed:	*<Report Findings Here>*		
	Describe how Host System configuration settings and vendor/solution provider documentation verified that the host enters an error state and generates an alert in the event of the following: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements 4D-1.6 and 4D-1.7 • Failure of a security function or mechanism			
	<Report Findings Here>			
4D-1.8.b Interview personnel and examine logs/records of actual or test alerts to verify that alerts are generated and received when the Host System enters an error state under one of the following conditions: • Failure of a cryptographic operation, and • Failure of a system self-test, as described in Requirements 4D-1.6 and 4D-1.7, and • Failure of a security function or mechanism	Personnel interviewed:	*<Report Findings Here>*		
	Logs/records of actual or test alerts examined:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.9 Alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.		☐	☐	☐
4D-1.9.a Review documented procedures to verify alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.	Documented procedures reviewed:	*<Report Findings Here>*		
4D-1.9.b Examine system configurations and records of documented alert events to verify alerts generated from the Host System are documented.	Records of documented alert events reviewed:	*<Report Findings Here>*		
	Describe how system configurations and records of documented alert events verified that alerts generated from the Host System are documented:			
	<Report Findings Here>			
4D-1.9.c Examine a sample of documented alert events and interview personnel assigned with security-response duties to verify alerts initiate a response procedure.	Sample of documented alert events examined:	*<Report Findings Here>*		
	Personnel assigned with security-response duties interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.10 The Host System must not perform any cryptographic operations under any of the following conditions: • While in an error state, as described in Requirement 4D-1.8 • During self-tests, as described in Requirements 4D-1.6 and 4D-1.7 • During diagnostics of cryptographic operations		☐	☐	☐
4D-1.10.a Examine documented procedures to verify that controls/processes are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement 4D-1.8 • During self-tests, as described in Requirements 4D-1.6 and 4D-1.7 • During diagnostics of cryptographic operations	Documented procedures reviewed:	*<Report Findings Here>*		
4D-1.10.b Inspect Host System configuration settings and interview personnel to verify that controls and/or procedures are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement 4D-1.8 • During self-tests, as described in Requirements 4D-1.6 and 4D-1.7 • During diagnostics of cryptographic operations	Personnel interviewed:	*<Report Findings Here>*		
	Describe how Host System configuration settings verified that controls and/or procedures are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement 4D-1.8 • During self-tests, as described in Requirements 4D-1.6 and 4D-1.7 • During diagnostics of cryptographic operations			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.11 All source code and executable code for cryptographic software and firmware on the Host System must be protected from unauthorized disclosure and unauthorized modification.		☐	☐	☐
4D-1.11.a Inspect configuration documentation to verify that access controls are defined to ensure all source code and executable code for cryptographic software and firmware is protected from unauthorized disclosure and unauthorized modification.	Configuration documentation inspected:	*<Report Findings Here>*		
4D-1.11.b Observe access controls for cryptographic software and firmware to verify that all source code and executable code is protected from unauthorized disclosure and unauthorized modification.	Describe how the access controls for cryptographic software and firmware observed verified that all source code and executable code is protected from unauthorized disclosure and unauthorized modification:			
	<Report Findings Here>			
4D-1.12 The clear-text data-decryption keys must not be accessible to any processes or functions not directly required for decryption operations.		☐	☐	☐
4D-1.12.a Review solution provider documentation, including data-flow diagrams, to verify that clear-text decryption keys are not accessible to any processes or functions not directly required for decryption operations.	Solution provider documentation reviewed (including data-flow diagrams):	*<Report Findings Here>*		
4D-1.12.b Inspect Host System configurations and access controls and to verify that clear-text decryption keys are not accessible to any processes or functions not directly required for decryption operations.	Describe how the Host System configurations and access controls inspected verified that clear-text decryption keys are not accessible to any processes or functions not directly required for decryption operations:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.13 The clear-text data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys		☐	☐	☐
4D-1.13.a Examine documented key-management policies and procedures to verify clear-text data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
4D-1.13.b Inspect Host System configuration settings and verify that clear-text data-decryption keys are only accessible to authorized personnel with a defined job-related need to access the keys.	Describe how the Host System configuration settings inspected verified that clear-text data-decryption keys are only accessible to authorized personnel with a defined job-related need to access the keys:			
	<Report Findings Here>			
4D-1.14 The Host System must not write clear-text cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory "swap/page" file purposes • "Core dumps" of memory required for troubleshooting In the above circumstances, the following conditions apply:		☐	☐	☐
4D-1.14.a Examine documented configuration procedures to verify that the Host System must not write clear-text cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory swap/page file purposes • Core dumps of memory required for trouble-shooting	Documented configuration procedures reviewed:	*<Report Findings Here>*		
4D-1.14.b Examine Host System configuration settings and interview personnel to verify that clear-text cryptographic keys are not written to persistent storage except in the following circumstances: • Memory swap/page file purposes. • core dumps of memory required for trouble-shooting	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the Host System configuration settings examined verified that clear-text cryptographic keys are not written to persistent storage except in the following circumstances: • Memory swap/page file purposes. • core dumps of memory required for trouble-shooting			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.14.c Verify documented procedures include Requirements 4D-1.14.1 through 4D-1.14.5 below.				
4D-1.14.1 The locations must be predefined and documented.		☐	☐	☐
4D-1.14.1.a Review Host System configuration standards to verify that storage locations of any swap/page files and core dumps are defined.	Host System configuration standards reviewed:	*<Report Findings Here>*		
4D-1.14.1.b Examine Host System configuration settings to verify that the Host System only outputs swap/page files and core dumps to the documented storage locations.	Describe how the Host System configuration settings examined verified that the Host System only outputs swap/page files and core dumps to the documented storage locations:			
	<Report Findings Here>			
4D-1.14.2 Storage can only be made to a dedicated hard drive (on its own bus) within the host.		☐	☐	☐
4D-1.14.2 Examine Host System configuration settings and storage locations to verify that swap/page files and core dumps are written to a dedicated hard drive on its own bus on the Host System.	Describe how the Host System configuration settings and storage locations examined verified that swap/page files and core dumps are written to a dedicated hard drive on its own bus on the Host System:			
	<Report Findings Here>			
4D-1.14.3 The swap/page files and/or core dumps must never be backed up or copied.		☐	☐	☐
4D-1.14.3.a Examine backup configuration settings for the Host System and storage locations to verify that swap/page files and core dumps are not backed up.	Describe how the backup configuration settings for the Host System and storage locations examined verified that swap/page files and core dumps are not backed up:			
	<Report Findings Here>			
4D-1.14.3.b Examine configurations of storage locations to verify that swap/page files and core dumps cannot be copied off the storage locations.	Describe how the configurations of storage locations examined verified that swap/page files and core dumps cannot be copied off the storage locations:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.14.4 Access to, and the use of, any tools used for trouble-shooting or forensics must be controlled and authorized by management.		☐	☐	☐
4D-1.14.4.a Examine documented procedures to verify that controls are defined to ensure that the access to, and use of, any tools used for trouble-shooting or forensics, are controlled and authorized by management.	Documented procedures reviewed:	*<Report Findings Here>*		
4D-1.14.4.b Observe the process for accessing the tools used for trouble-shooting or forensics, and verify that they are controlled and authorized by management in accordance with the documented procedure.	Describe how the process for accessing the tools used for trouble-shooting or forensics verified that they are controlled and authorized by management in accordance with the documented procedure:			
	<Report Findings Here>			
4D-1.14.4.c Observe the process for using the tools used for trouble-shooting or forensics, and verify that they are controlled and authorized by management in accordance with the documented procedure.	Describe how the process for using the tools used for trouble-shooting or forensics verified that they are controlled and authorized by management in accordance with the documented procedure:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-1.14.5 All files must be securely deleted in accordance with industry-accepted standards for secure deletion of data: Core dumps must be securely deleted immediately after analysis. Memory swap/page files must be securely deleted upon system shut down or reset.		☐	☐	☐
4D-1.14.5.a Review documented procedures to verify that it defines a process for securely deleting swap/page files and core dumps at the required times: • Core dumps must be securely deleted immediately after analysis. • Memory swap/page files must be securely deleted upon system shut down or reset.	Documented procedures reviewed:	*<Report Findings Here>*		
4D-1.14.5.b Verify, through the use of forensic tools and/or methods, that the secure procedure removes swap/page files and core dumps, in accordance with industry-accepted standards for secure deletion of data.	Describe the forensic tools and/or methods used to verify that the secure procedure removes swap/page files and core dumps, in accordance with industry-accepted standards for secure deletion of data:			
	<Report Findings Here>			
4D-2.1 Host user passwords must be changed at least every 30 days. ***Note:*** *This requirement applies to all user roles associated to persons with access to the Host System.*		☐	☐	☐
4D-2.1.a Examine documented policies and procedures to verify that the Host System (s) user passwords must be changed at least every 30 days.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.1.b Inspect Host System configuration settings to verify that user password parameters are set to require users to change passwords at least every 30 days.	Describe how the Host System configuration settings inspected verified that user password parameters are set to require users to change passwords at least every 30 days:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.2 User passwords must meet the following: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or Have equivalent strength/complexity.		☐	☐	☐
4D-2.2.a Examine documented policies and procedures to verify that user passwords must: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.2.b Inspect Host System (s) configuration settings to verify that user passwords: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.	Describe how the Host System configuration settings inspected verified that user passwords: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.3 Where log-on security tokens (e.g., smart cards) are used to access the Host System, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage. The PIN or password/passphrase must be at least ten alphanumeric characters in length, or equivalent.		☐	☐	☐
4D-2.3.a If log-on security tokens are used, observe the security tokens in use to verify that they have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage.	Log-on security tokens in use:	*<Report Findings Here>*		
	Describe how log-on security tokens in use verified that an associated usage-authentication mechanism is in place to enable their usage:			
	<Report Findings Here>			
4D-2.3.b Examine token-configuration settings to verify parameters are set to require that PINs or password/passphrases be at least ten alphanumeric characters in length, or equivalent.	Describe how the token-configuration settings examined verified that parameters are set to require that PINs or password/passphrases be at least ten alphanumeric characters in length, or equivalent:			
	<Report Findings Here>			
4D-2.4 User accounts must be locked out of the Host System after not more than five failed attempts.		☐	☐	☐
4D-2.4.a Examine documented policies and procedures to verify that authentication parameters on the Host System must be set to require that a user's account be locked out after not more than five invalid logon attempts.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.4.b Inspect Host System configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon attempts.	Describe how the Host System configuration settings inspected verified that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon attempts:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.5 The Host System must enforce role-based access control to include, at a minimum, the following roles: • Host System operator role – for day-to-day non-sensitive operations of the Host System • Host System administrator role – configuration of host OS, security controls, software and user accounts • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions		☐	☐	☐
4D-2.5.a Examine documented access-control procedures to verify they define, at a minimum, the following roles: • Host System operator role – for day-to-day non-sensitive operations of the Host System • Host System administrator role – configuration of host OS, security controls, software and user accounts • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions	Documented access-control procedures reviewed:	*<Report Findings Here>*		
4D-2.5.b Inspect the Host System configuration settings to verify that role-based access control is enforced and, at a minimum, the following roles are defined: • Host System operator role – for day-to-day non-sensitive operations of the Host System • Host System administrator role – configuration of host OS, security controls, software and user accounts • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions	Describe how the Host System configuration settings inspected verified that role-based access control is enforced and, at a minimum, the following roles are defined: • Host System operator role – for day-to-day non-sensitive operations of the Host System • Host System administrator role – configuration of host OS, security controls, software and user accounts • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions			
	<Report Findings Here>			
4D-2.5.c Interview a sample of users for each role to verify the assigned role is appropriate for their job function.	Sample of users for each role interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.6 The segregation of duties must be enforced between roles, through automated or manual processes, to ensure that no one person is able to control end-to-end processes; or be in a position to compromise the security of the Host System. The following conditions must be applied:		☐	☐	☐
4D-2.6.1 A Host System user must not be permitted to audit their own activity on the Host System.		☐	☐	☐
4D-2.6.1.a Examine documented procedures to verify that a Host System user is not permitted to audit their own activity on the Host System.	Documented procedures reviewed:	*<Report Findings Here>*		
4D-2.6.1.b Interview audit personnel to verify that a Host System user is not permitted to audit their own activity on the Host System.	Audit personnel interviewed:	*<Report Findings Here>*		
4D-2.6.2 A Host System administrator must use their operator-level account when performing non-administrative functions.		☐	☐	☐
4D-2.6.2.a Review documented policies and procedures to verify a Host System administrator is not permitted to use their administrative-level account when performing non-administrative functions.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.6.2.b Interview and observe a Host System administrator to verify they use their operator-level account when performing non-administrative functions.	Host System administrator interviewed:	*<Report Findings Here>*		
	Describe how the observation of the Host System administrator verified they use their operator-level account when performing non-administrative functions:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.7 Changes to a Host System user's account access privileges must be managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.		☐	☐	☐
4D-2.7.a Examine documented policies and procedures to verify that changes to a user's access privileges are managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.7.b Observe the process required to change a user's access privileges and verify that it is managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.	Describe how the observed process to change a user's access privileges verified that it is managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.			
	<Report Findings Here>			
4D-2.7.c Inspect the Host System configuration settings and, for a sample of user accounts, verify that any changes to their access privileges have been formally documented in the audit log.	Sample of user accounts:	<Report Findings Here>		
	Describe how the Host System configuration settings inspected verified that for the sample of user accounts, any changes to their access privileges have been formally documented in the audit log:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-2.8 All physical and logical access privileges must be reviewed at least quarterly to ensure that personnel with access to the decryption environment, the Host System and Host System software require that access for their position and job function.		☐	☐	☐
4D-2.8.a Examine documented policies and procedures to verify that access privileges are reviewed, at a minimum, on a quarterly basis to ensure that the access privileges for personnel authorized to access the decryption environment, the Host System, and Host System software required by their position and job function, are correctly assigned.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-2.8.b Examine records and interview personnel to verify that access privileges are reviewed, at a minimum, on a quarterly basis.	Personnel interviewed:	*<Report Findings Here>*		
	Records reviewed:	*<Report Findings Here>*		
4D-2.9 Tamper-detection mechanisms must be implemented on the host, to include an alert generation upon opening of the Host System case, covers and/or doors.		☐	☐	☐
4D-2.9.a Review Host System documentation to verify that tamper-detection mechanisms are defined for the Host System, including the generation of an alert upon opening of the Host System case, covers and/or doors.	Host System documentation reviewed:	*<Report Findings Here>*		
4D-2.9.b Observe tamper-detection mechanisms on the Host System to verify that a tamper-detection mechanism is implemented and includes the generation of an alert upon opening of the Host System case, covers and/or doors.	Identify the tamper-detection mechanisms observed:	*<Report Findings Here>*		
	Describe how the observed tamper-detection mechanisms are implemented and include the generation of an alert upon opening of the Host System case, covers and/or doors:			
	<Report Findings Here>			
4D-2.9.c Review records of alerts and interview personnel to verify an alert is generated upon opening of the Host System, covers and/or doors.	Records of alerts reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-3.1 All non-console access to the Host System must use strong cryptography and security protocols.		☐	☐	☐
4D-3.1.a For a sample of systems that are authorized to connect to the Host System via a non-console connection, inspect configuration settings to verify that access to the Host System is provided through the use of strong cryptography and security protocols.	Sample of systems reviewed:	*<Report Findings Here>*		
	Describe how the configuration settings inspected verified that access to the Host System is provided through the use of strong cryptography and security protocols:			
	<Report Findings Here>			
4D-3.1.b Inspect the configuration settings of system components to verify that all traffic transmitted over the secure channel uses strong cryptography.	Describe how the configuration settings of system components verified that all traffic transmitted over the secure channel uses strong cryptography:			
	<Report Findings Here>			
4D-3.2 Non-console access to the Host System must not provide access to any other service, or channel, outside of that used to connect to the Host, e.g., "split tunneling."		☐	☐	☐
4D-3.2.a Inspect the configuration settings of the secure channel, to verify that 'split tunneling' is prohibited.	Describe how the configuration settings of the secure channel verified that 'split tunneling' is prohibited:			
	<Report Findings Here>			
4D-3.2.b Observe a Host System administrator log on to the device which provides non-console access to the Host System to verify that "split tunneling" is prohibited.	Describe how the Host System administrator's log on to the device verified that 'split tunneling' is prohibited:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-3.3 All non-console access to the Host System must use multi-factor authentication.		☐	☐	☐
4D-3.3.a Inspect the configuration settings of the Host System and/or the device permitted to connect to the Host System, to verify that multi-factor authentication is required for non-console access to the Host System.	Describe how the configuration settings of the Host System and/or the device permitted to connect to the Host System verified that multi-factor authentication is required for non-console access to the Host System:			
	<Report Findings Here>			
4D-3.3.b Observe a Host System administrator log on to the device that provides non-console access to the Host System to verify that multi-factor authentication is required.	Describe how the Host System administrator's log on to the device that provides non-console access to the Host System verified that multi-factor authentication is required:			
	<Report Findings Here>			
4D-3.4 Non-console connections to the Host System must only be permitted from authorized systems.		☐	☐	☐
4D-3.4.a Examine documented policies and procedures to verify that a process is defined to authorize systems for non-console access, and not permit access until such times that authorization has been granted.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-3.4.b For a sample of systems, examine device configurations to verify that non-console access is permitted only from the authorized systems.	Sample of systems reviewed:	*<Report Findings Here>*		
	Describe how device configurations for the sample of systems verified that non-console access is permitted only from the authorized systems:			
	<Report Findings Here>			
4D-3.5 Non-console access to the Host System must only be permitted from a PCI DSS compliant environment.		☐	☐	☐
4D-3.5 Verify that non-console access to the Host System is only permitted from a PCI DSS compliant environment, including 4D-3.5.1 through 4D-3.5.2 Review solution provider documentation, including data-flow diagrams, and perform the following:	Solution provider documentation reviewed (including data-flow diagrams):	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-3.5.1 The authorized system (e.g., workstation) from which non-console access originates must meet all applicable PCI DSS requirements. For example, system hardening, patching, anti-virus protection, a local firewall etc.		☐	☐	☐
4D-3.5.1 Review solution provider documentation, including PCI DSS ROC and/or Attestation of Compliance (AOC), data-flow diagrams, policies and, system configuration standards, to verify that the system authorized for non-console access meets all applicable PCI DSS requirements.	Solution provider documentation reviewed (including PCI DSS ROC and/or AOC):	*<Report Findings Here>*		
4D-3.5.2 The network/system that facilitates non-console access to the Host System must: • Originate from and be managed by the solution provider. • Meet all applicable PCI DSS requirements.		☐	☐	☐
4D-3.5.2 Review solution provider documentation, including PCI DSS ROC and/or Attestation of Compliance (AOC), data-flow diagrams, policies and, system configuration standards, to verify that the network/system that facilitates non-console access to the Host System must: • Originate from and be managed by the solution provider. • Meet all applicable PCI DSS requirements.	Solution provider documentation reviewed (including PCI DSS ROC and/or AOC):	*<Report Findings Here>*		
4D-3.6 Users with access to non-console connections to the Host System must be authorized to use non-console connections.		☐	☐	☐
4D-3.6.a Examine documented policies and procedures to verify that non-console access to the Host System must only be provided to authorized users.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-3.6.b Examine a sample of access control records and compare them to Host System settings to verify that non-console access to the Host System is only provided to authorized users.	Sample of access control records reviewed:	*<Report Findings Here>*		
	Describe how the sample of access control records compared to Host System settings verified that non-console access to the Host System is only provided to authorized users:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-3.7 Non-console sessions to the Host System must be terminated after 15 minutes of inactivity.		☐	☐	☐
4D-3.7.a Review documented policies and procedures to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-3.7.b Inspect the system configuration settings to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.	Describe how system configuration settings verified that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity:			
	<Report Findings Here>			
4D-4.1 The Host System must be located within a physically secure room that is dedicated to decryption operations and transaction processing. Note: Where "secure room" is referred to in this section, these controls can be met at room level, rack level, or a combination of both. Whichever way the requirements are applied, they should ensure that access the Host System is appropriately secured, whether in a secure room or a secure rack. For example, access to systems in a rack should be limited to those with a direct need to access that rack.		☐	☐	☐
4D-4.1 Observe the physically secure room where the Host System is located and interview personnel to verify that all systems therein are designated to decryption operations and transaction processing.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how observation of the physically secure room where the Host System is located verified that all systems therein are designated to decryption operations and transaction processing:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.2 All individuals must be identified and authenticated before being granted access to the secure room—e.g., badge-control system, biometrics.		☐	☐	☐
4D-4.2.a Examine documented policies and procedures to verify that all individuals must be identified and authenticated before being granted access to the secure room.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.2.b Examine physical access controls to verify that all individuals are identified and authenticated before being granted access to the secure room.	Physical access controls examined:	*<Report Findings Here>*		
4D-4.2.c Observe authorized personnel entering the secure room to verify that all individuals are identified and authenticated before being granted access.	Describe how observation of authorized personnel entering the secure room verified that all individuals are identified and authenticated before being granted access:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.3 All physical access to the secure room must be monitored and logs must be maintained as follows: • Logs must be retained for a minimum of three years. • Logs must be regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein. • Log reviews must be documented. • Logs must include but not be limited to: – Logs of access to the room from a badge access system – Logs of access to the room from a manual sign-in sheet		☐	☐	☐
4D-4.3.a Examine documented policies and procedures to verify all physical access to the secure room must be monitored and logs must be maintained. Policies and procedures must require the following: • Logs are retained for a minimum of three years. • Logs are regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein. • Log reviews are documented. • Logs include at a minimum: – Access to the room from a badge access system – Access to the room from a manual sign-in sheet	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.3.b Examine a sample of logs used to record physical access to the secure room to verify the following: • Logs are being retained for a minimum of three years. • Logs include at a minimum: – Access to the room from a badge access system – Access to the room from a manual sign-in sheet	Sample of logs reviewed:	*<Report Findings Here>*		
4D-4.3.c Interview personnel responsible for reviewing logs used to record physical access to the secure room, to verify the following: • Logs are regularly reviewed. • Log reviews are documented. • The person performing the review does not have access to the secure room or to the systems therein.	Responsible personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.4 Dual access must be required for the secure room housing the Host System.		☐	☐	☐
4D-4.4.a Inspect physical access controls to verify that dual access is enforced.	Physical access controls inspected:	*<Report Findings Here>*		
4D-4.4.b Observe authorized personnel entering the secure room to verify that dual access is enforced.	Describe how observation of authorized personnel entering the secure room verified that dual control is enforced:			
	<Report Findings Here>			
4D-4.5 Physical access must be only permitted to designated personnel with defined business needs and duties.		☐	☐	☐
4D-4.5.a Examine documented policies and procedures to verify that physical access to the secure room is only permitted to designated personnel with defined business needs and duties.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.5.b Examine the list of designated personnel and interview responsible personnel to verify that only personnel with defined business needs and duties are permitted access to the secure room.	Documented list of designated personnel:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
4D-4.5.c Examine physical access controls to verify that physical access to the secure room is only permitted to pre-designated personnel with defined business needs and duties.	Describe how physical access controls verified that physical access to the secure room is only permitted to pre-designated personnel with defined business needs and duties:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.6 The secure room must be monitored via CCTV on a 24-hour basis. This must include, at a minimum, the following areas: • All entrances and exists • Access to the Host System and HSM(s) ***Note:*** *Motion-activated systems that are separate from the intrusion-detection system may be used.*		☐	☐	☐
4D-4.6.a Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a 24 hour basis, and covers, at a minimum, the following areas: • All entrances and exists • Access to the Host System and HSM(s)	Sample of CCTV recordings reviewed:	*<Report Findings Here>*		
	Describe how CCTV configurations observed verified that CCTV monitoring is in place on a 24 hour basis, and covers, at a minimum, the following areas: • All entrances and exists • Access to the Host System and HSM(s)			
	<Report Findings Here>			
4D-4.6.b If CCTV is motion-activated, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.	Describe how system configurations for the motion-activated systems verified that they are separate from the intrusion-detection systems:			
	<Report Findings Here>			
4D-4.7 Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, or other systems which may expose sensitive data.		☐	☐	☐
4D-4.7 Observe CCTV camera positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any computer screens, PIN pads, keyboards, or other systems which may expose sensitive data.	Sample of CCTV recordings reviewed:	*<Report Findings Here>*		
	Describe how observed CCTV camera positioning and the sample of recordings verified that CCTV cameras do not monitor any computer screens, PIN pads, keyboards, or other systems which may expose sensitive data:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.8 CCTV recorded images must be securely archived for at least 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.		☐	☐	☐
4D-4.8.a Examine a sample of recordings to verify that at least the most recent 45 days of images are securely archived.	Sample of CCTV recordings reviewed:	*<Report Findings Here>*		
4D-4.8.b 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.	Describe how system configurations observed verified that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period: *<Report Findings Here>*			
4D-4.9 Personnel with access to the secure room must not have access to the media (e.g., VCR tapes, digital recording systems, etc.) with the recorded surveillance data.		☐	☐	☐
4D-4.9.a Examine documented access policies and procedures to verify that personnel with access to the secure room are not permitted to have access to the media containing recorded surveillance data for that environment.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.9.b Examine access lists for the secure room as well as access controls to the media containing surveillance data, to verify that personnel with access to the secure room do not have access to the media containing recorded surveillance data	Describe how access lists for the secure room as well as access controls to the media containing surveillance data verified that personnel with access to the secure room do not have access to the media containing recorded surveillance data: *<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.10 Continuous or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (e.g., when infrared cameras are used).*		☐	☐	☐
4D-4.10.a Observe the secure room to verify that continuous or motion-activated lighting is provided for the cameras monitoring the secure room.	Describe how the observed secure room verified that continuous or motion-activated lighting is provided for the cameras monitoring the secure room: *<Report Findings Here>*			
4D-4.10.b Examine a sample of recorded CCTV images to verify that appropriate lighting is provided when persons are present in the secure room.	Sample of recorded CCTV images examined:	*<Report Findings Here>*		
4D-4.11 A 24/7 physical intrusion-detection system must be in place for the secure room (e.g., motion detectors when unoccupied). This must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.		☐	☐	☐
4D-4.11.a Examine security policies and procedures to verify they require: • Continuous (24/7) physical intrusion-detection monitoring of the secure room. • The physical intrusion-detection must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.	Documented security policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.11.b Observe the physical intrusion-detection system to verify that it: • Provides continuous (24/7) monitoring of the secure room. • It is connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.	Describe how the physical intrusion-detection system verified that it: • Provides continuous (24/7) monitoring of the secure room. • It is connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room. *<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.12 Any windows in the secure room must be locked, protected by alarmed sensors, or otherwise similarly secured.		☐	☐	☐
4D-4.12.a Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.	Identify the P2PE Assessor who confirms all windows in the observed secure room are locked and protected by alarmed sensors:	*<Report Findings Here>*		
4D-4.12.b Examine configuration of window sensors to verify that the alarm mechanism is active.	Describe how configuration of window sensors verified that the alarm mechanism is active:			
	<Report Findings Here>			
4D-4.13 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.		☐	☐	☐
4D-4.13 Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	Identify the P2PE Assessor who confirms all windows in the observed secure room are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room:	*<Report Findings Here>*		
4D-4.14 Access-control and monitoring systems must be connected to an uninterruptible power source (UPS) to prevent outages.		☐	☐	☐
4D-4.14 Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems are powered through the UPS.	Describe how the UPS system configurations observed verified that all access-control and monitoring systems are powered through the UPS:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.15 All alarm events must be logged.		☐	☐	☐
4D-4.15.a Examine security policies and procedures to verify they require that all alarm events are logged.	Documented security policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.15.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.	Describe how security-system configurations and documented alarm events verified that all alarm events are logged:			
	<Report Findings Here>			
4D-4.16 Documented alarm events must be signed off by an authorized person who was not involved in the event.		☐	☐	☐
4D-4.16.a Examine security policies and procedures to verify alarm events must be signed off by an authorized person other than the individual who was involved in the event.	Documented security policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.16.b For a sample of documented alarm events, interview personnel who signed off on the event to verify that person was not involved in the event.	Sample of documented alarm events reviewed:	*<Report Findings Here>*		
	Signing personnel interviewed:	*<Report Findings Here>*		
4D-4.17 Use of an emergency entry or exit mechanism must cause an alarm event.		☐	☐	☐
4D-4.17 Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.	Describe how security system configurations observed verified that an alarm event is generated upon use of any emergency entry or exit mechanism:			
	<Report Findings Here>			
4D-4.18 Authorized personnel must respond to all physical intrusion alarms within 30 minutes.		☐	☐	☐
4D-4.18.a Examine documented policies and procedures to verify they define that all alarm events are responded to by authorized personnel within 30 minutes.	Documented policies and procedures reviewed:	*<Report Findings Here>*		
4D-4.18.b Examine documented alarm events and interview personnel to verify alarm events were responded by authorized personnel within 30 minutes.	Documented alarm events reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.19 A process for synchronizing the time and date stamps of the access-control, intrusion-detection and monitoring (camera) systems must be implemented. ***Note:*** *This may be done by either automated or manual mechanisms.*		☐	☐	☐
4D-4.19.a Examine documented procedures to verify that mechanisms are defined for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems.	Documented procedures reviewed:	*<Report Findings Here>*		
4D-4.19.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.	Describe how system configurations for access, intrusion-detection, and monitoring (camera) systems verified that time and date stamps are synchronized:			
	<Report Findings Here>			
4D-4.19.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.	Sample of logs from the access, intrusion-detection, and monitoring (camera) systems:	*<Report Findings Here>*		
4D-4.19.1 If a manual synchronization process is used, synchronization must occur at least quarterly, and documentation of the synchronization must be retained for at least a one-year period.		☐	☐	☐
4D-4.19.1.a If a manual synchronization process is implemented, interview responsible personnel and examine records of synchronization to verify the mechanism is performed at least quarterly.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Records of synchronization examined:	*<Report Findings Here>*		
4D-4.19.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.	Records of synchronization examined:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4D-4.20 The entrance to the secure room must include a mechanism to ensure the door is not left open. *For example:* • *A door that is contact monitored and fitted with automatic closing or locking devices.* • *An airlock entrance system.*		☐	☐	☐
4D-4.20 Observe authorized personnel entering the secure room to verify that a mechanism is in place to ensure the door is not left open. *Examples include:* • *A door that is contact monitored and fitted with automatic closing or locking devices.* • *An airlock entrance system.*	Describe how the observation of authorized personnel entering the secure room verified that a mechanism is in place to ensure the door is not left open:			
	<Report Findings Here>			
4D-4.21 An audible alarm must sound if the entrance to the secure room remains open for more than 30 seconds.		☐	☐	☐
4D-4.21.a Examine secure room entry mechanisms to verify that an audible alarm is configured to sound if the entrance remains open for more than 30 seconds.	Identify the secure room entry mechanisms examined:	*<Report Findings Here>*		
4D-4.21.b Observe authorized personnel entering the secure room and request the door is held open. Verify that an audible alarm sounds if the entrance remains open for more than 30 seconds.	Describe how the observation of authorized personnel entering the secure room and holding the door open more than 30 seconds verified an audible alarm sounds:			
	<Report Findings Here>			
4E-1.1 Determine whether, for this submission, the vendor is a component provider.	Indicate for this submission, whether the vendor is a component provider. (yes/no).	*<Report Findings Here>*		
If "yes", complete 4E-1.1 to 4E-1.2.b (otherwise leave blank).				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4E-1.1 Track status of the decryption-management service and provide reports to solution provider annually and upon significant changes, including at least the following: • Types/models of HSMs • Number of HSMs deployed and any change in numbers since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per 4C-1.2		☐	☐	☐
4E-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: • Providing reports annually and upon significant changes • Types/models of HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per 4C-1.2	Component provider's documented procedures reviewed:	*<Report Findings Here>*		
	Responsible component provider personnel interviewed:	*<Report Findings Here>*		
4E-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 HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per 4C-1.2	Identify reports reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
4E-1.2 Manage and monitor changes to decryption-management services and notify the solution provider upon occurrence of any of the following: • Addition and/or removal of HSM types. • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status ***Note:*** *Adding or removing HSM types may require adherence to PCI SSC's process for P2PE Designated Changes to Solutions. Please refer to the P2PE Program Guide for details about obligations when adding, changing, or removing elements of a P2PE solution.*		☐	☐	☐
4E-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 infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types	Component provider's documented procedures reviewed:	*<Report Findings Here>*		
	Responsible component provider personnel interviewed:	*<Report Findings Here>*		
4E-1.2.b Observe reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types	Identify reports reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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 DMS				
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.*		☐	☐	☐
1-3 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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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		☐	☐	☐
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 Review the PCI approval listing(s) for any implementation-specific notes and if present, verify they are accounted for.	For each PCI-approved HSM used in the solution, describe how the HSM device configurations observed verified that all of the device characteristics at **1-4.a** match the PTS listing: *<Report Findings Here>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 *FIPS 140-2* 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 in the solution, describe how the HSM device configurations observed verified that all of the device characteristics at **1-4.b** match the FIPS140-2 Level 3 (or higher) approval listing: *<Report Findings Here>*			
1-5 Not used in DMS				
Requirements 2, 3, and 4 not used in P2PE				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.*		☐	☐	☐
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 key management policies and procedures reviewed:	*<Report Findings Here>*		
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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5-1.c Examine procedures to be used for future generations and logs of past key generation to verify devices used for key-generation are those as noted above, including validation of firmware used.	Describe how the reviewed devices used for key generation verified that devices are as noted above, including validation of the firmware:			
	<Report Findings Here>			
6-1 Implement security controls, including dual control and tamper detection, to prevent the unauthorized disclosure of keys or key components. Perform the following:		☐	☐	☐
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 the entire key.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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-generations 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>			
	Describe how the key-generations processes observed verified that there is no mechanism (including connectivity) that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component:			
	<Report Findings Here>			
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.*		☐	☐	☐
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 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>			
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 examined:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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.		☐	☐	☐
6-1.3 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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>*			
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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 the key-component/key-generation process cannot be observed or accessed by unauthorized personnel: *<Report Findings Here>*			

Decryption Management Services – Reporting				
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*				
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 reviewed:	*<Report Findings Here>*		
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 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.		☐	☐	☐
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 detected.	Documented procedures for printed key components reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 detected.	Describe how the blind mailers or other sealed containers used for key components observed verified that tampering can be detected:			
	<Report Findings Here>			
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.		☐	☐	☐
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>			
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>			
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.		☐	☐	☐
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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.		☐	☐	☐
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>			
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>			
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.		☐	☐	☐
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.		☐	☐	☐
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>			
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.		☐	☐	☐
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>			
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>			

Decryption Management Services – Reporting				
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).*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 and 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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>*			

Decryption Management Services – Reporting				
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		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>*		
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>			
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>			
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>*		

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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	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: • 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.			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
components using pre-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>*			
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 reviewed:	*<Report Findings Here>*		
	Records of key conveyances examined:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 reviewed:	*<Report Findings Here>*		
	Records of key conveyances examined:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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*		☐	☐	☐
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 procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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: • Only designated custodians can send/receive the component or share. • 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. • Any 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.			
	<Report Findings Here>			
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.	Records of key conveyances examined:	*<Report Findings Here>*		
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.				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
8-3 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>			

Decryption Management Services – Reporting				
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 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 certificates 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.*		☐	☐	☐
8-4 For all methods used to convey public keys, perform the following:				
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 reviewed:	*<Report Findings Here>*		
8-4.b Validate that procedures dictate that self-signed certificates must not be used as the sole method of authentication.	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.	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>			
	Responsible personnel interviewed:	*<Report Findings Here>*		
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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 • 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.			
	<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 a 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		☐	☐	☐
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>*		
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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>*		
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 • 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>			
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	Records related to escalated transmital events examined:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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.		☐	☐	☐
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.	Documentation reviewed:	*<Report Findings Here>*		
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 and upon removal of a secured key component from transmittal packaging			
	<Report Findings Here>			
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>*		

Decryption Management Services – Reporting				
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 tamper 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.*		☐	☐	☐
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 tamper 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.	Documentation reviewed:	*<Report Findings Here>*		
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 tamper 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.	Logs reviewed:	*<Report Findings Here>*		
	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 tamper 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>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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	Identify the P2PE Assessor who determined that if components or shares of multiple 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	*<Report Findings Here>*		
9-6.b Examine logs to verify that procedures are followed.	Logs reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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 must have a bit strength of at least 112 bits.		☐	☐	☐
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>*		
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).	Document(s) reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
	Keys identified that protect other keys for transmission.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 this: • 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.	Documented procedures reviewed:	*<Report Findings Here>*		
	Appropriate personnel interviewed:	*<Report Findings Here>*		
	Documented procedures reviewed:	*<Report Findings Here>*		
	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>			
10-2 Not used in P2PE				
10-3 Not used in P2PE				
10-4 Not used in P2PE				
10-5 Not used in P2PE				

Decryption Management Services – Reporting				
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.		☐	☐	☐
11-1.a Verify documented procedures exist for all key transmission and conveyance processing.	Documented procedures reviewed:	*<Report Findings Here>*		
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.		☐	☐	☐
11-2 Verify documented procedures include all methods used for the conveyance or receipt of keys.	Documented procedures reviewed:	*<Report Findings Here>*		
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.*		☐	☐	☐
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 process reviewed:	*<Report Findings Here>*		
12-1.b Interview appropriate personnel to determine the number of key components for each manually loaded key.	Appropriate personnel interviewed:	*<Report Findings Here>*		
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>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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>			
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>			
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.	Documents reviewed:	*<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.		☐	☐	☐
12-2.a. Examine logs of access to security containers for key components/shares to verify that only the authorized custodian(s) have accessed. 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>*		

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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: • 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 are maintained separately.	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
12-3.b For each type of production SCD 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 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.			
	<Report Findings Here>			
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>*		
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.*		☐	☐	☐
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>*		
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 key-component lengths or device configuration settings verified that key components used to create a key are the same length as the resultant key:			
	<Report Findings Here>			
12-5 Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must use AES with a key size of at least 128 bits.		☐	☐	☐
12-5 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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.		☐	☐	☐
12-6 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 the observations that 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>			
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.		☐	☐	☐
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>*		
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>*		

Decryption Management Services – Reporting				
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 Domain of 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.		☐	☐	☐
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.	Documentation reviewed:	*<Report Findings Here>*		
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 DMS				

Decryption Management Services – Reporting				
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.		☐	☐	☐
13-1 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: – 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.	Documented procedures reviewed:	*<Report Findings Here>*		
	Describe how the demonstration verified that • 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, which could lead to the disclosure of clear-text keying material.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
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, the PED must be managed in accordance with Requirement 13-9.*		☐	☐	☐
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>*		
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 key loading 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>			

Decryption Management Services – Reporting				
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**.		☐	☐	☐
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>*		
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 in accordance with **Requirement 24**. *<Report Findings Here>*			
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**.	Records examined:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
13-4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:		☐	☐	☐
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.		☐	☐	☐
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>			
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.		☐	☐	☐
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.		☐	☐	☐

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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. Such personnel must ensure that a key-recording device is not inserted between the SCDs.			
	<Report Findings Here>			
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>			
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.		☐	☐	☐
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 (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.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>*		
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 reviewed:	*<Report Findings Here>*		
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>*		
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.		☐	☐	☐
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>			
13-7 Written or printed key component documents must not be opened until immediately prior to use.		☐	☐	☐
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>*		
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>			
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.*		☐	☐	☐
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 DMS				
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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. • 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.	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.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>			
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 the number of devices keys are loaded to.		☐	☐	☐
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>			
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>*		

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>*		
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>*		
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>*		
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>*		
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.		☐	☐	☐
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>*		
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>*		
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.*		☐	☐	☐
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>*		
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>*			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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>			
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.*		☐	☐	☐
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>*		
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 DMS				
15-4 Not used in DMS				
15-5 Not used in DMS				

Decryption Management Services – Reporting				
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.		☐	☐	☐
16-1.a Verify documented procedures exist for all key-loading operations.	Documented procedures reviewed:	*<Report Findings Here>*		
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>*		
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.		☐	☐	☐
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>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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>*		
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) verified key uniqueness between the two organizations: *<Report Findings Here>*			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
18-1.a Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.	Documented procedures reviewed:	*<Report Findings Here>*		
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 reviewed:	*<Report Findings Here>*		
18-2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.		☐	☐	☐
18-2.a Verify documented procedures require that key-component packaging/containers showing signs of tampering 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 reviewed:	*<Report Findings Here>*		
18-2.b Interview personnel and observe processes to verify 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.	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>			

Decryption Management Services – Reporting				
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*.		☐	☐	☐
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.	Documented procedures reviewed:	*<Report Findings Here>*		
	Describe how the observed key operations 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, or where key blocks are not implemented, identify and examine project plans to implement in accordance with the prescribed timeline.			
	<Report Findings Here>			
18-4 Not used in DMS				
18-5 Not used in DMS				
18-6 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
18-7 Not used in DMS				
19-1 Encryption keys must be used only for the purpose they were intended (i.e., key-encryption keys must not to be used as PIN-encryption keys, PIN-encryption keys must not be used for account data, etc.). 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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Key custodians interviewed:	*<Report Findings Here>*		
	Key-management supervisory personnel interviewed:	*<Report Findings Here>*		
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>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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 reviewed:	<*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).		☐	☐	☐
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 reviewed:	<*Report Findings Here*>		
	Key custodians interviewed:	<*Report Findings Here*>		
	Key-management supervisory personnel interviewed:	<*Report Findings Here*>		

Decryption Management Services – Reporting				
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: • Key used for production keys must never be present or used in a test system, and • Keys used for testing keys must never be present or used in a production system.		☐	☐	☐
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 development systems.	Key-management documentation reviewed:	*<Report Findings Here>*		
	Key custodians interviewed:	*<Report Findings Here>*		
	Key-management supervisory personnel interviewed:	*<Report Findings Here>*		
19-4.b Observe processes for generating and loading keys into in 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>			
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>			
19-4.d Compare check, hash, cryptogram, or fingerprint values for production and test/development keys for higher-level keys (e.g., 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>			

Decryption Management Services – Reporting				
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 key-injection 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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
19-6 Not used in DMS				
19-7 Not used in DMS				
19-8 Not used in DMS				
19-9 Not used in DMS				
19-10 Not used in DMS				
19-11 Not used in DMS				
19-12 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
20-1 POI devices must 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 that 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.		☐	☐	☐
20-1.a Examine documented procedures for the generation, 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 reviewed:	*<Report Findings Here>*		
20-1.b Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POIs 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>			
20-1.c Examine check values, hashes, 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 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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
20-2 If a POI device directly interfaces with more than one entity for decryption of account data (e.g., a different acquiring organization), the POI must have a completely different and unique key or set of keys for each acquiring organization. These different keys, or sets of keys, must be totally independent and not variants of one another.		☐	☐	☐
20-2 Determine whether POI devices are intended to interface with multiple entities for decryption.	Indicate whether POI devices are intended to interface with multiple entities for decryption (yes/no)	*<Report Findings Here>*		
If "no," describe how it was verified that POI devices are not intended to interface with multiple entities for decryption. (Leave 20-2.a to 20-2.c blank)		*<Report Findings Here>*		
If "yes", complete 20-2.a to 20-2.c:				
20-2.a Examine documented procedures for generating all types of keys and verify the procedures ensure that unique keys, or sets of keys, are used for each acquiring organization and are totally independent and not variants of one another.	Documented procedures reviewed:	*<Report Findings Here>*		
20-2.b Interview personnel and observe key-generation processes to verify that unique keys or sets of keys are generated for each acquiring organization.	Personnel interviewed:	*<Report Findings Here>*		
20-2.c Observe processes for generation and injection of keys into a single POI device for more than one acquiring organization, to verify: • The POI device has a completely different and unique key, or set of keys, for each acquiring organization. • These different keys, or sets of keys, are totally independent and not variants of one another.	Describe how the key-generation processes observed verified that unique keys or sets of keys are generated for each acquiring organization: *<Report Findings Here>*			

Decryption Management Services – Reporting				
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 the derivation of other keys once loaded—e.g., as done with DUKPT. ***Note**: The same BDK with the same KSN installed in multiple injection systems or installed multiple times within the same injection system will not meet uniqueness requirements.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Describe how the observed processes 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 device.			
	<Report Findings Here>			
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 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>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the observed key-injection processes for devices associated with different acquiring organizations verified that Base Derivation Key(s) unique to each organization are used:			
	<Report Findings Here>			
20-5 Not used in DMS				
20-6 Not used in DMS				

Decryption Management Services – Reporting				
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		☐	☐	☐
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.	Documented procedures reviewed:	*<Report Findings Here>*		
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.	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 Wherever key components/shares are used, they must have the following properties:		☐	☐	☐
21-2 Examine documented procedures and interview responsible personnel to determine all instances where key components/shares are used.	Documented procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
21-2.1 Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.		☐	☐	☐
21-2.1 Examine processes for creating key components/shares to verify that knowledge of any one key component/share must not convey any knowledge of any part of the actual cryptographic key.	Describe how the processes observed for creating key components verified that knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key: *<Report Findings Here>*			
21-2.2 Construction of the cryptographic key must require the use of at least two key components/shares.		☐	☐	☐
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/shares are required for each key construction: *<Report Findings Here>*			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Key custodians interviewed:	*<Report Findings Here>*		
	Key-management supervisory personnel interviewed:	*<Report Findings Here>*		
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/share access controls and key-custodian authorizations/assignments observed verified that all individuals with access to key components/shares are designated as key custodians for those particular components/shares:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
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 of a secret or private key to reconstruct a 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), as; and a second custodian (with, in this example, share C) would be required to reconstruct the final key, ensuring that dual control is maintained.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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/share 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:		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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.*		☐	☐	☐
21-3.1.a Examine key components and storage locations to verify that components are stored in individual opaque, pre-numbered tamper-evident 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 individual opaque, pre-numbered tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging: <*Report Findings Here*>			
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*>		
21-3.1.c Interview responsible personnel to determine that clear-text key components do not exist in non-secure containers, such as databases or in software programs.	Responsible personnel interviewed:	<*Report Findings Here*>		
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*>		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.*		☐	☐	☐
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/share storage container: • 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).	*<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.		☐	☐	☐
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>			
21-4 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
22-1 Procedures for known or suspected compromised keys must include the following:		☐	☐	☐
22-1 Verify documented procedures exist for replacing known or suspected compromised keys that include all of the following (22-1.1 through 22-1.5 below):	Documented procedures reviewed:	*<Report Findings Here>*		
22-1.1 Key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.		☐	☐	☐
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 has been compromised.	Responsible personnel interviewed:	*<Report Findings Here>*		
	Describe how the implemented processes observed verified that key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised:			
	<Report Findings Here>			
22-1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.		☐	☐	☐
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 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 has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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, 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, all the following are performed: • Use of 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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>*		
	Documented procedures reviewed:	*<Report Findings Here>*		
22-1.4.b Verify notifications include the following: • A damage assessment including, where necessary, the engagement of outside consultants. • Details of 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>*		

Decryption Management Services – Reporting				
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		☐	☐	☐
22-1.5 Interview responsible personnel and examine 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	Responsible personnel interviewed:	*<Report Findings Here>*		
	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
22-2.2 If attempts to load a secret key or key component into a KLD or POI 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		☐	☐	☐
22-2.2 Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into a KLD or POI 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.	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:			
	<Report Findings Here>			
22-3 Not used in DMS				
22-4 Not used in DMS				
22-5 Not used in DMS				

Decryption Management Services – Reporting				
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 PIN 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.*		☐	☐	☐
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>*		
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
23-2 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>*		
23-2.b Examine vendor documentation to determine support for key variants.	Vendor documentation reviewed:	*<Report Findings Here>*		
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 examination 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>			

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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 reviewed:	*<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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>*		
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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>			
24-2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic DB 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.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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 components—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>			

Decryption Management Services – Reporting				
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 custodian. The third-party witness must sign an affidavit of destruction, and this affidavit is retained for a minimum of two years.		☐	☐	☐
24-2.2.a Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian.	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>*		
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>*		
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.		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
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:		☐	☐	☐
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>*		

Decryption Management Services – Reporting				
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.		☐	☐	☐
25-1.1 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 observed for each component verified that: • A primary and a backup key custodian 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.		☐	☐	☐
25-1.2.a Examine completed key-custodian forms to verify that key custodians sign the form.	Completed key-custodian forms reviewed:	*<Report Findings Here>*		
25-1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form.	Completed key-custodian forms reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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 for the custodian's access • Signature of management authorizing the access		☐	☐	☐
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 for the custodian's access • Signature of management authorizing the access	Completed key-custodian forms reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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 such 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 and must sign key-custodian agreements that includes an attestation to the requirement.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Documented organization charts reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 reviewed:	*<Report Findings Here>*		
25-2 Not used in DMS				
25-3 Not used in DMS				
25-4 Not used in DMS				
25-5 Not used in DMS				
25-6 Not used in DMS				
25-7 Not used in DMS				
25-8 Not used in DMS				
25-9 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 • Tamper-evident package number (if applicable)		☐	☐	☐
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>*		
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 reviewed:	*<Report Findings Here>*		
	Describe how the audit log settings observed 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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
26-1.c Examine log files and verify they are: • Archived for a minimum of two years subsequent to key destruction • Securely stored	Log files reviewed:	*<Report Findings Here>*		
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 reviewed:	*<Report Findings Here>*		
	Describe how the audit log settings observed 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 • Name and signature of a non-custodian (for that component/share) witness • Tamper-evident and authenticable package number (if applicable)			
	<Report Findings Here>			
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.		☐	☐	☐
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.	Documented procedures reviewed:	*<Report Findings Here>*		
	Personnel interviewed:	*<Report Findings Here>*		
	Backup records reviewed:	*<Report Findings Here>*		
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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	Describe how the backup storage locations observed 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>			
27-2 If backup copies are created, the following must be in place: • Creation (including cloning) 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.		☐	☐	☐
27-2 Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies 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 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>			

Decryption Management Services – Reporting				
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 performed by a key-injection facilities 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		☐	☐	☐
28-1.a Examine documented procedures for key-administration operations to verify they 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 reviewed:	*<Report Findings Here>*		
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>*		
28-1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.	Personnel interviewed:	*<Report Findings Here>*		
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 DMS				
28-3 Not used in DMS				
28-4 Not used in DMS				
28-5 Not used in DMS				

Decryption Management Services – Reporting				
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.*		☐	☐	☐
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 processes reviewed:	*<Report Findings Here>*		
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.	*<Report Findings Here>*		

Decryption Management Services – Reporting				
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:		☐	☐	☐
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.		☐	☐	☐
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>*		
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>			
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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.*		☐	☐	☐
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 authorized by management in an auditable manner. • The authorizations are reviewed annually.	Documented authorizations reviewed:	*<Report Findings Here>*		
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.	Identify the P2PE Assessor who verified the access controls ensure only personnel documented and authorized in an auditable manner have access to devices.	*<Report Findings Here>*		
	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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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.	Documentation reviewed:	*<Report Findings Here>*		
29-1.2.b Observe implemented processes and interview personnel to verify that default keys or passwords are not used.	Personnel interviewed:	*<Report Findings Here>*		
	Identify the P2PE Assessor who verified the access controls ensure only personnel documented and authorized in an auditable manner have access to devices.	*<Report Findings Here>*		
29-2 Not used in DMS				

Decryption Management Services – Reporting				
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 in use. 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.		☐	☐	☐
29-3.a Examine documented procedures to confirm that 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>*		
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
29-4 Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle. 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 must not supplant the implementation of dual-control mechanisms.		☐	☐	☐
29-4.a Examine documented procedures to confirm 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 reviewed:	*<Report Findings Here>*		
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.	Responsible personnel interviewed:	*<Report Findings Here>*		
	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>*		
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 the manufacturer's invoice or similar document.*		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
29-4.1.b For a sample of received devices, examine sender documentation sent via a different communication channel than the devices 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>*		

Decryption Management Services – Reporting				
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 in account-data-processing equipment 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.		☐	☐	☐
29-4.2.a Obtain and review the defined security policy to be enforced by the HSM.	Documented security policy reviewed:	*<Report Findings Here>*		
29-4.2.b Examine documentation of the HSM configuration settings to determine that the functions and command authorized to be enabled are in accordance with the security policy.	HSM configuration settings documentation reviewed:	*<Report Findings Here>*		
29-4.2.c For a sample of HSMs, review 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				
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.	Documented procedures reviewed:	*<Report Findings Here>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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:		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
29-4.4.1 Running self-tests to ensure the correct operation of the device		☐	☐	☐
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 reviewed:	*<Report Findings Here>*		
	Describe how records of device inspections and test results 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		☐	☐	☐
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>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
29-4.3.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed		☐	☐	☐
29-4.3.3 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>			
29-4.4.4 Maintaining records of the tests and inspections, and retaining records for at least one year		☐	☐	☐
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>*		
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		☐	☐	☐
29-5.a Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.	Documented procedures reviewed:	*<Report Findings Here>*		
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				
30-3 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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: ***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.*		☐	☐	☐
31-1 Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all secret and private keys and key material stored within the device be securely destroyed. • Procedures cover all devices removed from service or for repair. • Procedures cover requirements at 31-1.1 through 31-1.6 below.	Documented procedures reviewed:	*<Report Findings Here>*		
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.		☐	☐	☐
31-1.1.a Examine documented procedures for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes.	Documented procedures reviewed:	*<Report Findings Here>*		
31-1.1.b Interview personnel and observe demonstration (if HSM is available) of processes for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes.	Personnel interviewed:	*<Report Findings Here>*		
	Describe how the demonstration verified that dual control is implemented for all critical decommissioning processes:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
31-1.2 Keys 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.		☐	☐	☐
31-1.2 Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material is 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 is rendered irrecoverable, or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys:			
	<Report Findings Here>			
31-1.3 SCDs being decommissioned are tested and inspected to ensure keys have been rendered irrecoverable.		☐	☐	☐
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 have been rendered irrecoverable or the devices are physically destroyed.	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.		☐	☐	☐
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.		☐	☐	☐
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>*		

Decryption Management Services – Reporting				
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 maintained for at least one year.		☐	☐	☐
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 Not used in DMS				
32-2 Not used in DMS				
32-3 Not used in DMS				
32-4 Not used in DMS				
32-5 Not used in DMS				
32-6 Not used in DMS				
32-7 Not used in DMS				
32-8 Not used in DMS				
32-9 Not used in DMS				

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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 by key-injection facilities on PIN-processing devices before they are placed into service, as well as devices being decommissioned.		☐	☐	☐
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 devices placed into service, initialized, deployed, used, and decommissioned,	Documented procedures reviewed:	*<Report Findings Here>*		
	Responsible personnel interviewed:	*<Report Findings Here>*		
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>*		

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>*		
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>			
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.		☐	☐	☐
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>*		
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>			

Decryption Management Services – Reporting				
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.		☐	☐	☐
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>*		
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>			

Decryption Management Services – Reporting				
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		☐	☐	☐
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>*		
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
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*)		☐	☐	☐
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>*		
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>*		

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5H-1.1 The Data Decryption Keys (DDKs) used in software to decrypt account data must have defined usage limits. This can be achieved through the use of either one of the following approaches: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in *NIST SP800-57, ISO TR 14742* and *NIST SP800-131.* The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). • Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the Host System. *OR* • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.		☐	☐	☐
5H-1.1.a Examine documented key-management policies and procedures to verify that DDKs managed on the Host System meet one or both of the following: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in *NIST SP800-57, ISO TR 14742* and *NIST SP800-131.* The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). • Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the host processing system. *OR* • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.1.b Observe the key-management methods used to manage DDKs on the Host System to verify they meet one, or both of the above options.	Describe how the key-management methods used to manage DDKs on the Host System meet one, or both, of the above options:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5H-1.2 DDKs must be erased from the Host System volatile memory via a mechanism that ensures the key cannot be recovered or reconstructed.		☐	☐	☐
5H-1.2.a Examine documented key-management policies and procedures to verify that the mechanism used to erase a DDK from the Host System volatile memory is sufficient to ensure the key cannot be recovered or reconstructed.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.2.b Verify, through the use of forensic tools and/or methods, that the mechanism used to erase the DDK from the host volatile memory, is sufficient to ensure the key cannot be recovered or reconstructed.	Describe the forensic tools and/or other methods used that verified that the mechanism used to erase the DDK from the host volatile memory, is sufficient to ensure the key cannot be recovered or reconstructed:			
	<Report Findings Here>			
5H-1.3 If the DDK is generated from a master key, the following conditions apply: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generate the DDK must be dedicated to generating DDKs.		☐	☐	☐
5H-1.3.a Examine key-management policies and procedures to verify that the following is required for any DDKs generated from a master key: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generated the DDK must be dedicated to generating DDKs.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.3.b Observe key-generation processes for generating DDKs from a master key to verify: • A one-way derivation process is used. • The DDK is never generated as a variant of the HSM master file key. • The master key used to generate the DDK is dedicated to generating DDKs.	Describe how the key-generation processes observed verified that: • A one-way derivation process is used. • The DDK is never generated as a variant of the HSM master file key. • The master key used to generate the DDK is dedicated to generating DDKs.			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5H-1.4 The DDK must be encrypted between the HSM and the Host System, e.g., using a fixed transport key or a cryptographic protocol. The method of encryption used must maintain the security policy to which the HSM was approved (either FIPS140-2, Level 3 or higher, or approved to the PCI HSM standard).		☐	☐	☐
5H-1.4.a Examine key-management policies and procedures to verify that DDKs must be encrypted between the HSM and the Host System.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.4.b Examine HSM and Host System configurations to verify that DDKs are encrypted between the HSM and the Host System.	Describe how the HSM and Host System configurations examined verified that DDKs are encrypted between the HSM and the Host System:			
	<Report Findings Here>			
5H-1.4.c Examine the HSM security policies and observe HSM implementations to verify that the method of encryption used maintains the security policy to which the HSM was approved.	Describe how the HSM security policies and HSM implementations examined verified that the method of encryption used maintains the security policy to which the HSM was approved:			
	<Report Findings Here>			
5H-1.5 The encryption mechanism used to protect the DDK between the HSM and the Host System:		☐	☐	☐
5H-1.5 Verify the encryption mechanism used to protect the DDK between the HSM and the Host System, includes 5H-1.5.1 through 5H-1.5.2 Perform the following:				
5H-1.5.1 The encryption key must be equal or greater in strength than the key it protects.		☐	☐	☐
5H-1.5.1.a Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is equal or greater in strength than the key it protects.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.5.1.b Observe key-management processes to verify the encryption mechanism used to protect the DDK between the HSM and the Host System uses an encryption key that is equal or greater in strength than the key it protects.	Describe how the key-management processes observed verified that the encryption mechanism used to protect the DDK between the HSM and the Host System uses an encryption key that is equal or greater in strength than the key it protects:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5H-1.5.2 The encryption key must be unique for each Host System.		☐	☐	☐
5H-1.5.2.a Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is unique for each Host System.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.5.2.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is unique for each Host System.	Describe how the key-management processes observed verified that the encryption mechanism uses an encryption key that is unique for each Host System:			
	<Report Findings Here>			
5H-1.5.3 The encryption key must only be used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.		☐	☐	☐
5H-1.5.3.a Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.5.3.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.	Describe how the key-management processes observed verified that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose:			
	<Report Findings Here>			

Decryption Management Services – Reporting				
Requirements and Testing Procedures	**Reporting Instructions**	**Assessor's Findings**		
		In Place	**N/A**	**Not In Place**
5H-1.5.4 The encryption key must have a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.		☐	☐	☐
5H-1.5.4.a Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.	Documented key-management policies and procedures reviewed:	*<Report Findings Here>*		
5H-1.5.4.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.	Describe how the key-management processes observed verified that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices:			
	<Report Findings Here>			