



Payment Card Industry (PCI) **Point-to-Point Encryption Key Management Services**

**Template for Report on Validation for use
with P2PE v3.0 for P2PE Key Management
Services Assessments**

December 2019

Document Changes

Date	Use with Version	Template Revision	Description
December 2019	P2PE v3.0	Revision 1.0	<p>To introduce the template for submitting P2PE Reports on Validation for P2PE Solutions and Components assessed against the P2PE v3.0 Standard for Key Management Services.</p> <p><i>This document serves as both the Reporting Template and Reporting Instructions document; there are not separate documents for this under P2PE v3.0.</i></p>

Contents

Document Changes	i
Introduction to the P-ROV Template for P2PE Key-Management Services	1
<i>P-ROV Sections 3</i>	
<i>P-ROV Summary of Findings</i>	3
<i>P-ROV Reporting Details</i>	4
Do's and Don'ts: Reporting Expectations	6
P-ROV Key Management Services Template for P2PE v3.0 Standard.....	7
1. Contact Information and Report Date	7
1.1 Contact Information	7
1.2 Date and timeframe of assessment.....	8
1.3 P2PE Version	8
2. Summary Overview	9
2.1 P2PE Assessment Details	9
2.2 Listed P2PE Component Providers used in the P2PE Solution/Component.....	10
2.3 Other Third-Party Service Provider entities involved in P2PE Solution/Component	10
2.4 All other Secure Cryptographic Devices (SCDs)	11
2.5 Summary of P2PE Compliance Status.....	11
3. Details and Scope of P2PE Assessment	12
3.1 Scoping Details	12
3.2 Key Management Services Diagram	12
3.3 Key-management processes	13
3.4 Facilities	15
3.5 Documentation Reviewed.....	16
3.6 Individuals Interviewed.....	16
3.7 Device Samples for P2PE Assessment.....	17
4. Findings and Observations	18
Key Management Services – Summary of Findings	18
Table 4.1 – Key Matrix. List of all cryptographic keys (by type) used in P2PE Solution/Component.....	27
P2PE Key Management Services – Reporting	27
Key Management Services – Reporting	27

Introduction to the P-ROV Template for P2PE Key-Management Services

This document, the *PCI Point-to-Point Encryption: Template for Report on Validation for use with P2PE v3.0 for Key Management Services*: (“Key Management Services P-ROV Reporting Template”), is the mandatory template for completing a P2PE Report on Validation (P-ROV) assessments against the *P2PE: Security Requirements and Testing Procedures, v3.0* (“P2PE v3.0 Standard”). This Reporting Template provides reporting instructions and the template form for QSA (P2PE) and PA-QSA (P2PE) assessors to provide a more consistent level of reporting among assessors.

Use of this Reporting Template is mandatory for all P2PE v3.0 Key Management Services Component Provider assessments (i.e., for a KIF, KMCP, KLCP, or a CA/RA assessment).

Use of this Reporting Template is mandatory for all P2PE v3.0 Solution (and MMS) assessments where the Solution Provider is directly responsible for all or part of the Key Management Services requirements (i.e., when they have not outsourced the entirety of their key management services to PCI-listed 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, or to change column width. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable but limited to the title page.

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

A P2PE compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The P-ROV is effectively a **summary of evidence** derived from the assessor’s work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the P-ROV provides a comprehensive **summary of testing activities performed and information collected** during the assessment against the P2PE v3.0 Standard. The information contained in a P-ROV must provide enough detail and coverage to verify that the P2PE submission is compliant with all applicable P2PE requirements.

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

SP = Solution Provider

CP = Component Provider

P-ROV Name	Used for the Following 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. Note: A separate Merchant-Managed Solution P-ROV is used as part of 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 POI devices in a P2PE Solution. Solution assessments that do not outsource the entirety of their Encryption Management Services to PCI-Listed Component Providers, either to an EMCP or to BOTH a PDCP AND a PMCP, must complete this P-ROV in addition to the Solution P-ROV. Component Provider assessments for an EMCP, PDCP, or a PMCP must complete this P-ROV.
P2PE Application	P2PE Application	Any assessment that utilizes software on the POI devices intended for use in a P2PE Solution that has the potential to access clear-text cardholder data must complete this P-ROV.
Decryption Management Services (DMS)	Solution (SP) Decryption Management CP (DMCP)	Decryption Management Services relates to the management of a decryption environment, including applicable devices (e.g., HSMs) used to support a P2PE Solution. Solution assessments that do not outsource the entirety of their Decryption Management Services to a PCI Listed DMCP must complete this P-ROV in addition to the Solution P-ROV. Component Provider assessments for a DMCP must complete this 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 key management services requirements (Domain 5) either through the use of PCI-listed Component Providers and/or through the assessment of their Encryption Management Services and/or Decryption Management Services must complete the KMS P-ROV. E.g., if the P2PE Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account-data encryption, or the operation of an applicable CA/RA, or any other relevant key management service that has not already been assessed as part of the inclusion of a PCI-listed Component Provider, then the Solution assessment must include the use of the KMS P-ROV. Component Provider assessments for a KIF, KMCP, KLCP, or a CA/RA must complete this P-ROV.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices may be added if the assessor feels

there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document. Personalization, such as the addition of company logos, is acceptable but limited to the title page.

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

A P2PE compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The P-ROV is effectively a **summary of evidence** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the P-ROV provides a **summary of testing activities performed and information collected** during the assessment of the P2PE Solution against the P2PE v3.0 Standard. The information contained in the submitted P-ROV(s) must provide enough detail and coverage to verify that the P2PE submission is compliant with all applicable P2PE requirements.

P-ROV Sections

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

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

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

P-ROV Summary of Findings

This version of the P2PE Reporting Template reflects an on-going effort to simplify assessor summary reporting. All summary findings for "In Place," "Not in Place," and "Not Applicable" are found at the beginning of 4. Findings and Observations and are only addressed at that high-level. A summary of all domain findings is also at "2.5 Summary of P2PE Compliance Status."

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

Response	When to use this Response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated. This may be a mix of In Place and Not Applicable responses, but no Not in Place response. Requirements fulfilled by other P2PE Components or Third Parties should be In Place, unless the requirement does not apply.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the P2PE Product. All Not Applicable responses require reporting on testing performed and must explain how it was determined that the requirement does not apply.

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 within each assessor response. As noted earlier, responses should be specific, but simple. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

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

- **“Identify the P2PE Assessor who confirms...”**
Indicates only an affirmative response where further reporting is deemed unnecessary by PCI SSC. The P2PE Assessor’s name or a Not Applicable response are the two appropriate responses here. A Not Applicable response will require brief reporting to explain how this was confirmed via testing.
- **Document name or interviewee reference**
At 3.5, “Documentation Reviewed,” and 3.6, “Individuals Interviewed,” there is a space for a reference number and **it is the P2PE Assessor’s choice** to use the document name/interviewee job title or the reference number in responses. A listing is sufficient here, no further detail required.
- **Sample reviewed**
Brief list is expected or sample identifier. Again, where applicable, it is the P2PE Assessor’s choice to list out each sample within reporting or to utilize sample identifiers from the sampling summary table.

- **Brief description/short answer – “Describe how...”**

These are the only reporting instructions that will stretch across half of the table; the above are all a quarter-table’s width to serve as a visual indicator of detail expected in response. These responses must be a narrative response that provides explanation as to the observation—both a summary of what was witnessed and how that verified the criteria of the testing procedure.

Do's and Don'ts: Reporting Expectations

DO:	DON'T:
<ul style="list-style-type: none"> ▪ Complete all applicable P-ROVs based on the assessment. ▪ 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 each 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. 	<ul style="list-style-type: none"> ▪ Don't report items in the “In Place” column unless they have been verified as being “in place.” ▪ Don't include forward-looking statements or project plans in responses. ▪ Don't simply repeat or echo the Testing Procedure in the response. ▪ Don't copy responses from one Testing Procedure to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment.

P-ROV Key Management Services Template for P2PE v3.0 Standard

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

1. Contact Information and Report Date

1.1 Contact Information

P2PE Solution/Component Provider contact information

Company name:		Company URL:	
Company contact name:		Contact e-mail address:	
Contact phone number:		Company address:	

P2PE Company and Lead Assessor contact information

Company name:		Assessor company credentials:	<input type="checkbox"/> QSA (P2PE)	<input type="checkbox"/> 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:	<input type="checkbox"/> QSA (P2PE)	<input type="checkbox"/> PA-QSA (P2PE)
Assessor phone number:		Assessor e-mail address:		
Confirm that internal QA was fully performed on the entire P2PE submission, per requirements in relevant program documentation.		<input type="checkbox"/> Yes <input type="checkbox"/> No (if no, this is not in accordance with PCI Program requirements)		
QA reviewer name:		Assessor credentials: (Leave blank if not applicable)		
QA reviewer phone number:		Assessor e-mail address:		

P2PE additional Assessor contact information (add additional rows as needed)

Assessor name:		Assessor credentials:	<input type="checkbox"/> QSA (P2PE)	<input type="checkbox"/> PA-QSA (P2PE)
Assessor phone number:		Assessor e-mail address:		

1.2 Date and timeframe of assessment

Date of Report:

Timeframe of assessment:

1.2.a Additional services provided by PA-QSA(P2PE)/QSA (P2PE)/QSA company

The P2PE QSA (P2PE) and PA-QSA (P2PE) Qualification Requirements v2.1, Section 2.2 “Independence” specifies requirements for QSAs around disclosure of such services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the sections below after review of this portion of the Validation Requirements, to ensure responses are consistent with documented obligations.

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

1.3 P2PE Version

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

2. Summary Overview

2.1 P2PE Assessment Details

Is this P-ROV assessment being submitted as part of a Solution assessment?	<input type="checkbox"/> Yes	If Yes , please enter Solution Name. If any PCI-listed KMS Component Providers are being used in the Solution complete Table 2.2.	Solution Name
	<input type="checkbox"/> No	If No (this is a Component Provider assessment ONLY), complete Part A. Also complete Table 2.2 for any PCI-listed KMS Components are being used.	<Solution Name>

P2PE Component Details – Part A

P2PE Component name:		Is the Component already listed on the PCI SSC List of Validated P2PE Components?	<input type="checkbox"/> Yes (if yes, provide ref #)	<input type="checkbox"/> No
			PCI SSC Ref #	

P2PE Component Type. Please select only **one** of the following:

<input type="checkbox"/> KIF	<input type="checkbox"/> Key Management Component Provider (KMCP)
<input type="checkbox"/> Key Loading Component Provider (KLCP)	<input type="checkbox"/> CA/RA

Notes: Within Section 4, “Findings and Observations,” applicable requirements are identified as follows (KLCP, KMCP, KIF, CA/RA, RKD and SP).

2.2 Listed P2PE Component Providers used in the P2PE Solution/Component

Are any PCI-listed KMS Component Providers used in the P2PE Solution/Component?

Yes No

If 'no,' the remainder of this table (2.2) is not required.

Description of how other P2PE Component Providers are used:

Type of Component (select one per row)				P2PE Component Provider Name	P2PE Component Name	PCI SSC Reference #
KLCP	KMCP	KIF	CA/RA			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

2.3 Other Third-Party Service Provider entities involved in P2PE Solution/Component

This could include Key Management Services who have opted NOT to list with PCI SSC as a P2PE Component and therefore must be assessed fully for each P2PE Component in which the service is used. This could also include other third-party service providers in use as applicable.

“Other details” is to be used as needed. For example, if there is a third-party service provider providing Key Management Services but it is not a P2PE Component at 2.2, use “Other details” to address data. Mark as “N/A” if no other details are needed.

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

2.4 All other Secure Cryptographic Devices (SCDs)

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

This includes SCDs used to generate or load cryptographic keys, encrypt keys, or sign applications to be loaded onto POI devices, as well as HSMs used in the P2PE decryption environment. Examples include HSMs, key-injection/loading devices (KLDs), and other devices that generate or load keys or sign applications and/or whitelists.

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

2.5 Summary of P2PE Compliance Status

P2PE Function	Compliant	Comments (optional):
Key Management Services		
Solution Provider (or MMS as a Solution Provider)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
KIF	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
Key Management Component Provider	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
Key Loading Component Provider	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
Remote Key Distribution using Asymmetric Techniques	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	
CA/RA	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	

3. Details and Scope of P2PE Assessment

3.1 Scoping Details

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

- Describe the methods or processes used to identify all elements in scope of the P2PE assessment:
- Describe how the P2PE assessor confirmed that the scope of the assessment is accurate and covers all components and facilities for Key Management Services:

3.2 Key Management Services Diagram

Provide one or more ***high-level*** diagrams to illustrate the functioning of the P2PE Key Management Services, including:

- Locations of critical facilities
- Location of systems performing key-management functions



<Insert Key Management Services high level diagram(s)>

3.3 Key-management processes

Description of Cryptographic Key-Management Processes

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

- Key Generation
- Key Distribution / Loading / Injection onto POI devices
- Other Key Distribution / Loading / Injection activities
- Key Storage
- Key Usage
- Key Archiving (if applicable)

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



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

Description of Cryptographic Keys used in Key Management Services

Provide a brief description* of all types of cryptographic keys used in the Key Management Service, as follows:

Key type/description	Purpose/function of the key

Note: A detailed Key Matrix is included in Findings and Observations, below.

3.4 Facilities

Lab environment used by the P2PE Assessor for this assessment

Identify whether the lab was provided by the P2PE Assessor or the Solution/Component Provider:

P2PE Assessor's Lab Solution/Component Provider's Lab

Address of the lab environment used for this assessment:

Describe the lab environment used for this assessment:

List of all facilities INCLUDED in this assessment

Description and purpose of facility included in assessment	Address of facility

List of facilities used in P2PE Solution/Component that were EXCLUDED from this assessment*

Description and purpose of facility excluded from assessment	Address of facility	Explanation why the facility was excluded from the assessment	Details of any separate assessments performed for the facility, including how the other assessment was verified to cover all Solution/Components in scope for this Solution/Component

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

3.5 Documentation Reviewed

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

All documentation reviewed for this P2PE Assessment:

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

3.6 Individuals Interviewed

List of all personnel interviewed for this Assessment:

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

3.7 Device Samples for P2PE Assessment

Complete for all sampled devices in the P2PE assessment, including every SCD type at Section 2.4 above.

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

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

4. Findings and Observations

Key Management Services – Summary of Findings

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

Abbreviations:	
KLCP Key Loading Component Provider	KMCP Key Management Component Provider
KIF Key Injection Facility	CA/RA Certification Authority/Registration Authority
SP Solution Provider (or MMS as a Solution Provider)	RKD Remote Key Distribution

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
DOMAIN 5									
Applies to:						Control Objective 1: Account data is processed using equipment and methodologies that ensure they are kept secure.			
Not used in P2PE						1-1		<input checked="" type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				1-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	1-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				1-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
Requirements 2, 3 and 4 are not used in P2PE.									
Applies to:						Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys			
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	5-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	6-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	7-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	7-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Control Objective 3: Keys are conveyed or transmitted in a secure manner			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	8-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	8-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	8-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	8-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	9-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	10-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not used in P2PE						10-2		<input checked="" type="checkbox"/>	
Not used in P2PE						10-3		<input checked="" type="checkbox"/>	
Not used in P2PE						10-4		<input checked="" type="checkbox"/>	
Not used in P2PE						10-5		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	11-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		11-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner			
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	12-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	12-8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				12-9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	12-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	13-9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	14-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	14-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	14-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	14-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	14-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	15-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	15-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		15-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		15-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		15-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	16-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	16-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage			

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
					<input checked="" type="checkbox"/>	17-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	18-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	18-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		18-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		18-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				18-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				18-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				18-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	19-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	19-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	19-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	19-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	19-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		19-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		19-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input checked="" type="checkbox"/>		19-8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			19-9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			19-10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			19-11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			19-12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	20-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	20-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	20-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	20-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				20-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				20-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Control Objective 6: Keys are administered in a secure manner			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	21-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	21-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	21-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		21-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	22-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	22-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			22-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			22-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			22-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	23-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	23-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	23-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	24-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	24-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	25-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
			<input checked="" type="checkbox"/>			25-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			25-9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	26-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	27-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	27-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	28-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			28-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			28-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			28-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			28-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Control Objective 7: Equipment used to process account data and keys is managed in a secure manner			
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	29-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			29-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	29-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	29-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Key Management Services: P2PE Validation Requirements							Summary of Findings (check one)		
KMCP	KLCP	KIF	CA/RA	RKD	SP	Control Objective and Requirements	In Place	N/A	Not in Place
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	29-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not used in P2PE						30-1		<input checked="" type="checkbox"/>	
Not used in P2PE						30-2		<input checked="" type="checkbox"/>	
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				30-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	31-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	32-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input checked="" type="checkbox"/>			32-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				32-8 (8.1, 8.2)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				32-8 (8.3 – 8.7)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				32-9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	33-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Requirement 5A: Account data is processed using algorithms and methodologies that ensure they are kept secure			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	5A-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applies to:						Requirement 5I: Component providers ONLY: report status to solution providers			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			5I-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 4.1 – Key Matrix. List of all cryptographic keys (by type) used in P2PE Solution/Component

Key type/ description:	Algorithm – e.g., TDEA, AES, RSA	Cryptographic Mode(s) of Operation (as applicable)	Full Key Length (bits)	Purpose/function of the key (including types of devices using key):	Key-creation method:	How key is distributed – e.g., manually via courier, and/or via remote key distribution (RKD).	Types of media used for key storage:	Method of key destruction:

P2PE Key Management Services – Reporting

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
DOMAIN 5			
1-1 Not used in P2PE			
KIF KLCP	1-2 Key-injection facilities must only inject keys into equipment that conforms to the requirements for SCDs.		
KIF KLCP	1-2.a Examine documented procedures and system documentation to verify that key-injection platforms and systems used for managing cryptographic keys are required to conform to the requirements for SCDs.	Documented procedures reviewed:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>1-3 All hardware security modules (HSMs) must be either:</p> <ul style="list-style-type: none"> FIPS140-2 or 140-3 Level 3 or higher certified, or PCI approved <p>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.</p>			
CA/RA KIF KMCP KLCP SP	<p>1-3.a For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval), and examine the list of approved devices to verify that all HSMs are either:</p> <ul style="list-style-type: none"> Listed on the <i>NIST Cryptographic Module Validation Program (CMVP)</i> list, with a valid listing number, and approved to FIPS 140-2 or 140-3 Level 3, or higher. Refer to http://csrc.nist.gov. Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class “HSM.” Refer to https://www.pcisecuritystandards.org. 	Approval documentation examined:	<Report Findings Here>
<p>1-4 The approval listing must match the deployed devices in the following characteristics:</p> <ul style="list-style-type: none"> 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 			
CA/RA KIF	1-4.a For all PCI-approved HSMs used, examine HSM devices and examine the PCI SSC list of Approved PCI	For each PCI-approved HSM used, describe how the observed HSM device configurations verified that all of the device characteristics at 6A-1.4.a match the PTS listing:	

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KMCP KLCP SP	PTS Devices to verify that all of the following device characteristics match the PCI PTS listing for each HSM: <ul style="list-style-type: none"> • 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 	<Report Findings Here>	
SP CA/RA KIF KMCP KLCP	1-4.b For all FIPS-approved HSMs used, examine HSM devices and review the <i>NIST Cryptographic Module Validation Program (CMVP)</i> 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: <ul style="list-style-type: none"> • Vendor name • Model name/number • Hardware version number • Firmware version number • The FIPS 140 Approval Number 	For each FIPS-approved HSM used, describe how the observed HSM device configurations verified that all of the device characteristics at 6A-1.4.b match the FIPS140-2 Level 3 (or higher) approval listing:	
		<Report Findings Here>	
1-5 The documentation should indicate how personnel interaction and inventory management of KIF components are integrated into the flow. The KIF platform provider must: <ul style="list-style-type: none"> • Maintain current documentation that describes or illustrates the architecture of the KIF, including all KIF functionality. • Maintain documentation detailing the flow of keys from the key generation, through the functionality to the destination device. 			
KIF KMCP KLCP	1-5.a Interview relevant personnel and examine documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the KIF.	Relevant personnel interviewed:	<Report Findings Here>
		Documented procedures examined:	<Report Findings Here>
KIF KMCP KLCP	1-5.b Interview relevant personnel and examine documentation that describes and/or illustrates the architecture of the KIF to verify that all KIF components, key-management flows, and personnel interaction with key-management flows are identified and documented.	Relevant personnel interviewed:	<Report Findings Here>
		Documented procedures examined:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KMCP KLCP	<p>1-5.c Examine the key-management flows and interview personnel to verify:</p> <ul style="list-style-type: none"> Documentation shows all key-management flows across functions and networks from the point the key is generated through to the point the key is injected into the POI. Documentation is kept current and updated as needed upon changes to the KIF architecture 	Documented key-management flows examined:	<Report Findings Here>
Requirements 2, 3 and 4 are not used in P2PE			
<p>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:</p> <ul style="list-style-type: none"> An approved key-generation function of a PCI-approved HSM or POI device An approved key-generation function of a FIPS 140-2 or 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 <i>NIST SP800-22</i> <p>Note: <i>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.</i></p>			
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> An approved key-generation function of a PCI-approved HSM or POI device An approved key-generation function of a FIPS 140-2 or 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 <i>NIST SP 800-22</i> 	Documented POI configuration and deployment procedures examined:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> An approved key-generation function of a PCI-approved HSM or POI device An approved key-generation function of a FIPS 140-2 or 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 <i>NIST SP 800-22</i> 	Certification Letters/technical documentation examined:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>5-1.c Examine procedures to be used for future generations and/or logs of past key generation to verify devices used for key-generation are those as noted above, including validation of firmware used.</p>	Identify the P2PE Assessor who confirms that devices used for key-generation are those noted above, including validation of firmware used.	<Report Findings Here>
<p>6-1 Implement security controls, including dual control and tamper detection, to prevent the unauthorized disclosure of keys or key components.</p>			
<p>6-1.1 Any clear-text output of the key-generation process must be managed under dual control. Only the assigned custodian can have direct access to the clear text of any key component/share. Each custodian's access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian, and not to the entire key.</p>			
CA/RA KIF KMCP SP	<p>6-1.1.a Examine documented procedures to verify the following.</p> <ul style="list-style-type: none"> Any key-generation process with clear-text output is performed under dual control Any output of a clear-text component or share is overseen by only the assigned key custodian(s) for that component/share Each custodian's access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian, and not the entire key 	Documented procedures examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>6-1.1.b Observe key-generation process demonstration and interview responsible personnel to verify:</p> <ul style="list-style-type: none"> 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 	Describe how the key generation processes observed verified that any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key:	<Report Findings Here>
<p>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.</p> <p>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.</p>			
CA/RA KIF KMCP SP	<p>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.</p>	Describe how the end-to-end process observed verified that there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>6-1.2.b Examine key-generation logs to verify that:</p> <ul style="list-style-type: none"> The documented procedures were followed, and At least two individuals performed the key-generation processes. 	Key-generation logs reviewed:	<Report Findings Here>
<p>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.</p> <p>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.</p>			

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>6-1.3.a Examine documented procedures for all key-generation methods. Verify procedures require that:</p> <ul style="list-style-type: none"> Key-generation devices that generate clear-text key components are powered off when not in use or require re-authentication whenever key generation is invoked; or If the device used for key generation is logically partitioned for concurrent use in other processes, the key-generation capabilities are enabled for execution of the procedure and disabled when the procedure is complete. 	Documented key-generation procedures examined:	<Report Findings Here>
<p>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.</p> <p>Note: This does not apply to logically partitioned devices located in data centers that are concurrently used for other purposes, such as transaction processing.</p>			
CA/RA KIF KMCP SP	<p>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).</p>	Documented key-generation procedures examined:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>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).</p>	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>
<p>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.</p>			
CA/RA KIF KMCP SP	<p>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.</p>	Documentation examined:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
SP CA/RA KIF KMCP	6-1.5.b During the demonstration for 6-1.1.b, observe the physical security controls (e.g., partitions or barriers) used, and validate that they ensure the key-generation process cannot be observed or accessed by unauthorized personnel directory or via camera monitoring (including those on cellular devices).	Describe how the physical security controls observed verified that key-component/key-generation process cannot be observed or accessed by unauthorized personnel: <Report Findings Here>	
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>SCDs used for key generation must meet Requirement 5-1.</p> <p>Note: See Requirement 5 and Requirement 13.</p>			
CA/RA KIF KMCP SP	6-2.a Examine documented procedures to verify that multi-purpose computing systems are not permitted for key generation where any clear-text secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP SP	6-2.b Observe the generation process and examine documentation for each type of key to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD except where Requirement 5 and Requirement 13 are met.	Vendor documentation reviewed for each type of key:	<Report Findings Here>
		Describe how the generation process observed for each type of key verified that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory:	
		<Report Findings Here>	
CA/RA KIF KMCP SP	6-2.c Where single-purpose computers with an installed SCD or a modified PED are used, verify that either: <ul style="list-style-type: none"> Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) or 	Describe how the single-purpose computers with an installed SCD verified that either: <ul style="list-style-type: none"> Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) or Where clear keying material passes through unprotected memory of the PC, the PC requirements of Requirement 13 are met. 	

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<ul style="list-style-type: none"> Where clear keying material passes through memory of the PC, the PC requirements of Requirement 13 are met. 	<Report Findings Here>	
<p>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:</p> <ul style="list-style-type: none"> Only approved key custodians can observe the key component. Tampering can be visually detected. <p>Printers used for this purpose must not be used for other purposes, must not be networked (i.e., locally connected), and must be managed under dual control, including use of a secure room that meets the requirements of 32-9.</p>			
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> Only approved key custodians can observe their the key component. Tampering can be visually detected. Printers used for this purpose are not used for other purposes, are managed under dual control in a secure room that meets the requirements of 32-9 and are not networked. 	Documented procedures for printed key components examined:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>6-3.b Observe processes for printing key components to verify that :</p> <ul style="list-style-type: none"> 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 used only under dual control and only within a secure room that meets the requirements of 32-9; and Printers are not networked 	Describe how processes observed for printing key components verified that key components are printed within blind mailers or sealed immediately after printing, such that no one but the authorized custodian ever has physical access to the output:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	6-3.c Observe blind mailers, tamper-evident and authenticable, or other sealed containers used for key components to verify that components cannot be read from within and that tampering can be visually detected.	Describe how the blind mailers or other sealed containers used for key components observed verified that tampering can be visually detected:	
		<Report Findings Here>	
<p>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.</p> <p><i>Examples of where such key residue may exist include (but are not limited to):</i></p> <ul style="list-style-type: none"> • <i>Printing material, including ribbons and paper waste</i> • <i>Memory storage of a key-loading device, after loading the key to a different device or system</i> • <i>Other types of displaying or recording (e.g., printer memory, printer drum)</i> 			
CA/RA KIF KMCP SP	<p>6-4.a Examine documented procedures to identify all locations where key residue may exist. Verify procedures ensure the following:</p> <ul style="list-style-type: none"> • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • Specific direction as to the method of destruction is included in the procedure. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device(s) that will use the key. • Examine logs of past destructions and deletions to verify that procedures are followed. 	Documented procedures examined:	<Report Findings Here>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>6-4.b Observe the destruction process of each identified type of key residue and verify the following:</p> <ul style="list-style-type: none"> 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. <p>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.</p>	Describe how the destruction process of the identified key residue observed verified that any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation:	
		<Report Findings Here>	
		Identify the P2PE Assessor who confirms that the method of destruction is consistent with Requirement 24 .	<Report Findings Here>
		If a key is generated in a separate device before being exported into the end-use device, describe how the destruction process of the identified key residue observed verified that the key and all related critical security parameters are deleted from the generation and/or injection device immediately after the transfer to the device that will use the key:	
<Report Findings Here>			
<p>6-5 Asymmetric-key pairs must either be:</p> <ul style="list-style-type: none"> 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. 			
CA/RA KIF KMCP SP	<p>6-5.a Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either:</p> <ul style="list-style-type: none"> Generated by the device that will use the key pair, or If generated externally, the key pair and all related critical security parameters are deleted (zeroized) immediately after the transfer to the device that will use the key pair. 	Documented procedures for asymmetric-key generation examined:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>6-5.b Observe key-generation processes to verify that asymmetric-key pairs are either:</p> <ul style="list-style-type: none"> 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:	
		<ul style="list-style-type: none"> 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>			

Key Management Services – Reporting		
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings
<p>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:</p> <ul style="list-style-type: none"> • 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 		
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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 	<p>Documented policy and procedures examined:</p> <p><i><Report Findings Here></i></p>

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> 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 	<p>Describe how the key-management processes observed verified that key components are not transmitted across insecure channels, including but not limited to:</p> <ul style="list-style-type: none"> 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>	
<p>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.</p>			
CA/RA KIF KMCP SP	<p>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.</p>	Documented key-generation procedures examined:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>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.</p>	Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>7-1.c Observe key-generation ceremonies, whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.</p>	Describe how the observation of actual or demonstrative key-generation ceremonies verified that the documented procedures are demonstrably in use:	
		<Report Findings Here>	

Key Management Services – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
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.			
CA/RA KIF KMCP SP	7-2.a Examine documented key-generation procedures to verify that key-generation events for higher-level keys (e.g., KEKs shared with other organizations or otherwise manually loaded as components and MFKs and BDks) are logged.	Documented key-generation procedures examined:	<Report Findings Here>
CA/RA KIF KMCP SP	7-2.b Observe demonstrations for the generation of higher-level keys to verify that all key-generation events are logged.	Describe how the demonstrations for all types of key-generation events observed verified that all key-generation events are logged:	
		<Report Findings Here>	
CA/RA KIF KMCP SP	7-2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded and that all required elements were captured.	Key generation logs examined:	<Report Findings Here>

Key Management Services – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<p>8-1 Keys must be transferred either encrypted, as two or more full-length clear-text components, key shares, or within an SCD.</p> <ul style="list-style-type: none"> • 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. <p>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.</p>		
CA/RA KIF KMCP KLCP SP	<p>8-1.a Determine whether keys are transmitted encrypted, as clear-text components/shares, or within an SCD.</p>	Identify the P2PE Assessor who determined whether keys are transmitted encrypted, or as clear-text components, or within an SCD:	<p><Report Findings Here></p>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>8-1.b If key components are transmitted in clear text using pre-numbered, tamper-evident, authenticable packaging, perform the following:</p> <ul style="list-style-type: none"> • Examine documented procedures for sending components in tamper-evident, authenticable packaging to verify that: <ul style="list-style-type: none"> – They define how the details of the package serial number are to be transmitted. – There is a requirement that the package serial number is to be sent separately from the package itself. – Each component is to be sent to/from only the custodian(s) authorized for the component. – At least two communication channels are used to send the components of a given key (not just separation by sending on different days). – Prior to the use of the components, the serial numbers are to be confirmed. • Confirm through observation, interview, and inspection of the records of past key transfers that the process used to transport clear-text key components using pre-numbered, tamper-evident, authenticable packaging, is sufficient to ensure: <ul style="list-style-type: none"> – 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. 	Documented procedures reviewed:	<Report Findings Here>
		Records of key conveyances examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
		Describe how the observed method to transport clear-text key components using tamper-evident mailers verified that details of the serial number of the package are transmitted separately from the package itself:	
		<Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	8-1.c Where SCDs are used to convey components/shares: <ul style="list-style-type: none"> Examine documented procedures to verify that the mechanism to obtain the keying material (e.g., PIN) is conveyed using a separate communication channel from the associated SCD. Examine documented procedures to verify that each SCD is inspected to ensure that there are not any signs of tampering. Examine the chain-of-custody document for the SCDs and any transport logs to ensure the movement of each device is tracked and that there is evidence that the SCDs and dual-control mechanisms were separated sufficiently to ensure that no one person gained access to the SCDs and both SCD enablers. 	Documented procedures examined:	<Report Findings Here>
		Records of key conveyances examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	8-1.d Where an SCD is conveyed with pre-loaded secret and/or private keys, perform the following: <ul style="list-style-type: none"> Examine documented procedures to verify that the SCD requires dual-control mechanisms to become operational. Examine the documented procedures to ensure the method of shipment of the SCD and dual-control mechanisms (e.g., smart cards or passphrases) are separated in a way that ensures there is no opportunity for one person to gain access to the SCD and both authorization mechanisms (e.g., both smartcards, etc.). Examine documented procedures to verify that the SCD is inspected to ensure there are no signs of tampering. Examine records of key transfers and interview responsible personnel to verify the mechanisms that make the SCD operational are conveyed using separate communication channels. 	Documented procedures examined:	<Report Findings Here>
		Records of key conveyances examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>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.</p> <p>Note: An <i>m-of-n</i> scheme is a component- or share-allocation scheme where <i>m</i> is the number of shares or components necessary to form the key, and <i>n</i> 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</p> <p><i>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.</i></p>			
CA/RA KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • Designation of person(s) permitted to convey/receive keys. • Reminder that any person with access to one component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component or shares sufficient to form the necessary threshold to derive the key. • Steps to ensure any person with access to the media conveying a component/share of a key could not have access to other components/shares of this key, or to any other medium conveying any other component of this key that is sufficient to form the necessary threshold to derive the key, without detection. 	Documented device-configuration procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> An individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying other components or shares of this key that are sufficient to form the necessary threshold to derive the key. Any person with access to the media conveying a key component or key share must not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key. 	
		<Report Findings Here>	
CA/RA KIF KMCP KLCP SP	<p>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.</p>	Logs examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
<p>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.</p> <p>Other similar mechanisms, such as SMS, fax, or telephone must not be used to convey clear-text key values.</p>			
CA/RA KIF KMCP KLCP SP	8-3.a Validate through interviews, observation, and log inspection that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components/shares.	Personnel interviewed:	<i><Report Findings Here></i>
		Logs reviewed:	<i><Report Findings Here></i>
		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:	
		<i><Report Findings Here></i>	
<p>8-4 Public keys must be conveyed in a manner that protects their integrity and authenticity.</p> <p>Examples of acceptable methods include:</p> <ul style="list-style-type: none"> Use of public-key certificates as defined in within this Domain that are created by a trusted CA that meets the applicable requirements of this Domain Validating a hash of the public key sent by a separate channel (e.g., mail) Using a MAC (message authentication code) created using the algorithm defined in <i>ISO 16609</i> Conveyance within an SCD Encrypted <p>Note: <i>Self-signed certificates must not be used as the sole method of authentication.</i></p> <p><i>Self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data. The authenticity of the root certificate is based on the use of secure procedures to distribute them. Specifically, they must be directly installed into the PIN pad of the ATM or POS device and not remotely loaded to the device subsequent to manufacture.</i></p> <p>For all methods used to convey public keys, perform the following:</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>ISO 16609</i> • Conveyance within an SCD • Encrypted 	<p>Documented procedures examined:</p> <p><Report Findings Here></p>	
CA/RA KIF KMCP KLCP SP	<p>8-4.b Validate that procedures dictate that self-signed certificates must not be used as the sole method of authentication.</p>	<p>Identify the P2PE Assessor who attests that self-signed certificates must not be used as the sole method of authentication:</p>	<p><Report Findings Here></p>
CA/RA KIF KMCP KLCP SP	<p>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.</p>	<p>Responsible personnel interviewed:</p>	<p><Report Findings Here></p>
<p>9-1 During the process to convey it, any single clear-text secret or private key component/share must at all times be either:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> • Under the continuous supervision of a person with authorized access to this component, • Sealed in a security container or courier mailer (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or • Contained within a physically secure SCD. 	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> 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>
		<p>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:</p> <ul style="list-style-type: none"> Under the continuous supervision of a person with authorized access to this component Locked in a security container (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or Contained within a physically secure SCD. 	
		<Report Findings Here>	
<p>9-2 Packaging or mailers (i.e., pre-numbered, tamper-evident packaging) containing clear-text key components are examined for evidence of tampering before being opened. Any sign of package tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the destruction and replacement of:</p> <ul style="list-style-type: none"> The set of components Any keys encrypted under this (combined) key 			
CA/RA KIF KMCP SP	9-2.a Verify documented procedures include requirements for all packaging or mailers containing clear-text key components to be examined for evidence of tampering before being opened.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KMCP SP	9-2.b Interview responsible personnel and observe processes to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being opened.	Responsible personnel interviewed:	<Report Findings Here>
		<p>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:</p> <p><Report Findings Here></p>	

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	9-2.c Verify documented procedures require that any sign of package tampering is identified, reported, and ultimately results in the destruction and replacement of both: <ul style="list-style-type: none"> • The set of components • Any keys encrypted under this (combined) key 	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KMCP SP	9-2.d Interview responsible personnel and observe processes to verify that if a package shows signs of tampering indicating a component was potentially compromised, processes are implemented to identify the tampering, report/escalate it, and ultimately result in the destruction and replacement of both: <ul style="list-style-type: none"> • The set of components, and • Any keys encrypted under this (combined) key 	Responsible personnel interviewed :	<Report Findings Here>
		Describe how the process observed verified that if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: <ul style="list-style-type: none"> • The set of components • Any keys encrypted under this (combined) key 	
		<Report Findings Here>	
CA/RA KIF KMCP SP	9-2.e Examine records related to any escalated transmittal events. Verify that it resulted in the destruction and replacement of both: <ul style="list-style-type: none"> • The set of components • Any keys encrypted under this (combined) key 	Documented records examined:	<Report Findings Here>
9-3 Only an authorized key custodians—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.			
CA/RA KIF KMCP SP	9-3.a Verify the existence of a list(s) of key custodians—and designated backup(s)—authorized to have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.	Documented reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KMCP SP	9-3.b Observe implemented access controls and processes to verify that only those authorized key custodians—and designated backup(s)—have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.	Describe the implemented access controls and processes observed that verified that only those authorized key custodians (and designated backup(s)) have physical access to key components prior to being secured in transmittal packaging:	
CA/RA KIF KMCP SP		<Report Findings Here>	
CA/RA KIF KMCP SP	9-3.c Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each component.	Physical access logs examined:	<Report Findings Here>
9-4 Mechanisms must exist to ensure that only authorized custodians: <ul style="list-style-type: none"> Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal. Check tamper-evident packaging upon receipt for signs of tampering prior to opening tamper-evident authenticable packaging containing key components. Check the serial number of the tamper-evident packaging upon receipt of a component package. Note: See Requirement 26 for logging.			
CA/RA KIF KMCP SP	9-4.a Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: <ul style="list-style-type: none"> Place the key component into pre-numbered tamper-evident packaging for transmittal. Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. Check the serial number of the tamper-evident packaging upon receipt of a component package. 	Documented reviewed:	<Report Findings Here>
CA/RA KIF KMCP SP	9-4.b Observe implemented mechanisms and processes and examine logs to verify that only the authorized key custodians can perform the following: <ul style="list-style-type: none"> Place the key component into pre-numbered tamper-evident packaging for transmittal. 	Describe how the implemented mechanisms and processes observed verified that only the authorized key custodians can perform the following: <ul style="list-style-type: none"> Place the key component into pre-numbered tamper-evident packaging for transmittal. Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. Check the serial number of the tamper-evident packaging upon receipt of a component package. 	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<ul style="list-style-type: none"> Upon receipt, check the tamper-evident packaging for signs of tampering prior to opening the tamper-evident packaging containing the key component. Check the serial number of the tamper-evident packaging upon receipt of a component package. 	<Report Findings Here>	
<p>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.</p> <p>Note: Numbered courier bags are not sufficient for this purpose.</p>			
CA/RA KIF KMCP SP	<p>9-5 Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following:</p> <ul style="list-style-type: none"> Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. Examine logs to verify that procedures are followed. 	Documented procedures reviewed:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
		Describe how the observed method used to transport clear-text key components using tamper-evident mailers verified that details of the serial number of the package are transmitted separately from the package itself:	
		Documented procedures reviewed:	
		<Report Findings Here>	
<p>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:</p> <ul style="list-style-type: none"> 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. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	<p>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:</p> <ul style="list-style-type: none"> • The components inside the tamper-evident and authenticable package are in separate opaque and identifiable packaging (e.g., individually sealed within labeled, opaque envelopes or within PIN mailers) to prevent confusion and/or inadvertent observation when the package is opened. • The components are repackaged at receipt into separate tamper-evident and authenticable packages for storage at the receiving location. • Records reflect the receipt of the shipped bag and association with subsequent individual bags. 	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KMCP SP	<p>9-6.b Examine logs to verify that procedures are followed.</p>	Logs reviewed:	<Report Findings Here>
<p>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.</p> <ul style="list-style-type: none"> • TDEA keys used for encrypting keys must be at least triple-length keys (have bit strength of 112 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. • A triple-length TDEA key must not be encrypted with a TDEA key of lesser strength. • TDEA keys must not be used to protect AES keys. • TDEA keys must not be used to encrypt keys greater in strength than 112 bits. • RSA keys encrypting keys greater in strength than 80 bits shall must have a bit strength of at least 112 bits. 			
KIF KMCP KLCP SP	<p>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).</p>	Documented procedures reviewed:	<Report Findings Here>

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KMCP KLCP SP	<p>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).</p>	Appropriate Personnel interviewed:	<Report Findings Here>
		Documented procedures reviewed:	<Report Findings Here>
KIF KMCP KLCP SP	<p>10-1.c Observe key-generation processes for the key types identified above. Verify that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed, except as noted for RSA keys. To verify that:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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. 	<p>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.</p> <p><Report Findings Here></p>	
KIF KMCP KLCP SP	<p>10-1.d Examine system documentation and configuration files to validate the above, including HSM settings.</p>	System documentation examined:	<Report Findings Here>
11-1 Written procedures must exist and be known to all affected parties.			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP SP	11-1.a Verify documented procedures exist for all key transmission and conveyance processing.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP SP	11-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.	Responsible personnel interviewed:	<Report Findings Here>
11-2 Methods used for the conveyance or receipt of keys must be documented.			
CA/RA KIF KMCP KLCP SP	11-2.a 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.			
CA/RA KIF KLCP SP	12-1.a Using the summary of cryptographic keys, identify keys that are loaded from components and examine documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	12-1.b Interview appropriate personnel to determine the number of key components for each manually loaded key.	Appropriate personnel interviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	12-1.c Witness a structured walk-through/demonstration of various key-loading processes for all key types (MFKs, AWKs, TMKs, PEKs, etc.). Verify the number and length of the key components against information provided through verbal discussion and written documentation.	Describe how the structured walk-through/demonstration verified that the number and length of the key components is consistent with information provided through verbal discussion and written documentation: <Report Findings Here>	

Key Management – Reporting

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

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<p>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.</p> <p>Dual control must be implemented using one or more of, but not limited to, the following techniques:</p> <ul style="list-style-type: none"> • 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 <p>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.</p> <p>Note: Passwords/authentication codes to the same object may be assigned to a custodian group team—e.g., custodian team for component A.</p> <p>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.</p>		
CA/RA KIF KLCP SP	<p>12-3.a Identify instances where a key-loading device is used to load clear-text keys. Examine documented procedures for loading of clear-text cryptographic keys to verify that:</p> <ul style="list-style-type: none"> • Procedures require dual control to authorize any key-loading session. • The techniques to be used to achieve dual control are identified. • There is a requirement to change any default passwords/authentication codes and set passwords/authentication codes that have at least five characters. • There is a requirement that if passwords/authentication codes or tokens are used, they be maintained separately. 	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	<p>12-3.b For each type of production SCDs loaded using a key-loading device, observe for the process (e.g., a demonstration) of loading clear-text cryptographic keys and interview personnel. Verify that:</p> <ul style="list-style-type: none"> • 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. 	<p>Describe how the observed processes for loading clear-text cryptographic keys for all types of production SCDs verified that dual control is required to authorized any key-loading sessions, expected techniques are used, any passwords used are a minimum of five characters (default passwords/authentication codes are reset) and any passwords/authentication codes or tokens are maintained separately:</p> <p><Report Findings Here></p>	
CA/RA KIF KLCP SP	<p>12-3.c Examine documented records of key-loading to verify the presence of two authorized persons during each type of key-loading activity.</p>	Documented records of key-loading processes reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>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.</p>	<p>Describe how default dual-control mechanisms were verified to have been disabled or changed:</p> <p><Report Findings Here></p>	
<p>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.</p> <p>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.</p>			
CA/RA KIF KLCP SP	<p>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.</p>	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>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.</p>	<p>Describe how the key-component lengths or device configuration settings observed verified that key components used to create a key are the same length as the resultant key:</p> <p><Report Findings Here></p>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
12-5 Hardware security module (HSM) Master File Keys (MFK), including those generated internal to the HSM and never exported, must use AES with a key size of at least 128 bits.			
CA/RA KIF KLCP SP	12-5.a Examine vendor documentation describing options for how the HSM MFK is created and verify the current MFK was created using AES (or double- or triple-length TDEA for existing implementations only). Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.	Vendor documentation reviewed:	<Report Findings Here>
		Identify the P2PE Assessor who corroborated how the HSM MFK is created:	<Report Findings Here>
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.			
CA/RA KIF KLCP SP	12-6.a Thorough examination of documented procedures, interviews, and observation, confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key.	Documented procedures reviewed:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
		Describe how it was confirmed that any devices that are loaded with the same key components use the same mathematical process to derive the final key:	
		<Report Findings Here>	
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: <ul style="list-style-type: none"> • 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.			
KIF KLCP SP	12-7.a Examine documented procedures for the loading of TMKs and initial DUKPT keys to verify that they require asymmetric key-loading techniques or manual techniques for initial loading and allowed methods for replacement TMK or initial DUKPT key loading.	Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP SP	12-7.b Examine documented procedures to verify that keys are withdrawn from use if they were loaded to a device that has been compromised or gone missing.	Documented procedures reviewed:	<Report Findings Here>
<p>12-8 If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, these must meet the applicable requirements detailed in this document. For example:</p> <p>A public-key technique for the distribution of symmetric secret keys must:</p> <ul style="list-style-type: none"> • 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. 			
KIF KLCP SP	12-8.a For techniques involving public-key cryptography, examine documentation to illustrate the process, including the size and sources of the parameters involved, and the mechanisms utilized for mutual device authentication for both the host and the POI device.	Documented procedures reviewed:	<Report Findings Here>
KIF KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>12-9 Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (e.g., POIs and other SCDs).</p> <p>Note: Such controls may include but are not limited to:</p> <ul style="list-style-type: none"> Physical dual access controls that electronically provide for restricted entry and egress from a room dedicated to key injection such that the badge-access system enforces the presence of at least two authorized individuals at all times in the room so no one person can singly access the key-loading equipment. Access is restricted to only appropriate personnel involved in the key-loading process. Logical dual control via multiple logins with unique user IDs to the key-injection platform application such that no one person can operate the application to singly inject cryptographic keys into devices Key-injection platform applications that force the entry of multiple key components and the implementation of procedures that involve multiple key custodians who store and access key components under dual-control and split-knowledge mechanisms Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry Separate key-loading devices for each component 			
KIF KLCP	12-9.a Examine documented key-injection procedures to verify that the procedures define use of dual control and split knowledge controls for the loading of keys into devices.	Documented key-injection procedures reviewed:	<Report Findings Here>
KIF KLCP	12-9.b Interview responsible personnel and observe key-loading processes and controls to verify that dual control and split-knowledge controls are in place for the loading of keys into devices.	Responsible personnel interviewed:	
		Describe how the observed key-loading processes and controls verified that dual control and split-knowledge controls are in place for the loading of keys into devices:	
		<Report Findings Here>	
KIF KLCP	12-9.c Examine records of key-loading processes and controls to verify that the loading of keys does not occur without dual control and split knowledge.	Records of key-loading processes and controls reviewed:	<Report Findings Here>
<p>13-1 Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that:</p> <ul style="list-style-type: none"> 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. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	<p>13-1.a Observe key-loading environments, processes, and mechanisms (e.g., terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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:	<ul style="list-style-type: none"> • SCDs must be inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. • An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are identified by the device. • There is not any mechanism (including cabling) at the interface between the conveyance medium and the SCD device that might disclose the transferred keys. • The SCD is inspected to ensure it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying material. 	
<p>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.</p> <p>Note: The addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS POI Security Requirements and listed as such in the approval listings. If a PED that has been modified to perform these functions has not been validated and approved to the KLD approval class, they must be managed in accordance with Requirement 13-9.</p>			
CA/RA KIF KLCP SP	<p>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.</p>	Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KLCP SP	13-2.b Observe a demonstration of key loading to verify that only SCDs are used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility.	Describe how the observed demonstration verified that only SCDs are used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility.	
		<Report Findings Here>	
<p>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</p> <ul style="list-style-type: none"> • 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. 			
CA/RA KIF KLCP SP	13-3.a Examine documented procedures for the loading of secret or private key components from electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key injection, including: <ul style="list-style-type: none"> • 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>
		<Report Findings Here>	
CA/RA KIF KLCP SP	13-3.b Observe key-loading processes to verify that the injection process results in one of the following: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium. 	
		<Report Findings Here>	
CA/RA KIF KLCP SP	13-3.c Examine records/logs of erasures to confirm that: <ul style="list-style-type: none"> • The documented procedure was followed. • The method used was in accordance with Requirement 24. 	Logs examined:	<Report Findings Here>
		<Report Findings Here>	

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
13-4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:			
CA/RA KIF KLCP SP	13-4 Examine documented procedures and observe processes for the use of key-loading devices. Perform the following:		
13-4.1 The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected. <i>Note: A PCI-approved KLD meets this requirement for an SCD.</i>			
CA/RA KIF KLCP SP	13-4.1 Verify the key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.	Documented procedures reviewed:	<Report Findings Here>
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected:	
		<Report Findings Here>	
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. <i>Note: Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.</i>			
CA/RA KIF KLCP SP	13-4.2 Verify the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.	Documented procedures reviewed:	<Report Findings Here>
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it:	
		<Report Findings Here>	
13-4.3 The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.			
CA/RA KIF KLCP SP	13-4.3.a Verify the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD.	Documented procedures reviewed:	<Report Findings Here>
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD:	

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
		<Report Findings Here>	
CA/RA KIF KLCP SP	13-4.3.b Verify that both authorized personnel involved in key-loading activity inspect the key-loading device prior to use to ensure that a key-recording device has not been inserted between the SCDs.	Documented procedures reviewed:	<Report Findings Here>
		Describe how the observed processes for the use of key-loading devices verified that authorized personnel inspect the key-loading device prior to use to ensure that a key-recording device has not been inserted between the SCDs:	
		<Report Findings Here>	
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.			
CA/RA KIF KLCP SP	13-4.4 Verify the key-loading device does not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred. For example, attempt to output the same value more than one time from the device or cause the device to display check values for its contents both before and after injection and compare.	Documented procedures reviewed:	<Report Findings Here>
		Describe how the observed processes for the use of key-loading devices verified that the key-loading device does not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred:	
		<Report Findings Here>	
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.			
CA/RA KIF KLCP SP	13-5.a Interview personnel and observe media locations to verify that the media is maintained in a secure location accessible only to custodian(s) authorized to access the key components.	Personnel interviewed:	<Report Findings Here>
		Media locations observed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KLCP SP	<p>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:</p> <ul style="list-style-type: none"> Requirement that media/devices be in the physical possession of only the designated component holder(s). The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process. 	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>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).</p>	Designated component holder(s) interviewed:	<Report Findings Here>
		Key-management logs examined:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>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.</p>	Key-injection personnel interviewed:	<Report Findings Here>
		Logs examined:	<Report Findings Here>
<p>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.</p>			
CA/RA KIF KLCP SP	<p>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.</p>	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>	
<p>13-7 Written or printed key component documents must not be opened until immediately prior to use.</p>			
CA/RA KIF KLCP SP	<p>13-7.a Examine documented procedures and confirm that printed/written key component documents are not opened until immediately prior to use.</p>	Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	13-7.b Observe key-loading processes and verify that printed/written key component documents are not opened until immediately prior to use.	Describe how the observed key-loading processes verified that printed/written key-component documents are not opened until immediately prior to use: <Report Findings Here>	
<p>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.</p> <p><i>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.</i></p>			
CA/RA KIF KLCP SP	13-8.a Examine documented procedures for the use of key components to verify that procedures ensure that any individual custodian only has access to their assigned components and never has access to sufficient key components to reconstruct a cryptographic key.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	13-8.b Examine key-component access controls and access logs to verify that any single authorized custodian can and has only had access to their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.	Describe how the observed key-component access controls and access logs verified that any single authorized custodian can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key: <Report Findings Here>	
<p>13-9 Key-injection facilities that use PC-based key-loading software platforms or similar devices (e.g., modified PEDs) that allow clear-text secret and/or private keys and/or their components to exist in memory outside the secure boundary of an SCD must minimally implement the following additional controls:</p> <p>Note: Effective 1 January 2021, entities engaged in key loading on behalf of others must not be allowed to use PC based key-loading methodologies where clear-text secret and/or private keying material appears in the clear in memory outside the secure boundary of an SCD.</p> <p>Effective 1 January 2023, entities only performing key loading for devices for which they are the processor shall no longer have this option.</p>			
KIF KLCP	13-9 Interview appropriate personnel and examine documentation to determine the procedures for key loading to POIs, key-loading devices, and HSMs that are part of the key-loading platform. Examine any logs of key loading.	Appropriate personnel interviewed:	<Report Findings Here>
		Documented procedures reviewed:	<Report Findings Here>
		Key-loading logs reviewed:	<Report Findings Here>
<p>13-9.1 PCs and similar devices must be:</p> <ul style="list-style-type: none"> • Standalone (i.e., without modems, not connected to a LAN or WAN, not capable of wireless connections, etc.); • Dedicated to only the key-loading function (e.g., there must not be any other application software installed); and • Located in a physically secure room meeting the criteria of Requirement 32-9 that is dedicated to key-loading activities. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP SP	<p>13-9.1 For facilities using PC-based key-loading software platforms or similar devices, verify through interviews and observation that the platform is:</p> <ul style="list-style-type: none"> Standalone Dedicated to only key loading Located in a physically secure room meeting the criteria of Requirement 32-9 that is dedicated to key loading activities 	Personnel interviewed:	<Report Findings Here>
		Identify the P2PE Assessor who confirms that for facilities using PC-based key-loading software platforms or similar devices, the platform is standalone, dedicated to only key loading, and located in a physically secure room that is dedicated to key-loading activities.	<Report Findings Here>
	<p>13-9.2 All hardware used in key loading (including the PC) must be managed under dual control. Key-injection must not occur unless there are minimally two individuals in the key-injection room at all times during the process. If a situation arises that would cause only one person to be in the room, all individuals must exit until at least two can be inside.</p>		
KIF KLCP SP	<p>13-9.2 Verify through interviews and observation that:</p> <ul style="list-style-type: none"> All hardware used in key loading (including the PC) is managed under dual control. Key-injection cannot occur unless there are minimally two individuals in the key-injection room at all times during the process. Mechanisms exist (See Requirement 32) that do not permit the room to be occupied by fewer than two authorized individuals. 	Personnel interviewed:	<Report Findings Here>
		Describe how observation of the facilities verified that:	
		<ul style="list-style-type: none"> All hardware used in key loading (including the PC) is managed under dual control. Key-injection cannot occur unless there are minimally two individuals in the key-injection room at all times during the process. Mechanisms exist (See Requirement 32) that do not permit the room to be occupied by fewer than two authorized individuals 	
		<Report Findings Here>	
<p>13-9.3 PC access and use must be monitored, and logs of all key loading must be maintained. These logs must be retained for a minimum of three years. The logs must be regularly (no less frequently than weekly) reviewed by an authorized person who does not have access to the room or to the PC. The reviews must be documented. The logs must include but not be limited to:</p> <ul style="list-style-type: none"> Logs of access to the room from a badge-access system; Logs of access to the room from a manual sign-in sheet; User sign-on logs on the PC at the operating-system level; User sign-on logs on the PC at the application level; Logs of the device IDs and serial numbers that are loaded, along with the date and time and the individuals performing the key-injection; Video surveillance logs with a minimum retention period of 45 days. 			

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP SP	13-9.3.a Verify through interviews and observation that logs of key-loading activities are maintained and meet the following: <ul style="list-style-type: none"> • Retained for a minimum of three years. • Regularly reviewed by an authorized person who does not have access to the room or to the PC. • The reviews are documented. 	Personnel interviewed:	<Report Findings Here>
		Logs of key-loading activities reviewed:	<Report Findings Here>
KIF KLCP SP	13-9.3.b Verify through interviews and observation that logs of key-loading activities are maintained and meet the following: <ul style="list-style-type: none"> • Retained for a minimum of three years. • Regularly reviewed by an authorized person who does not have access to the room or to the PC. • The reviews are documented. • Logs include a minimum of: <ul style="list-style-type: none"> – Access to the room from a badge access system, – Access to the room from a manual sign-in sheet, – User sign-on logs on the PC at the operating system level, – User sign-on logs on the PC at the application level, – Logs of the device IDs and serial numbers that are loaded along with the date and time and the individuals performing the key-injection, and – Video surveillance logs with a minimum retention period of 45 days. 	Personnel interviewed:	<Report Findings Here>
		Logs of key-loading activities reviewed:	<Report Findings Here>
13-9.4 Additionally:			
KIF KLCP	13-9.4 Verify through interviews and observation that:	Personnel interviewed for 13.9.4.x:	<Report Findings Here>
13-9.4.1 Cable attachments and the key-loading device must be examined before each use to ensure the equipment is free from tampering.			
KIF KLCP SP	13-9.4.1 Cable attachments and the key-loading device are examined before each use to ensure the equipment is free from tampering.	Describe how it was verified that cable attachments and the key-loading device are examined before each use to ensure the equipment is free from tampering:	
		<Report Findings Here>	
13-9.4.2 The key-loading device must be started from a powered-off position every time key-loading activities occur.			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings
KIF KLCP SP	13-9.4.2 The key-loading device is started from a powered-off position every time key-loading activities occur.	Describe how it was verified that the key-loading device is started from a powered-off position every time key-loading activities occur:
		<Report Findings Here>
13-9.4.3 The software application must load keys without recording any clear-text values on portable media or other unsecured devices.		
KIF KLCP SP	13-9.4.3 The software application loads keys without recording any clear-text values on portable media or other unsecured devices.	Describe how it was verified that the software application loads keys without recording any clear-text values on portable media or other unsecured devices:
		<Report Findings Here>
13-9.4.4 Clear-text keys must not be stored except within an SCD.		
KIF KLCP SP	13-9.4.4 Clear-text keys are not stored except within an SCD.	Describe how it was verified that clear-text keys are not stored except within an SCD:
		<Report Findings Here>
13-9.4.5 The personnel responsible for the systems administration of the PC (e.g., a Windows administrator who configures the PC's user IDs and file settings, etc.) must not have authorized access into the room—they must be escorted by authorized key-injection personnel—and they must not have user IDs or passwords/authentication codes to operate the key-injection application.		
KIF KLCP SP	13-9.4.5 Personnel responsible for the systems administration of the PC do not have authorized access into the room—i.e., they are escorted by authorized key-injection personnel—and do not have user IDs or passwords/authentication codes to operate the key-injection application.	Describe how it was verified that personnel responsible for the systems administration of the PC do not have authorized access into the room and do not have user IDs or passwords to operate the key-injection application:
		<Report Findings Here>
13-9.4.6 The key-injection personnel must not have system-administration capability at either the O/S or the application level on the PC.		
KIF KLCP SP	13-9.4.6 Key-injection personnel do not have system-administration capability at either the O/S or the application level on the PC.	Describe how it was verified that key-injection personnel do not have system-administration capability at either the O/S or the application level on the PC:
		<Report Findings Here>
13-9.4.7 The PC must not be able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.		
KIF KLCP SP	13-9.4.7 The PC is not able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.	Describe how it was verified that the PC is not able to boot from external media and must boot from the hard drive only:
		<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings
	<p>13-9.4.8 Key-injection facilities must cover all openings on the PC that are not used for key-injection with security seals that are tamper-evident and serialized. Examples include but are not limited to PCMCIA, network, infrared and modem connections on the PC, and access to the hard drive and memory. The seals must be recorded in a log, and the log must be maintained along with the other key-loading logs in a dual-control safe. Verification of the seals must be performed prior to key-loading activities.</p>	
<p>KIF KLCP SP</p>	<p>13-9.4.8 All openings on the PC that are not used for key-injection are covered with security seals that are tamper-evident and serialized. The seals are recorded in a log, and the log is maintained along with the other key-loading logs in a dual-control safe. Verification of the seals must be performed prior to key-loading activities.</p>	<p>Describe how it was verified that:</p> <ul style="list-style-type: none"> All openings on the PC that are not used for key-injection are covered with security seals that are tamper-evident and serialized. The seals are recorded in a log, and the log is maintained along with the other key-loading logs in a dual-control safe. Verification of the seals must be performed prior to key-loading activities. <p><Report Findings Here></p>
	<p>13-9.4.9 If the PC application stores clear-text key components (e.g., BDKs or TMKs) on portable electronic media (e.g., smart cards), the media must be secured as components under dual control when not in use. The key components must be manually entered at the start of each key-injection session from components that are maintained under dual control and split knowledge.</p> <p>Note: For DUKPT implementations, the BDK must be loaded from components each time and this requires manual tracking of the device ID counter and serial numbers from the previous key-loading session. Key-injection facilities with PC applications that require passwords/authentication codes to be used to initiate decryption of keys on portable electronic media (e.g., smart cards) must ensure the passwords/authentication codes are maintained under dual control and split knowledge.</p>	
<p>KIF KLCP SP</p>	<p>13-9.4.9 If the PC application stores keys (e.g., BDKs or TMKs) on portable electronic media (e.g., smart cards), the media is secured as components under dual control when not in use. The key components are manually entered at the start of each key-injection session from components that are maintained under dual control and split knowledge.</p>	<p>Describe how it was verified that if the PC application stores keys on portable electronic media:</p> <ul style="list-style-type: none"> The media is secured as components under dual control when not in use. The key components are manually entered at the start of each keyinjection session from components that are maintained under dual control and split knowledge. <p><Report Findings Here></p>
	<p>13-9.4.10 Manufacturer's default passwords/authentication codes for PC-based applications must be changed.</p>	
<p>KIF KLCP SP</p>	<p>13-9.4.10 Manufacturer's default passwords/authentication codes for PC-based applications are changed.</p>	<p>Describe how manufacturer's default passwords for PC-based applications were verified to be changed:</p> <p><Report Findings Here></p>
	<p>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.</p> <p>Note: Where key-loading is performed for POI devices, the secure environment as defined in Requirement 32-9 must additionally be met.</p>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP SP	<p>14-1.a Examine documented procedures to verify they require the following:</p> <ul style="list-style-type: none"> Any hardware used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. Any resources (e.g., passwords/authentication codes and associated hardware) used in the key-loading function or for the signing of authenticated applications must be controlled and managed such that no single individual has the capability to enable key loading of clear-text keys or their components. 	Documented procedures examined:	<Report Findings Here>
KIF KLCP SP	<p>14-1.b Observe key-loading environments and controls to verify the following:</p> <ul style="list-style-type: none"> 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. 	<p>Describe how the observation of key-loading environments and controls verified that:</p> <ul style="list-style-type: none"> 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>
<p>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.</p> <p>The secure room for key injection must include the following:</p> <ul style="list-style-type: none"> Effective 1 January 2021, the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. Only encrypted key injection shall be allowed for POI v3.0 and higher devices. Effective 1 January 2023, the same restriction applies to entities engaged in key injection of devices for which they are the processors. <p>Note: This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the PCI PTS POI Security Requirements. It does apply to all other methods of loading of clear-text keying material for POI v3.0 and higher devices.</p>			
CA/RA KIF KLCP SP	<p>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.</p>	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	14-2.b Observe key-loading processes to verify that all cable attachments are properly examined at the beginning of an entity's key-activity operations (system power on/authorization) or application-signing operations.	Describe how the key-loading processes observed verified that all cable attachments are properly examined prior to key-loading functions: <Report Findings Here>	
14-3 Key-loading equipment usage must be monitored and a log of all key-loading and application-signing activities maintained for audit purposes, containing at a minimum date, time, personnel involved, and number of devices keys are loaded to.			
CA/RA KIF KLCP SP	14-3.a Observe key-loading and application-signing activities to verify that key-loading equipment usage is monitored.	Describe how the key-loading activities observed verified that key-loading equipment usage is monitored: <Report Findings Here>	
CA/RA KIF KLCP SP	14-3.b Verify logs of all key-loading and application-signing activities are maintained and contain all required information.	Logs of key-loading activities reviewed:	<Report Findings Here>
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.			
CA/RA KIF KLCP SP	14-4.a Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key loading or the signing of authenticated applications. Verify procedures require that physical tokens must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	14-4.b Inspect locations and controls for physical tokens to verify that tokens used to enable key loading or the signing of authenticated applications are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control.	Identify the P2PE Assessor who inspected locations and controls for physical tokens and confirms that tokens used to enable key loading are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	14-4.c Examine storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.	Identify the P2PE Assessor who confirms adequacy of reviewed storage locations for physical tokens to ensure that only the authorized custodian(s) can access their specific tokens:	<Report Findings Here>
CA/RA KIF KLCP SP	14-4.d Verify that access-control logs exist and are in use including notation of tamper-evident, authenticable bag numbers.	Access-control logs reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	14-4.e Reconcile storage contents to access-control logs.	Identify the P2PE Assessor who reconciled storage contents to access-control logs:	<Report Findings Here>
14-5 Default passwords/authentication codes used to enforce dual-control mechanisms must be changed, and documented procedures must exist to require that these password/PINs be changed, when assigned personnel change.			
CA/RA KIF KLCP SP	14-5.a Verify that documented procedures require default passwords/authentication codes used to enforce dual-control mechanisms are changed.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	14-5.b Verify that documented procedures exist to require that these passwords/authentication codes be changed when assigned personnel change.	Documented procedures reviewed:	<Report Findings Here>
<p>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 <i>ISO 11568</i>. Where check values are used, recorded, or displayed key-component check values and key check values must be generated by 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.</p> <p>Note: Check values are computed by encrypting an all-zero 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). Either this method must be used for TDEA or TDEA must use, and AES shall use a technique where the KCV is calculated by MACing an all-zero 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.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>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 <i>ISO 11568</i>. 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.</p> <p>Note: Check values are computed by encrypting an all-zero 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). Either this method must be used for TDEA or TDEA must use, and AES must use a technique where the KCV is calculated by MACing an all-zero block using the CMAC algorithm as specified in <i>ISO 9797-1</i> (see also <i>NIST SP 800-38B</i>). 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.</p>			
CA/RA KIF KLCP SP	15-1.a Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and/or components.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	15-1.b Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and is verified by the applicable key custodians.	Describe how the key-loading processes observed verified that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and is verified by the applicable key custodians:	<Report Findings Here>
CA/RA KIF KLCP SP	15-1.c Verify that the methods used for key validation are consistent with <i>ISO 11568</i> —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 <i>ISO 11568</i> :	<Report Findings Here>
<p>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:</p> <ul style="list-style-type: none"> • 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 <i>ISO 16609</i>. 			
CA/RA KIF KLCP SP	15-2.a Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.	Personnel interviewed:	<Report Findings Here>
		Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KLCP SP	15-2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.	Describe how the observed public-key stores and mechanisms verified that public keys exist only in an approved form:	
<p>15-3 Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange, or key establishment with POIs. POIs and key-distribution hosts (KDHs) using public-key schemes must validate authentication credentials of other such devices involved in the communication immediately prior to any key transport, exchange, or establishment.</p> <p>Mutual authentication of the sending and receiving devices must be performed.</p> <p>Note: Examples of this kind of validation include ensuring the SCD serial number is listed in a table of “permitted” devices, checking current certificate revocation lists or embedding valid authorized KDH certificates in devices and disallowing communication with unauthorized KDHs, as delineated by techniques defined in the Technical FAQs for PCI PTS POI Security Requirements.</p>			
RKD	15-3.a Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: <ul style="list-style-type: none"> POI devices must validate authentication credentials of KDHs prior to any key transport, exchange, or establishment with that device. KDHs must validate authentication credentials of POIs prior to any key transport, exchange, or establishment with that device. 	Documented procedures examined:	<Report Findings Here>
RKD	15-3.b Interview applicable personnel to verify that mutual authentication of the sending and receiving devices is performed, as follows: <ul style="list-style-type: none"> POI devices validate authentication credentials of KDHs immediately prior to any key transport, exchange, or establishment with that device. KDHs validate authentication credentials of POIs immediately prior to any key transport, exchange, or establishment with that device. 	Applicable personnel interviewed:	<Report Findings Here>
<p>15-4 Key-establishment and distribution procedures must be designed such that:</p> <ul style="list-style-type: none"> Within an implementation design, there must be no means available for “man-in-the-middle” attacks—e.g., through binding of the KDH certificate upon the initial communication. System implementations must be designed and implemented to prevent replay attacks—e.g., through the use of random nonces and time stamps as noted in ANS/ TR-34. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
RKD	<p>15-4 Examine system and process documentation to verify that key-establishment and distribution procedures are designed such that:</p> <ul style="list-style-type: none"> • There are no means available in the implementation design for “man-in-the-middle” attacks. • System implementations are designed to prevent replay attacks. 	System and process documentation reviewed:	<Report Findings Here>
<p>15-5 Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device and must provide for key protection in accordance with this document. That is, the secrecy of the private key and the integrity of the public key must be ensured. The process must ensure that once keys are injected they are no longer available for injection into other POI devices—i.e., key pairs are unique per POI device.</p>			
CA/RA RKD	<p>15-5 If key pairs are generated external to the device that uses the key pair, perform the following:</p> <ul style="list-style-type: none"> • Examine documented procedures to verify that controls are defined to ensure the secrecy of private keys and the integrity of public keys during key transfer and loading. • Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured. • Verify the process ensures that key pairs are unique per POI device. 	Documented procedures reviewed:	<Report Findings Here>
		Describe how key transfer and loading operations verified that the secrecy of private keys and the integrity of the public keys are ensured:	
		<Report Findings Here>	
		Describe how key transfer and loading operations verified that the process ensures that key pairs are unique per POI device:	
<Report Findings Here>			
<p>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.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	16-1.a Verify documented procedures exist for all key-loading operations.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	16-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.	Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	16-1.c Observe the key-loading process for keys loaded as components and verify that the documented procedures are demonstrably in use. This may be done as necessary on test equipment—e.g., for HSMs.	Identify the P2PE Assessor who confirms that the documented procedures for keys loaded as components are demonstrably in use:	<Report Findings Here>
16-2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.			
CA/RA KIF KLCP SP	16-2 Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.	Log files examined:	<Report Findings Here>
		Describe how the logging processes observed verified that audit trails are in place for all key-loading events:	
		<Report Findings Here>	
<p>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:</p> <ul style="list-style-type: none"> • Be unique to those two entities or logically separate systems, and • Not be given to any other entity or logically separate systems. <p>Note: This requirement does not apply after the decryption environment.</p>			
SP	17-1.a Examine the documented key matrix and operational procedures and interview personnel to determine whether any	Documented key matrix reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	keys are shared between organizations or logically separate systems.	Documented operational procedures reviewed:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
SP	<p>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:</p> <ul style="list-style-type: none"> • Generate or otherwise obtain key check values for any key-encipherment keys (KEKs) to verify key uniqueness between the two organizations. A random sample may be used where more than 10 zone connections are in use. This is not intended to be based on values retained on paper or otherwise sent as part of the original conveyance of the keying material, but rather on values generated from stored zone production keys from the production host database. Cryptograms may be used for this purpose if it is verified that the same MFK variant is used to encrypt the KEKs. • If a remote key-establishment and distribution scheme is implemented between networks, examine public keys and/or hash values and/or fingerprints of the keys to verify key uniqueness of the asymmetric-key pairs. • Compare key check values against those for known or default keys to verify that known or default key values are not used. 	Describe how the generation of (or otherwise obtaining) key check values for any key-encipherment keys (KEKs), public keys, and/or hash values and/or fingerprints (where a remote key-establishment and distribution scheme is implemented) verified key uniqueness between the two organizations:	<Report Findings Here>
<p>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.</p> <p>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.</p>			
SP	18-1.a Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
SP	<p>18-1.b Verify that implemented procedures include:</p> <ul style="list-style-type: none"> • Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) • Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event. 	Documented procedures examined:	<Report Findings Here>
<p>18-2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of the component and the associated key at all locations where they exist.</p>			
CA/RA KIF KMCP KLCP SP	<p>18-2.a Verify that documented procedures require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.</p>	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	<p>18-2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed,</p>	Personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	<p>and the result is that one person could have knowledge of the key, it results in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.</p>	<p>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:</p> <p><Report Findings Here></p>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings
	<p>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</p> <p>The phased implementation dates are as follows:</p> <ul style="list-style-type: none"> • 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 June 2021. • Phase 3 – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Effective date: 1 June 2023. <p>Acceptable methods of implementing the integrity requirements include, but are not limited to:</p> <ul style="list-style-type: none"> • 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; • 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 <i>ANSI X9.102</i>. 	
<p>KIF KLCP SP</p>	<p>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.</p> <p>Where key blocks are not implemented, identify and examine project plans to implement in accordance with the prescribed timeline.</p>	<p>Describe how the documented procedures examined and the key operations observed verified that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of the acceptable methods or an equivalent.</p> <p><Report Findings Here></p> <p>Where key blocks are not implemented, describe how the examined project plans verified that key block implementation is in accordance with the prescribed timeline(s).</p> <p><Report Findings Here></p>
		<p>18-4 POI devices must only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate-issuing authority generates the key pair on behalf of the POI); and with KDHS for key management, normal transaction processing, and certificate (entity) status checking.</p>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
RKD	<p>18-4.a Examine documented procedures to verify that:</p> <ul style="list-style-type: none"> POI devices only communicate with CAs for the purpose of certificate signing, or for key injection where the certificate-issuing authority generates the key pair on behalf of the device; POI devices only communicate with KDHS for key management, normal transaction processing, and certificate (entity) status checking. 	Documented procedures examined:	<Report Findings Here>
RKD	<p>18-4.b Interview responsible personnel and observe POI configurations to verify that:</p> <ul style="list-style-type: none"> POI devices only communicate with CAs for the purpose of certificate signing, or for key injection where the certificate issuing authority generates the key pair on behalf of the device; POI devices only communicate with KDHS or key management, normal transaction processing, and certificate (entity) status checking. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the POI configurations observed verified that POIs only communicate with CAs for the purpose of certificate signing, or for key-injection where the certificate issuing authority generates the key pair on behalf of the device:	
		<Report Findings Here>	
		Describe how the POI configurations observed verified that POIs only communicate with KDHS or key management, normal transaction processing, and certificate (entity) status checking:	
		<Report Findings Here>	
<p>18-5 KDHS must only communicate with POI devices for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.</p>			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
RKD	18-5.a Examine documented procedures to verify that: <ul style="list-style-type: none"> • KDHs only communicate with POI devices for the purpose of key management and normal transaction processing; • KDHs only to communicate with CAs for the purpose of certificate signing and certificate (entity) status checking. 	Documented procedures reviewed:	<Report Findings Here>
RKD	18-5.b Interview responsible personnel and observe KDH configurations to verify that: <ul style="list-style-type: none"> • KDHs only communicate with POIs for the purpose of key management and normal transaction processing; • KDHs only communicate with CAs for the purpose of certificate signing and certificate (entity) status checking. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the KDH configurations observed verified that KDHs only communicate with POIs for the purpose of key management and normal transaction processing:	
		<Report Findings Here>	
		Describe how the KDH configurations observed verified that KDHs only communicate with CAs for the purpose of certificate signing and certificate (entity) status checking:	
		<Report Findings Here>	
18-6 Controls must be in place to prevent and detect the loading of unencrypted private and secret keys or their components by any one single person. Note: Controls include physical access to the room, logical access to the key-loading application, video surveillance of activities in the key-injection room, physical access to secret or private cryptographic key components or shares, etc.			
KIF KLCP	18-6.a Examine documented key-injection procedures to verify that controls are defined to prevent and detect the loading of keys by any one single person.	Documented procedures examined:	<Report Findings Here>
KIF KLCP	18-6.b Interview responsible personnel and observe key-loading processes and controls to verify that controls—e.g., viewing CCTV images—are implemented to prevent and detect the loading of keys by any one single person.	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the key-loading processes and controls observed verified that controls are implemented to prevent and detect the loading of keys by any one single person:	
		<Report Findings Here>	
18-7 Key-injection facilities must implement controls to protect against unauthorized substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to: <ul style="list-style-type: none"> • All devices loaded with keys must be tracked at each key-loading session by serial number. • Key-injection facilities must use something unique about the POI (e.g., logical identifiers) when deriving the key (e.g., DUKPT, TMK) injected into it. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	18-7.a Examine documented procedures to verify they include: <ul style="list-style-type: none"> • Controls to protect against unauthorized substitution of keys, and • Controls to prevent the operation of devices without legitimate keys. 	Documented procedures reviewed:	<Report Findings Here>
KIF KLCP	18-7.b Interview responsible personnel and observe key-loading processes and controls to verify that: <ul style="list-style-type: none"> • Controls are implemented that protect against unauthorized substitution of keys, and • Controls are implemented that prevent the operation of devices without legitimate keys. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the key-loading processes observed verified that: <ul style="list-style-type: none"> • Controls are implemented that protect against unauthorized substitution of keys, and • Controls are implemented that prevent the operation of devices without legitimate keys. 	
		<Report Findings Here>	
19-1 Encryption keys must only be used for the purpose they were intended—i.e., key-encryption keys must not be used as PIN-encryption keys, PIN-encryption keys must not be used for account-data, etc. Derivation Keys may be derived into multiple keys, each with its own purpose. For example, a DUKPT Initial Key may be used to derive both a PIN encryption key and a data encryption key. The derivation key would only be used for its own purpose—key derivation. This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	19-1.a Examine key-management documentation (e.g., the cryptographic-key inventory) and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are defined for a specific purpose.	Key-management documentation examined:	<Report Findings Here>
		Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	19-1.b Using a sample of device types, validate via examination of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.	Sample of device types reviewed:	<Report Findings Here>
		Describe how review of check values, terminal definition files, etc. verified that keys used for key encipherment or PIN encipherment are not used for any other purpose:	
		<Report Findings Here>	
19-2 Private keys: <ul style="list-style-type: none"> 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.			
CA/RA KIF KLCP SP	19-2 Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are :	Key-management documentation examined:	<Report Findings Here>
		Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
19-3 Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	19-3 Examine key-management documentation and interview key custodian and key-management supervisory personnel to verify that public keys are only used:	Key-management documentation examined:	<Report Findings Here>
	<ul style="list-style-type: none"> To perform encryption operations or to verify digital signatures. 	Key custodians interviewed:	<Report Findings Here>
	<ul style="list-style-type: none"> 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 supervisory personnel interviewed:	<Report Findings Here>
<p>19-4 Keys must never be shared or substituted between production and test/development systems. Keys used for production must never be present or used in a test/development system, and Keys used for testing must never be present or used in a production system.</p> <p>Note: For logically partitioned HSMS and computing platforms, if one or more logical partitions of a physical device are used for production and one or more other logical partitions are used for testing, including QA or similar, the entire configuration that is impacted—computing platform(s) and networking equipment—must be managed and controlled as production.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	19-4.a Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and test/development systems.	Key-management documentation examined:	<Report Findings Here>
		Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	19-4.b Observe processes for generating and loading keys into production systems to ensure that they are in no way associated with test or development keys.	Describe how the observed processes for generating and loading keys into production systems verified that they are in no way associated with test or development keys: <Report Findings Here>	
CA/RA KIF KLCP SP	19-4.c Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.	Describe how the observed processes for generating and loading keys into test systems verified that they are in no way associated with production keys: <Report Findings Here>	
CA/RA KIF KLCP SP	19-4.d Compare check, hash, cryptogram, or fingerprint values for production and test/development keys with higher-level keys (MFKs, KEKs shared with other network nodes, and BDks) to verify that development and test keys have different key values.	Describe how the observed compared check, hash, cryptogram, or fingerprint values for production and test/development keys with higher-level keys (MFKs, KEKs shared with other network nodes, and BDks) verified that development and test keys have different key values:	
		<Report Findings Here>	
<p>19-5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.</p> <p>At all times, the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.</p> <p>Note: This does not apply to HSMs that are never intended to be used for production.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	<p>19-5 Interview personnel to determine whether production platforms are ever temporarily used for test purposes.</p> <p>If they are, verify that documented procedures require that:</p> <ul style="list-style-type: none"> • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes, the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements. 	Personnel interviewed:	<Report Findings Here>
	Documented procedures examined:	<Report Findings Here>	
<p>19-6 Key pairs must not be reused for certificate renewal or replacement—i.e., new key pairs must be generated. Each key pair must result in only one certificate.</p>			
RKD CA/RA	<p>19-6 Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each:</p> <ul style="list-style-type: none"> • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate 	Documented procedures examined:	<Report Findings Here>
<p>19-7 KDH private keys must not be shared between devices except for load balancing and disaster recovery.</p>			
RKD	<p>19-7 Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.</p>	Documented procedures examined:	<Report Findings Here>
<p>19-8 POI device private keys must not be shared between POI devices.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
RKD	19-8.a Examine documented processes to verify that POI device private keys are not permitted to be shared between POI devices.	Documented procedures examined:	<Report Findings Here>
RKD	19-8.b Inspect public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI device.	Describe how public key certificates on the host processing system confirmed that a unique certificate exists for each connected POI: <Report Findings Here>	
19-9 Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose—that is, keys must be used in accordance with their certificate policy. See <i>RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> for an example of content.			
CA/RA	19-9.a Examine key-usage documentation and ensure that the usage is in accordance with the certificate policy.	Documented procedures examined:	<Report Findings Here>
CA/RA	19-9.b Examine vendor documentation and device configuration settings to verify that the device mechanisms are implemented that preclude the use of a key for other than its designated and intended purpose.	Describe how the vendor documentation and device configuration settings observed verified that the device mechanisms are implemented that preclude the use of a key for other than its designated and intended purpose: <Report Findings Here>	
<p>19-9.1 CA certificate signature keys, certificate (entity) status checking (e.g., Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorized host lists in encryption devices must not be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates.</p> <p>Note: The keys used for certificate signing and certificate (entity) status checking (and if applicable, self-signed roots) may be for combined usage or may exist as separate keys dedicated to either certificate-signing or certificate (entity) status checking.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	<p>19-9.1.a Examine certificate policy and documented procedures to verify that the following:</p> <ul style="list-style-type: none"> • Certificate signature keys, • Certificate status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POI devices <p>Are not used for any purpose other than:</p> <ul style="list-style-type: none"> • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates. 	Certificate policy and documented procedures examined:	<Report Findings Here>
CA/RA	<p>19-9.1.b Interview responsible personnel and observe demonstration to verify that the following:</p> <ul style="list-style-type: none"> • Certificate signature keys, • Status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs <p>Are not used for any purpose other than:</p> <ul style="list-style-type: none"> • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the demonstration verified that:	
		<ul style="list-style-type: none"> • Certificate signature keys, • Status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs <p>Are not used for any purpose other than:</p> <ul style="list-style-type: none"> • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates. 	
		<Report Findings Here>	
<p>19-9.2 CAs that issue certificates to other CAs must not be used to issue certificates to POIs (i.e., a CA cannot sign certificates to both subordinate CAs and end-entity [POI] devices).</p>			
CA/RA	<p>19-9.2 If a CA issues certificates to other CAs, examine the CA certificate policy and documented procedures to verify that the CA does not also issue certificates to POI devices.</p>	CA certificate policy and documented procedures examined:	<Report Findings Here>
<p>19-10 Public-key-based implementations must provide mechanisms for restricting and controlling the use of public and private keys. For example, this can be accomplished through the use of X.509 compliant certificate extensions.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	19-10 Examine documented procedures to verify that mechanisms are defined for restricting and controlling the use of public and private keys such that they can only be used for their intended purpose.	Documented procedures examined:	<Report Findings Here>
19-11 CA private keys must not be shared between devices except for load balancing and disaster recovery.			
CA/RA	19-11 Examine CA's documented processes to verify that CA private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.	CA documented processes examined:	<Report Findings Here>
<p>19-12 Certificates used in conjunction with remote key-distribution functions must only be used for a single purpose.</p> <ul style="list-style-type: none"> • Certificates associated with encryption for remote key distribution functions must not be used for any other purpose. • Certificates associated with authentication of the KDH must not be used for any other purpose. • Certificates associated with authentication of the POI must not be used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications must not be used for any other purpose. <p>If CA separation is used to ensure certificate segmentation:</p> <ul style="list-style-type: none"> • Sub-CAs used to produce certificates used for remote key delivery functions must not be used to produce certificates used for any other purpose. • Sub-CAs used to produce certificates for POI firmware and POI application authentication must not be used for any other purpose. <p>If policy-based certificate segmentation is used to achieve unique purpose certificates:</p> <ul style="list-style-type: none"> • The method of segmentation between certificates must be reflected in the certificate practice statement (CPS) for the CA. • Certificates issued for remote key-distribution purposes must include a mechanism to identify designation for this purpose. • Each SCD using a certificate in a remote key-delivery function must ensure there is a designation included in the certificate indicating that it is for use in the remote key-delivery function for which it is being used. • Each SCD using a certificate in a remote key-delivery function must ensure that if there is a designation included in a certificate that indicates it is for use in a remote key-delivery function, the SCD does not use it for any other purpose. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	19-12.a Examine implementation schematics and other relevant documentation to identify PKI architecture and where certificates are used in the implementation.	Schematics and documentation examined:	<Report Findings Here>
CA/RA	19.12.b Identify mechanism(s) used to restrict certificates to a single-purpose use as either: <ul style="list-style-type: none"> • Separation of the Sub-CAs issuing the certificates, or • Policy-based certificate segmentation that depends upon a characteristic of the certificate. 	Describe the identified mechanisms used to restrict certificates to a single-purpose: <Report Findings Here>	
CA/RA	19-12.c If CA separation is used to ensure certificate segmentation, confirm that the following are true: <ul style="list-style-type: none"> • The designation of each Sub-CA is documented. • Policies and procedures are in place to support and require appropriate use of each Sub-CA. • Any Sub-CA used to produce certificates used for remote key-delivery functions (i.e. encryption, POI authentication, or KDH authentication) is not used to produce certificates used for any other purpose. • Any Sub-CA used to produce certificates for POI firmware and POI application authentication is not used for any other purpose. 	If CA separation is used to ensure certificate segmentation, identify the P2PE Assessor who confirms that: <ul style="list-style-type: none"> • The designation of each Sub-CA is documented. • Policies and procedures are in place to support and require appropriate use of each Sub-CA. • Any Sub-CA used to produce certificates used for remote key-delivery functions (i.e. encryption, POI authentication, or KDH authentication) is not used to produce certificates used for any other purpose. • Any Sub-CA used to produce certificates for POI firmware and POI application authentication is not used for any other purpose. 	<Report Findings Here>

<p>CA/RA</p>	<p>19-12.d If policy-based certificate segmentation is used to ensure certificate segmentation, confirm that all of the following are true:</p> <ul style="list-style-type: none"> • The method of segmentation between certificates is clearly stated in the certificate practice statement (CPS) for the CA. • Certificates issued for all of the remote key-distribution functions (i.e. encryption, POI authentication, or KDH authentication) include a mechanism to identify designation for this purpose. • Policies and procedures are in place to support and require specific function designation for each certificate issued, and there is evidence that such procedures are followed. • The SCDs involved in the remote key-delivery functions ensure that the certificates used for these functions are designated for the purpose for which they are being used. • The SCDs involved in remote key delivery ensure that certificates with remote key-delivery designation are not used for some other purpose. 	<p>If policy-based certificate separation is used to ensure certificate segmentation, identify the P2PE Assessor who confirms that:</p> <ul style="list-style-type: none"> • The method of segmentation between certificates is clearly stated in the certificate practice statement (CPS) for the CA. • Certificates issued for all of the remote key-distribution functions (i.e. encryption, POI authentication, or KDH authentication) include a mechanism to identify designation for this purpose. • Policies and procedures are in place to support and require specific function designation for each certificate issued, and there is evidence that such procedures are followed. • The SCDs involved in the remote key-delivery functions ensure that the certificates used for these functions are designated for the purpose for which they are being used. • The SCDs involved in remote key delivery ensure that certificates with remote key-delivery designation are not used for some other purpose. 	<p><Report Findings Here></p>
--------------	---	--	-------------------------------------

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings
CA/RA	<p>19-12.e Confirm that the mechanisms in place are effective in restricting the certificates to a single purpose use as noted below:</p> <ul style="list-style-type: none"> • Certificates associated with encryption for remote key-distribution functions are not used for any other purpose. • Certificates associated with authentication of the KDH are not used for any other purpose. • Certificates associated with authentication of the POI are not used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications are not used for any other purpose. 	<p>Describe how the mechanisms in place are effective in restricting the certificates to a single purpose use as follows:</p> <ul style="list-style-type: none"> • Certificates associated with encryption for remote key-distribution functions are not used for any other purpose. • Certificates associated with authentication of the KDH are not used for any other purpose. • Certificates associated with authentication of the POI are not used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications are not used for any other purpose. <p><Report Findings Here></p>
<p>20-1 POI devices must each implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.</p> <p><i>This means not only the account-data-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.</i></p> <p>POI device private keys must not exist anywhere but the specific POI device they belong to, except where generated external to the POI device and prior to the injection into the POI device.</p>		

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KMCP KLCP SP	<p>20-1.a Examine documented procedures for the loading and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are:</p> <ul style="list-style-type: none"> • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations. 	Documented procedures examined:	<Report Findings Here>
KIF KMCP KLCP SP	<p>20-1.b Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POI devices to verify that unique keys are generated and used for each POI device.</p>	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>	
KIF KMCP KLCP SP	<p>20-1.c Examine check values, hash, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI device vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.</p>	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>	
<p>20-2 If a POI device directly interfaces with more than one entity for decryption of account data (e.g., different acquiring organizations), the POI device must have a completely different and unique key or set of keys for each acquirer. These different keys, or sets of keys, must be totally independent and not variants of one another.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KMCP KLCP SP	20-2.a Examine documented procedures for generating all types of keys and verify procedures exist to ensure that unique keys or sets of keys are used for each acquiring organization and totally independent and are not variants of one another.	Documented procedures examined:	<Report Findings Here>
KIF KMCP KLCP SP	20-2.b Interview personnel and observe key-generation processes to verify that unique keys or sets of keys will be generated for each acquiring organization when required.	Personnel interviewed:	<Report Findings Here>
		Describe how the key-generation processes observed verified that unique keys or sets of keys are generated for each acquiring organization:	
		<Report Findings Here>	
<p>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 <i>ISO 11568</i> 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.</p> <p><i>This requirement refers to the use of a single “base” key to derive initial keys for many different POI devices, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys once loaded—e.g., as done with DUKPT.</i></p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI device. Examine key-generation/injection logs to ensure that sequential values included in unique key derivation are not repeated. 	Documented procedures examined:	<Report Findings Here>
		Key generation logs examined:	<Report Findings Here>
		Describe how the processes observed for generating master keys verified that the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key:	
		<ul style="list-style-type: none"> Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI. 	
<Report Findings Here>			
KIF KMCP KLCP SP	<p>20-3.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.</p>	Describe how the processes observed for generating master keys verified that derivation keys used to generate keys for multiple devices are never loaded into a POI device:	
		<Report Findings Here>	
<p>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:</p> <ul style="list-style-type: none"> 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 <p>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.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>	Documented procedures examined:	<Report Findings Here>
<p>20-5 Key-injection facilities that load DUKPT keys for various POI types for the same entity must use separate BDks per terminal type if the terminal IDs can be duplicated among the multiple types of terminals. In other words, the key-injection facility must ensure that any one given key cannot be derived for multiple devices except by chance.</p>			
KIF KLCP	<p>20-5.a If the key-injection facility loads DUKPT keys, examine documented procedures for generation and use of BDks to verify they require use of separate BDks per terminal type.</p>	Documented procedures examined:	<Report Findings Here>
KIF KLCP	<p>20-5.b Observe key-loading processes for a sample of terminal types used by a single entity, to verify that separate BDks are used for each terminal type.</p>	Sample of terminal types used by a single entity reviewed: Describe how the key-loading processes observed verified that separate BDks are used for each terminal type: <Report Findings Here>	<Report Findings Here>
<p>20-6 Remote Key-Establishment and Distribution Applications</p> <p>The following requirements apply to key-injection facilities participating in remote key-establishment and distribution applications:</p> <ul style="list-style-type: none"> • Keys must be uniquely identifiable in all hosts and POI Devices—e.g., EPPs/PEDs. Keys must be identifiable via cryptographically verifiable means—e.g., through the use of digital signatures or key check values. • Key pairs must be unique per POI device—e.g., EPPs and PEDs 			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	<p>20-6.a For techniques involving public key cryptography, examine documentation and develop a schematic to illustrate the process, including:</p> <ul style="list-style-type: none"> The size and sources of the parameters involved, and The mechanisms utilized for mutual device authentication for both the host and the POI device. 	Documented procedures examined:	<Report Findings Here>
KIF KLCP	<p>20-6.b If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that:</p> <ul style="list-style-type: none"> Cryptographic mechanisms exist to uniquely identify the keys. Key pairs used by POI devices are unique per device. 	Documented procedures examined:	<Report Findings Here>
<p>21-1 Secret or private keys must only exist in one or more of the following forms:</p> <ul style="list-style-type: none"> 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 <p>Note: Key-injection facilities may have clear-text keying material outside of a SCD when used within a secure room in accordance with Requirement 32.</p> <p>Note for hybrid decryption solutions: Clear-text Data Decryption Keys (DDKs) may temporarily be retained by the Host System in volatile memory for the purpose of decrypting account data.</p>			
CA/RA KIF KMCP KLCP SP	<p>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 (<i>with the exception of DDKs used on the Host System for hybrid decryption solutions</i>).</p>	Documented procedures examined:	<Report Findings Here>
		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>	
CA/RA KIF KMCP KLCP SP	<p>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 (<i>with the exception of DDKs used on the Host System for hybrid decryption solutions</i>).</p>	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>
		<Report Findings Here>	
<p>21-2.2 Construction of the cryptographic key must require the use of at least two key components/shares.</p>			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KMCP KLCP SP	21-2.2 Observe processes for constructing cryptographic keys to verify that at least two key components/shares are required for each key construction.	Describe how the processes observed for constructing keys verified that at least two key components are required for each key construction:	
		<Report Findings Here>	
21-2.3 Each key component/share must have one or more specified authorized custodians.			
CA/RA KIF KMCP KLCP SP	21-2.3.a Examine documented procedures for the use of key components/shares and interview key custodians and key-management supervisory personnel to verify that each key component/share is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component/share.	Key-management documentation examined:	<Report Findings Here>
		Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	21-2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components or shares are designated as key custodians for those particular components/shares.	Describe how the key-component access controls and key-custodian authorizations/assignments observed verified that all individuals with access to key components are designated as key custodians for those particular components:	
		<Report Findings Here>	
21-2.4 Procedures must exist to ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private key cryptographic key. <i>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.</i> <i>In an m-of-n scheme where n=5, where three shares are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key shares (e.g., share A and share B); and a second custodian (with, in this example, share C) would be required to reconstruct the final key, ensuring that dual control is maintained.</i>			
CA/RA KIF KMCP KLCP SP	21-2.4.a Examine documented procedures for the use of key components/shares to verify that procedures ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private cryptographic key.	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	21-2.4.b Examine key-component/share access controls and access logs to verify that authorized custodians cannot access sufficient key components or shares to reconstruct a secret or private cryptographic key.	Describe how the key-component access controls and access logs observed verified that authorized custodians cannot access sufficient key components or shares to reconstruct a secret or private cryptographic key: <Report Findings Here>	
21-3 Key components/shares must be stored as follows:			
CA/RA KIF KMCP KLCP SP	21-3 Examine documented procedures, interview responsible personnel and inspect key-component/share storage locations to verify that key components/shares are stored as outlined in Requirements 21-3.1 through 21-3.3 below:	Documented procedures examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
<p>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.</p> <p>Note: <i>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.</i></p>			
CA/RA KIF KMCP KLCP SP	21-3.1.a Examine key components and storage locations to verify that components are stored in individual opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging.	Describe how the key components and storage locations observed verified that components are stored in opaque, pre-numbered tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging: <Report Findings Here>	
CA/RA KIF KMCP KLCP SP	21-3.1.b Inspect any tamper-evident packaging used to secure key components—e.g., is the package sufficiently opaque to prevent reading of a component—and ensure that it prevents the determination of the key component without visible damage to the packaging.	Identify the P2PE Assessor who confirms that tamper-evident packaging prevents the determination of the key component without visible damage to the packaging:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	21-3.1.c Ensure clear-text key components do not exist in non-secure containers, such as databases or in software programs.	Responsible personnel interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>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).</p>	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>
<p>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).</p> <p>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.</p>			
CA/RA KIF KMCP KLCP SP	<p>21-3.2 Inspect each key component/share storage container and verify the following:</p> <ul style="list-style-type: none"> • Key components/shares for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s). 	Identify the P2PE Assessor who confirms that for each key component storage container: <ul style="list-style-type: none"> • Key components for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s). 	<Report Findings Here>
<p>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.</p>			

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA KIF KMCP KLCP SP	21-3.3 Interview responsible personnel and observe implemented processes to verify that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token’s owner—or designated backup(s)—has possession of both the token and its access code.	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the implemented processes observed verified that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token’s owner—or designated backup(s)—has possession of both the token and its access code:	
		<Report Findings Here>	
21-4 Private keys used to sign certificates, certificate status lists, messages, or for key protection must exist only in one or more of the following forms: <ul style="list-style-type: none"> • Within a secure cryptographic device that meets applicable PCI requirements for such a device, • Encrypted using an algorithm and key size of equivalent or greater strength, or • As components using a recognized (e.g., Shamir) secret-sharing scheme. 			
RKD CA/RA	21-4.a Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.	Documented key-management procedures examined:	<Report Findings Here>
RKD CA/RA	21-4.b Observe key-management operations and interview key custodians and key-management supervisory personnel to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.	Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
		Describe how the key-management operations observed verified that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times:	
		<Report Findings Here>	
22-1 Procedures for known or suspected compromised keys must include the following:			
CA/RA KIF KMCP KLCP SP	22-1 Verify documented procedures exist for replacing known or suspected compromised keys that includes all of the following (22-1.1 through 22-1.5 below):	Documented procedures examined:	<Report Findings Here>
22-1.1 Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised.			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>22-1.1 Interview responsible personnel and observe implemented processes to verify key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised.</p>	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the implemented processes observed verified that key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD (or, for hybrid decryption solutions, the Host System) has been compromised:	
		<Report Findings Here>	
<p>22-1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.</p>			
CA/RA KIF KMCP KLCP SP	<p>22-1.2 Interview responsible personnel and observe implemented processes to verify that if unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.</p>	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the implemented processes observed verified that if unauthorized alteration is suspected, new keys are not installed until the SCD (or, for hybrid decryption solutions, the Host System) has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification:	
		<Report Findings Here>	
<p>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).</p> <p>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.</p> <p>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</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>22-1.3 Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, and all the following are performed:</p> <ul style="list-style-type: none"> 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>
		<p>Describe how the implemented processes observed verified that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, the following are performed:</p> <ul style="list-style-type: none"> Processing with that key is halted, and the key is replaced with a new unique key. Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key. 	
		<Report Findings Here>	
<p>22-1.4 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including:</p> <ul style="list-style-type: none"> 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. 			
CA/RA KIF KMCP KLCP SP	<p>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).</p>	Responsible personnel interviewed:	<Report Findings Here>
		<p>Describe how the implemented processes observed verified that key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s):</p>	
		<Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>22-1.4.b A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including:</p> <ul style="list-style-type: none"> • Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc. 	Identify the P2PE Assessor who confirms that notifications include a damage assessment including, where necessary, the engagement of outside consultants and details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	<Report Findings Here>
<p>22-1.5 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to:</p> <ul style="list-style-type: none"> • 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 • <i>Host System tamper-detection mechanism has been activated, for hybrid decryption solutions</i> 			
CA/RA KIF KMCP KLCP SP	<p>22-1.5 Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, at a minimum, the following events:</p> <ul style="list-style-type: none"> • 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 • <i>Host System tamper-detection mechanism has been activated, for hybrid decryption solutions</i> 	Responsible personnel interviewed:	<Report Findings Here>
		Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>22-2 If attempts to load a secret key or key component into an KLD or POI device (<i>or a Host System, for hybrid decryption solutions</i>) fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (<i>or Host System</i>).</p>			
CA/RA KIF KMCP KLCP SP	<p>22-2 Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an KLD or POI device (<i>or a Host System, for hybrid decryption solutions</i>) 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 (<i>or Host System</i>).</p>	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 (<i>or Host System</i>):	
		<Report Findings Here>	
<p>22-3 Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.</p>			
CA/RA	<p>22-3 Through the examination of documented procedures, interviews, and observation, confirm that Root CAs provide for segmentation of risk to address key compromise.</p>	Documented procedures examined:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
		Describe the observations that confirmed that Root CAs provide for segmentation of risk to address key compromise:	
<Report Findings Here>			
<p>22-4 Mechanisms must be in place to respond to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke or otherwise invalidate the usage of subordinate certificates, and notification of affected entities.</p>			
CA/RA	<p>22-4 Examine documented procedures to verify that mechanisms are defined to respond to compromise of a CA. Verify the mechanisms include procedures to:</p> <ul style="list-style-type: none"> • Revoke subordinate certificates, and • Notify affected entities. 	Documented procedures examined:	<Report Findings Here>
<p>22-4.1 The CA must cease issuance of certificates if a compromise is known or suspected and perform a damage assessment, including a documented analysis of how and why the event occurred.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	22-4.1.a Examine documented procedures to verify that the following are required in the event a compromise is known or suspected: <ul style="list-style-type: none"> The CA will cease issuance of certificates. The CA will perform a damage assessment, including a documented analysis of how and why the event occurred. 	Documented procedures examined:	<Report Findings Here>
CA/RA	22-4.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: <ul style="list-style-type: none"> The CA will cease issuance of certificates. The CA will perform a damage assessment, including a documented analysis of how and why the event occurred. 	Responsible personnel interviewed:	<Report Findings Here>
22-4.2 In the event of confirming a compromise, the CA must determine whether to revoke and reissue all signed certificates with a newly generated signing key.			
CA/RA	22-4.2.a Examine documented procedures to verify that in the event of a confirmed compromise, procedures are defined for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.	Documented procedures examined:	<Report Findings Here>
CA/RA	22-4.2.b Interview responsible personnel to verify procedures are followed for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.	Responsible personnel interviewed:	<Report Findings Here>
22-4.3 Mechanisms (e.g., time stamping) must exist to prevent the usage of fraudulent certificates, once identified.			
CA/RA	22-4.3.a Examine documented procedures to verify that mechanisms are defined to prevent the usage of fraudulent certificates.	Documented procedures examined:	<Report Findings Here>
CA/RA	22-4.3.b Interview responsible personnel and observe implemented mechanisms to verify the prevention of the use of fraudulent certificates	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the implemented mechanisms observed verified the prevention of the use of fraudulent certificates:	<Report Findings Here>
22-4.4 The compromised CA must notify any superior or subordinate CAs of the compromise. The compromise damage analysis must include a determination of whether subordinate CAs and KDHS must have their certificates reissued and distributed to them or be notified to apply for new certificates.			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	<p>22-4.4.a Examine documented procedures to verify that the following procedures are required in the event of a compromise:</p> <ul style="list-style-type: none"> • The CA will notify any superior CAs. The CA will notify any subordinate CAs. • The CA will perform a damage assessment to determine the need to either: • Reissue and distribute certificates to affected parties, or • Notify the affected parties to apply for new certificates. 	Documented procedures examined:	<Report Findings Here>
CA/RA	<p>22-4.4.b Interview responsible personnel to verify that the following procedures are performed in the event a compromise:</p> <ul style="list-style-type: none"> • The CA notifies any superior CAs. • The CA notifies any subordinate CAs. • The CA performs a damage assessment to determine the need to either: <ul style="list-style-type: none"> – Reissues and distributes certificates to affected parties, or – Notifies the affected parties to apply for new certificates. 	Responsible personnel interviewed:	<Report Findings Here>
<p>22-5 Minimum cryptographic strength for the CA system must be:</p> <ul style="list-style-type: none"> • Root and subordinate CAs have a minimum RSA 2048 bits or equivalent; • EPP/PED devices and KDHS have a minimum RSA 2048 bits or equivalent. 			
CA/RA	<p>22-5.a Interview appropriate personnel and examine documented procedures for the creation of these keys.</p>	Appropriate personnel interviewed:	<Report Findings Here>
		Documented procedures Examined:	<Report Findings Here>
CA/RA	<p>22-5.b Verify that the following minimum key sizes exist for RSA keys or the equivalent for the algorithm used as defined in Annex C:</p> <ul style="list-style-type: none"> • 2048 for CAs • 2048 for KDHS and POI devices 	Appropriate personnel interviewed:	<Report Findings Here>
		Documented procedures Examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>23-1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from account-data keys.</p> <p>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.</p>			
CA/RA KIF KMCP KLCP SP	23-1.a Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.	Documented procedures reviewed:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	23-1.b Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.	Describe how the processes observed verified that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge:	
		<Report Findings Here>	
<p>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.</p> <p><i>A logical configuration is defined as one where all the components form a system used to undertake a particular task and are managed and controlled under a single operational and security policy.</i></p>			
CA/RA KIF KMCP KLCP SP	23-2.a Interview responsible personnel to determine which host MFKs keys exist as variants. Note: Some HSMS may automatically generate variants or control vectors for specific keys, but it is still up to the entity to specify exact usage.	Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	23-2.b Examine vendor documentation to determine support for key variants.	Vendor documentation examined:	<Report Findings Here>
CA/RA KIF KMCP	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	Describe how the review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used verified that variants of the MFK are not used external to the logical configuration that houses the MFK:	

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
KLCP SP	variants of the MFK are not used external to the logical configuration that houses the MFK.	<Report Findings Here>	
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>			
CA/RA KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • Variants used as KEKs must only be calculated from other key-encrypting keys • Variants of working keys must only be calculated from other working keys. 	Documented procedures examined:	<Report Findings Here>
		Describe how the implemented processes observed verified that reversible key transformations are not used across different levels of the key hierarchy, as follows:	
		<ul style="list-style-type: none"> • 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>
<p>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.</p>			
CA/RA KIF KMCP KLCP SP	24-1.a Verify documented procedures are in place for destroying secret or private keys, and their key components that are no longer used or that have been replaced by a new key.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-1.b Identify a sample of keys and key components that are no longer used or have been replaced. For each item in the sample, interview responsible personnel and examine key-history logs and key-destruction logs to verify that all keys have been destroyed.	Sample of keys and key components that are no longer used or have been replaced reviewed:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
		Key-history logs examined:	<Report Findings Here>

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
		Key-destruction logs examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-1.c Examine storage locations for the sample of destroyed keys to verify they are no longer kept.	Describe how the storage locations observed verified that the sample of destroyed keys are no longer kept:	
		<Report Findings Here>	
<p>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.</p> <p>Note: Key destruction for keys installed in HSMs and POI devices is addressed in Requirement 31.</p>			
CA/RA KIF KMCP KLCP SP	24-2.a Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.	Describe how the key-destruction processes observed verified that no part of the key or component can be recovered:	
		<Report Findings Here>	
<p>24-2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic database backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO-9564 or ISO-11568.</p> <p>For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.</p>			
CA/RA KIF KMCP KLCP SP	24-2.1.a Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—must be destroyed following the procedures outlined in ISO-9564 or ISO-11568.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-2.1.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or component—are destroyed following the procedures outlined in ISO-9564 or ISO-11568.	Describe how the key-destruction processes observed verified that keys on all other storage media types in all permissible forms—physically secured, enciphered, or component—are destroyed following the procedures outlined in ISO-9564 or ISO-11568:	
		<Report Findings Here>	

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
24-2.2 The key-destruction process must be observed by a third party other than the custodians of any component of that key—i.e., the third party must not be a key custodian for any part of the key being destroyed. The third-party witness must sign an affidavit of destruction.			
CA/RA KIF KMCP KLCP SP	24-2.2.a Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian for any component of that key.	Identify the P2PE Assessor who confirms the key-destruction process is witnessed by a third party other than a key custodian for any component of that key:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-2.2.b Inspect key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key destruction process.	Key-destruction logs inspected:	<Report Findings Here>
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.			
CA/RA KIF KMCP KLCP SP	24-2.3.a Verify documented procedures exist for destroying key components of keys once the keys are successfully loaded and validated as operational.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	24-2.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.	Describe how the key-conveyance/loading processes observed verified that any key components are destroyed once the keys are successfully loaded and validated as operational:	<Report Findings Here>
25-1 To reduce the opportunity for key compromise, the number of key custodians must be limited to the minimum required for operational efficiency. Controls must include:			
CA/RA KIF KMCP KLCP SP	25-1 Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:	Key custodians interviewed:	<Report Findings Here>
		Key-management supervisory personnel interviewed:	<Report Findings Here>
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.			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	25-1.1.a Examine key-custodian assignments for each component to verify that: <ul style="list-style-type: none"> • Key custodian(s) are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel. 	Describe how the key-custodian assignments reviewed for each component verified that: <ul style="list-style-type: none"> • 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. 	
		<i><Report Findings Here></i>	
25-1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.			
CA/RA KIF KMCP KLCP SP	25-1.2.a Examine completed key-custodian forms to verify that key custodians sign the form.	Completed key-custodian forms examined:	<i><Report Findings Here></i>
CA/RA KIF KMCP KLCP SP	25-1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form.	Completed key-custodian forms examined:	<i><Report Findings Here></i>
25-1.3 Each key-custodian form provides the following: <ul style="list-style-type: none"> • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>25-1.3 Examine all key-custodian forms to verify that they include the following:</p> <ul style="list-style-type: none"> • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access 	Completed key-custodian forms examined:	<Report Findings Here>
<p>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.</p> <p>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.</p> <p>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).</p> <p>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.</p> <p>When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented.</p> <p>Organizations that are of insufficient size that they cannot support the reporting-structure requirement must:</p> <ul style="list-style-type: none"> • Ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian); • Receive explicit training to instruct them from sharing key components with their direct manager; • Sign key-custodian agreements that include an attestation to the requirement; and • Receive training that includes procedures to report any violations. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	<p>25-1.4.a Examine key-custodian assignments and organization charts to confirm the following:</p> <ul style="list-style-type: none"> Key custodians that form the necessary threshold to create a key do not directly report to the same individual. Neither direct reports nor the direct reports in combination with their immediate supervisors possess the necessary threshold of key components sufficient to form any given key. Key custodians are not and have not been a custodian for another component/share of a key where that collectively would constitute a quorum to form the actual key. 	Documented key-custodian assignments examined:	<Report Findings Here>
		Documented organization charts examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> Ensure key custodians do not report to each other. Receive explicit training to instruct them from sharing key components with their direct manager. Sign key-custodian agreement that includes an attestation to the requirement. Ensure training includes procedures to report any violations. 	Documented procedures examined:	<Report Findings Here>
<p>25-2 All user access to material that can be used to construct secret and private keys (such as key components or key shares used to reconstitute a key) must be directly attributable to an individual user (e.g., through the use of unique IDs).</p> <p>Note: Individual user IDs may be assigned to a role or group.</p>			
CA/RA	<p>25-2.a Examine documented procedures to confirm that access to material that can be used to construct secret and private keys is directly attributable to an individual user.</p>	Documented procedures examined:	<Report Findings Here>
CA/RA	<p>25-2.b Observe the access-control mechanisms in place to verify that access to material that can be used to construct secret and private keys is directly attributable to an individual user.</p>	Describe how the access-control mechanisms observed verified that access to material that can be used to construct secret and private keys is directly attributable to an individual user:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-2.1 All user access must be restricted to actions authorized for that role.			
Note: Examples of how access can be restricted include the use of CA software and operating-system and procedural controls.			
CA/RA	25-2.1.a Examine documented procedures to confirm that access to material that can be used to construct secret and private keys must be restricted to actions authorized for that role.	Documented procedures examined:	<Report Findings Here>
CA/RA	25-2.1.b Observe user role assignments and access-control mechanisms to verify that access to material that can be used to construct secret and private keys is restricted to actions authorized for that role.	Describe how the user role assignments and access-control mechanisms observed verified that access to material that can be used to construct secret and private keys is restricted to actions authorized for that role: <Report Findings Here>	
25-3 The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include the following:			
25-3.1 CA systems that issue certificates to other CAs and KDHS must be operated offline using a dedicated closed network (not a network segment). <ul style="list-style-type: none"> The network must only be used for certificate issuance and/or revocation. Outside network access (e.g., using a separate platform in the DMZ) must exist only for the purposes of “pushing” certificate-status information to relying parties (e.g., KDHS). 			
CA/RA	25-3.1 Examine network diagrams and observe network and system configurations to verify: <ul style="list-style-type: none"> CA systems that issue certificates to other CAs and KDHS are operated offline using a dedicated closed network (not a network segment). The network is only used for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access must exist only for the purposes of “pushing” certificate-status information to relying parties (e.g., KDHS). 	Network diagrams examined Describe how the network diagrams and network and system configurations observed verified that: <ul style="list-style-type: none"> CA systems that issue certificates to other CAs and KDHS are operated offline using a dedicated closed network (not a network segment). The network is only used for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access shall exist only for the purposes of “pushing” certificate-status information to relying parties (e.g., KDHS) <Report Findings Here>	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-3.2 For CAs operated online—e.g., POI-signing CAs: CA or Registration Authority (RA) software updates must not be done over the network (local console access must be used for CA or RA software updates).			
CA/RA	25-3.2 Examine software update processes to verify that local console access is used for all CA or RA software updates.	Documented software update processes examined:	<Report Findings Here>
25-3.3 For CAs operated online—e.g., POI-signing CAs: Non-console access must use multi-factor authentication. This also applies to the use of remote console access.			
CA/RA	25-3.3 Examine remote-access mechanisms and system configurations to verify that all non-console access, including remote access, requires multi-factor authentication.	Describe how the remote-access mechanisms and system configurations examined verified that all non-console access, including remote access, requires multi-factor authentication: <Report Findings Here>	
25-3.4 For CAs operated online—e.g., POI-signing CAs: Non-console user access to the CA or RA system environments must be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. Note: Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.			
CA/RA	25-3.4.a Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions.	Describe how the non-console access mechanisms and system configurations examined verified that all non-console user access is protected by authenticated encrypted sessions: <Report Findings Here>	
CA/RA	25-3.4.b Observe an authorized CA personnel attempt non-console access to the host platform using valid CA credentials without using an authenticated encrypted session to verify that non-console access is not permitted.	Describe how observation of the authorized CA personnel's attempted nonconsole access to the host platform using valid CA credentials without using an authenticated encrypted session verified that non-console access is not permitted: <Report Findings Here>	
25-3.5 CA certificate (for POI/KDH authentication and validity status checking) signing keys must only be enabled under at least dual control. Note: Certificate requests may be vetted (approved) using single user logical access to the RA application.			
CA/RA	25-3.5.a Examine the certificate security policy and certification practice statement to verify that CA certificate-signing keys must only be enabled under at least dual control.	Documented certificate security policy and certification practice statement examined:	<Report Findings Here>
CA/RA	25-3.5.b Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.	Describe how the certificate-signing processes observed verified that signing keys are enabled only under at least dual control: <Report Findings Here>	

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-4 The CA must require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as “dual control.” At a minimum, there must be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).			
CA/RA	25-4.a Examine documented procedures to verify they include following: <ul style="list-style-type: none"> Definition of critical functions of the CA Separation of duties to prevent one person from maliciously using a CA system without detection Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s) 	Documented procedures examined:	<Report Findings Here>
CA/RA	25-4.b Observe CA operations and interview responsible personnel to verify: <ul style="list-style-type: none"> Definition of critical functions of the CA Separation of duties to prevent one person from maliciously using a CA system without detection Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s) 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the CA operations observed verified:	
		<ul style="list-style-type: none"> Definition of critical functions of the CA Separation of duties to prevent one person from maliciously using a CA system without detection Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s) 	
		<Report Findings Here>	
25-5 All CA systems that are not operated exclusively offline must be hardened to prevent insecure network access, to include:			
<ul style="list-style-type: none"> Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, telnet, ftp, etc.) must be removed or disabled. Unnecessary ports must also be disabled. Documentation must exist to support the enablement of all active services and ports. 			
CA/RA	25-5.a Examine system documentation to verify the following is required: <ul style="list-style-type: none"> Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, etc., commands in UNIX) must be removed or disabled. Unnecessary ports must also be disabled. Documentation must exist to support the enablement of all active services and ports. 	System documentation examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	<p>25-5.b For a sample of systems, examine documentation supporting the enablement of active services and ports, and observe system configurations to verify:</p> <ul style="list-style-type: none"> Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, etc., commands in UNIX) are removed or disabled. Unnecessary ports are disabled. There is documentation to support all active services and ports. 	Sample of systems reviewed:	<Report Findings Here>
		Documentation examined:	<Report Findings Here>
		Describe how the observed system configurations observed verified that: <ul style="list-style-type: none"> Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, etc., commands in UNIX) are removed or disabled. Unnecessary ports are disabled. There is documentation to support all active services and ports. 	
		<Report Findings Here>	
<p>25-5.1 All vendor-default IDs must be changed, removed, or disabled unless necessary for a documented and specific business reason. Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades must only be enabled when necessary and otherwise must be disabled from login.</p>			
CA/RA	<p>25-5.1.a Examine documented procedures to verify that:</p> <ul style="list-style-type: none"> Vendor-default IDs are changed, removed, or disabled unless necessary for a documented and specific business reason. Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades are only be enabled when required and otherwise must be disabled from login. 	Documented procedures examined:	<Report Findings Here>
CA/RA	<p>25-5.1.b Examine system configurations and interview responsible personnel to verify that:</p> <ul style="list-style-type: none"> Vendor-default IDs are changed, removed or disabled unless necessary for a documented and specific business reason. Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades are only be enabled when required and otherwise must be disabled from login. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the system configurations observed verified that vendor-default IDs are changed, removed or disabled unless necessary for a documented and specific business reason:	
		<Report Findings Here>	
		Describe how the system configurations observed verified that vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades are only be enabled when required and otherwise must be disabled from login:	
<Report Findings Here>			

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-5.2 Vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step must be changed, removed, or disabled before installing a system on the network.			
CA/RA	25-5.2.a Examine documented procedures to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.	Documented procedures examined:	<i><Report Findings Here></i>
CA/RA	25-5.2.b Examine system configurations and interview responsible personnel to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.	Responsible personnel interviewed:	<i><Report Findings Here></i>
		Describe how the system configurations observed verified that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network:	
		<i><Report Findings Here></i>	
25-6 Audit trails must include but not be limited to the following:			
<ul style="list-style-type: none"> All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, destruction, and certificate generation or revocation The identity of the person authorizing the operation The identities of all persons handling any key material (such as key components or keys stored in portable devices or media) Protection of the logs from alteration and destruction 			
CA/RA	25-6.a Examine system configurations and audit trails to verify that all key-management operations are logged.	Describe how the system configurations and audit trails observed verified that all key-management operations are logged:	
		<i><Report Findings Here></i>	
CA/RA	25-6.b For a sample of key-management operations, examine audit trails to verify they include: <ul style="list-style-type: none"> The identity of the person authorizing the operation The identities of all persons handling any key material Mechanisms exist to protect logs from alteration and destruction 	Sample of key-management operations reviewed:	<i><Report Findings Here></i>
		Describe how the examined audit trails for a sample of key-management operations verified they include: <ul style="list-style-type: none"> The identity of the person authorizing the operation The identities of all persons handling any key material Mechanisms exist to protect logs from alteration and destruction 	
		<i><Report Findings Here></i>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-6.1 Audit logs must be archived for a minimum of two years.			
CA/RA	25-6.1 Examine audit trail files to verify that they are archived for a minimum of two years.	Describe how the examined audit trails verified that they are archived for a minimum of two years:	
		<Report Findings Here>	
25-6.2 Records pertaining to certificate issuance and revocation must, at a minimum, be retained for the life of the associated certificate.			
CA/RA	25-6.2.a For a sample of certificate issuances, examine audit records to verify that the records are retained for at least the life of the associated certificate.	Sample of certificate issuances Examined:	<Report Findings Here>
		Audit records examined:	<Report Findings Here>
CA/RA	25-6.2.b For a sample of certificate revocations, examine audit records to verify that the records are retained for at least the life of the associated certificate.	Sample of certificate revocations examined:	<Report Findings Here>
		Audit records examined:	<Report Findings Here>
25-6.3 Logical events are divided into operating-system and CA application events. For both, the following must be recorded in the form of an audit record: <ul style="list-style-type: none"> • Date and time of the event, • Identity of the entity and/or user that caused the event, • Type of event, and • Success or failure of the event 			
CA/RA	25-6.3.a Examine audit trails to verify that logical events are divided into operating-system and CA application events.	Describe how the examined audit trails verified that logical events are divided into operating system and CA application events:	
		<Report Findings Here>	
CA/RA	25-6.3.b Examine a sample of operating-system logs to verify they contain the following information: <ul style="list-style-type: none"> • Date and time of the event, • Identity of the entity and/or user that caused the event, • Type of event, and • Success or failure of the event. 	Sample of operating-system logs examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	<p>25-6.3.c Examine a sample of application logs to verify they contain the following information:</p> <ul style="list-style-type: none"> Date and time of the event, Identity of the entity and/or user that caused the event, Type of event, and Success or failure of the event. 	Sample of application logs examined:	<Report Findings Here>
<p>25-7 CA application logs must use a digital signature or a symmetric MAC (based on one of the methods stated in <i>ISO 16609 – Banking – Requirements for message authentication using symmetric techniques</i>) mechanism for detection of alteration.</p> <p>The signing/MACing key(s) used for this must be protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document.</p>			
CA/RA	<p>25-7.a Examine log security controls to verify that CA application logs use a digital signature or a symmetric MAC (based on one of the methods stated in <i>ISO 16609 – Banking – Requirements for message authentication using symmetric techniques</i>) mechanism for detection of alteration.</p>	Describe how log security controls verified that CA application logs use a digital signature or a symmetric MAC (based on one of the methods stated in <i>ISO 16609 – Banking – Requirements for message authentication using symmetric techniques</i>) mechanism for detection of alteration:	<Report Findings Here>
CA/RA	<p>25-7.b Examine documentation and interview personnel and observe to verify that signing/MACing key(s) used for this are protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document.</p>	Documentation examined:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
		Describe how the observation of signing/MACing keys used for this verified they are protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document:	<Report Findings Here>
<p>25-7.1 Certificate-processing system components operated online must be protected by a firewall(s) from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to:</p> <ul style="list-style-type: none"> Deny all services not explicitly permitted. Disable or remove all unnecessary services, protocols, and ports. Fail to a configuration that denies all services and require a firewall administrator to re-enable services after a failure. Disable source routing on the firewall. Not accept traffic on its external interfaces that appears to be coming from internal network addresses. Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled. 			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings
CA/RA	25-7.1.a Examine network and system configurations to verify that certificate-processing system components operated online are protected from unauthorized access by firewall(s).	Describe how the observed network and system configurations verified that certificate-processing system components operated online are protected from unauthorized access by firewall(s): <i><Report Findings Here></i>
CA/RA	25-7.1.b Examine firewall configurations for verify they are configured to: <ul style="list-style-type: none"> • Deny all services not explicitly permitted. • Disable or remove all unnecessary services, protocols, and ports. • Fail to a configuration that denies all services and require a firewall administrator to re-enable services after a failure. • Disable source routing on the firewall. • Not accept traffic on its external interfaces that appears to be coming from internal network addresses. • Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. • Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled. 	Describe how the observed firewall configurations verified they are configured to: <ul style="list-style-type: none"> • Deny all services not explicitly permitted. • Disable or remove all unnecessary services, protocols, and ports. • Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure. • Disable source routing on the firewall. • Not accept traffic on its external interfaces that appears to be coming from internal network addresses. • Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. • Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled. <i><Report Findings Here></i>
25-7.2 Online certificate-processing systems must employ individually or in combination network and host-based intrusion detection systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments, must be covered.		
CA/RA	25-7.2.a Observe network-based and/or host-based IDS configurations to verify that on-line certificate-processing systems are protected by IDS to detect inappropriate access.	Describe how the observed network-based and/or host-based IDS configurations verified that on-line certificate-processing systems are protected by IDS to detect inappropriate access: <i><Report Findings Here></i>
CA/RA	25-7.2.b Verify that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.	Describe how the observed network-based and/or host-based IDS configurations verified that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments: <i><Report Findings Here></i>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25-8 Implement user-authentication management for all system components as follows:			
25.8.1 Initial, assigned passphrases are pre-expired (user must replace at first logon).			
CA/RA	25.8.1 Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and are pre-expired.	Documented password procedures examined:	<Report Findings Here>
		Describe the observations that verified that security personnel set first-time passwords for new users, and reset passwords for existing users, to a unique value for each user and are pre-expired:	
		<Report Findings Here>	
25.8.2 Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.			
CA/RA	25.8.2.a For a sample of system components, examine user ID lists to verify the following: <ul style="list-style-type: none"> • Generic user IDs and accounts are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used. 	Sample of system components examined:	<Report Findings Here>
		Describe how user ID lists verified that: <ul style="list-style-type: none"> • Generic user IDs and accounts are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used. 	
		<Report Findings Here>	
CA/RA	25.8.2.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	Documented authentication policies/procedures examined:	<Report Findings Here>
CA/RA	25.8.2.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed—even if requested.	System administrators interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25.8.3 If passwords are used, system-enforced expiration life must not exceed 90 days and a minimum life at least one day.			
CA/RA	25.8.3 For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days and have a minimum life of at least one day.	Sample of system components examined:	<Report Findings Here>
		Describe how the observed system configuration settings verified that user password parameters are set to require users to change passwords at least every 90 days and have a minimum life of at least one day:	
		<Report Findings Here>	
25.8.4 Passwords must have a minimum length of eight characters using a mix of alphabetic, numeric, and special characters or equivalent strength as defined in <i>NIST SP 800-63B</i> .			
CA/RA	25.8.4 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least eight characters long and contain numeric, alphabetic, and special characters or equivalent strength as defined in <i>NIST SP 800-63B</i> .	Sample of system components examined:	<Report Findings Here>
		Describe how the observed system configuration settings verified that password parameters are set to require passwords to be at least eight characters long and contain numeric, alphabetic, and special characters:	
		<Report Findings Here>	
25.8.5 Limit repeated access attempts by locking out the user ID after not more than five attempts.			
CA/RA	25.8.5 For a sample of system components, obtain and inspect 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.	Sample of system components examined:	<Report Findings Here>
		Describe how the observed system configuration settings 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>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
25.8.6 Authentication parameters must require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.			
CA/RA	25.8.6 For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.	Sample of system components examined:	<Report Findings Here>
		Describe how the observed system configuration settings verified that authentication parameters are set to require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months:	
		<Report Findings Here>	
25.8.7 Passwords are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.			
CA/RA	25.8.7 For a sample of system components, obtain and inspect system configuration settings to verify that passwords are not stored unless encrypted as part of a proprietary one-way hash.	Sample of system components examined:	<Report Findings Here>
		Describe how the observed system configuration settings verified that passwords are not stored unless encrypted as part of a proprietary one-way hash:	
		<Report Findings Here>	
25.8.8 The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.			
CA/RA	25.8.8.a Examine policies and procedures and interview personnel to determine that the embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.	Documented policies and procedures examined:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
CA/RA	25.8.8.b Inspect a sample of shell scripts, command files, communication scripts, etc. to verify that passwords are not embedded in shell scripts, command files, or communication scripts.	Sample of shell scripts, command files, communication scripts, etc. inspected:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>25.8.9 Where log-on security tokens (e.g., smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage. The PIN/passphrase must be at least eight decimal digits in length, or equivalent.</p> <p>Note: Log-on security tokens (e.g., smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.</p>			
CA/RA	<p>25.8.9.a If log-on security tokens are used, observe devices in use to verify that the security tokens have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage.</p>	Describe how the observed devices in use verified that the security tokens have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage:	
<Report Findings Here>			
CA/RA	<p>25.8.9.b Examine token-configuration settings to verify parameters are set to require that PINs/passwords be at least eight decimal digits in length, or equivalent.</p>	Describe how the observed token-configuration settings verified that parameters are set to require PINs/passwords be at least eight decimal digits in length, or equivalent:	
<Report Findings Here>			
<p>25.9 Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.</p>			
CA/RA	<p>25.9.a Examine documented procedures and system configuration standards to verify a method is defined to synchronize all critical system clocks and times for all systems involved in key-management operations.</p>	Documented procedures and system configuration standards examined:	<Report Findings Here>
CA/RA	<p>25.9.b For a sample of critical systems, examine the time-related system parameters to verify that system clocks and times are synchronized for all systems involved in key-management operations.</p>	Sample of critical systems examined:	<Report Findings Here>
Describe how the observed time-related system parameters verified that system clocks and times are synchronized for all systems involved in keymanagement operations:		<Report Findings Here>	
CA/RA	<p>25.9.c If a manual process is defined, verify that the documented procedures require that it occur at least quarterly.</p>	Documented procedures examined:	<Report Findings Here>
CA/RA	<p>25.9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.</p>	Describe how the observed system configurations and synchronization logs verified that where a manual process is defined, that the process occurs at least quarterly:	
<Report Findings Here>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>26-1 Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. These logs must be archived for a minimum of two years subsequent to key destruction.</p> <p>At a minimum, logs must include the following:</p> <ul style="list-style-type: none"> 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) 			
CA/RA KIF KMCP KLCP SP	<p>26-1.a Examine log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are:</p> <ul style="list-style-type: none"> Removed from secure storage Loaded to an SCD 	Log files examined:	<i><Report Findings Here></i>
		Describe how log files and audit log settings verified that logs are kept for any time that keys, key components, or related materials are:	
		<ul style="list-style-type: none"> Removed from secure storage Loaded to an SCD 	
<i><Report Findings Here></i>			
CA/RA KIF KMCP KLCP SP	<p>26-1.b Examine log files and audit log settings to verify that logs include the following:</p> <ul style="list-style-type: none"> Date and time in/out Key component identifier Purpose of access Name and signature of custodian accessing the component Name and signature of a non-custodian (for that component/share) witness Tamper-evident and authenticable package number (if applicable) 	Log files examined:	<i><Report Findings Here></i>
		Describe how log files and audit log settings verified that logs include the following:	
		<ul style="list-style-type: none"> 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) 	
<i><Report Findings Here></i>			
CA/RA KIF KMCP KLCP SP	<p>26-1.c Examine audit trail files to verify that they are archived for a minimum of two years subsequent to key destruction.</p>	Audit trail files examined:	<i><Report Findings Here></i>
		Describe how the audit train files examined verified that they are archived for a minimum of two years subsequent to key destruction.	
		<i><Report Findings Here></i>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
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.			
CA/RA KIF KMCP KLCP SP	27-1.a Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following:	Responsible personnel interviewed:	<Report Findings Here>
		Documented procedures examined:	<Report Findings Here>
		Backup records examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	27-1.b Observe backup processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys.	Describe how the backup processes observed verified that backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys:	
		<Report Findings Here>	
CA/RA KIF KMCP KLCP SP	27-1.c Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: <ul style="list-style-type: none"> Securely stored with proper access controls Under at least dual control Subject to at least the same level of security control as operational keys as specified in this document 	Documented procedures examined:	<Report Findings Here>
		Personnel interviewed:	<Report Findings Here>
		OR Describe how backup storage locations verified that backups are maintained as follows: <ul style="list-style-type: none"> 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>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>27-2 If backup copies are created, the following must be in place:</p> <ul style="list-style-type: none"> • Creation (including cloning) of top-level keys—e.g., MFKs—must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components. 			
CA/RA KIF KMCP KLCP SP	<p>27-2 Interview responsible personnel and observe backup processes to verify the following:</p> <ul style="list-style-type: none"> • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components. 	Responsible personnel interviewed:	<i><Report Findings Here></i>
		Describe how the backup processes observed verified that: <ul style="list-style-type: none"> • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process • All requirements applicable for the original keys also apply to any backup copies of keys and their components. 	
		<i><Report Findings Here></i>	
<p>28-1 Written procedures must exist and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as:</p> <ul style="list-style-type: none"> • 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 			
CA/RA KIF KMCP KLCP SP	<p>28-1.a Examine documented procedures for key-administration operations to verify they cover all activities related to key administration, and include:</p> <ul style="list-style-type: none"> • Training of all key custodians regarding their responsibilities, and forming part of their annual security training • Role definition—nominated individual with overall responsibility • Background checks for personnel (within the constraints of local laws) • Management of personnel changes, including revocation of access control and other privileges when personnel move 	Documented procedures examined:	<i><Report Findings Here></i>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	28-1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.	Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	28-1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.	Personnel interviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	28-1.d Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).	Responsible HR personnel interviewed:	<Report Findings Here>
28-2 CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.			
CA/RA	28-2.a Examine documented procedures to verify: <ul style="list-style-type: none"> CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems. 	Documented procedures examined:	<Report Findings Here>
CA/RA	28-2.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.	Describe how the observed CA system configurations and operations verified that they are dedicated to certificate issuance and management: <Report Findings Here>	
CA/RA	28-2.c Observe system and network configurations and physical access controls to verify that all physical and logical CA system components are separated from key-distribution systems.	Describe how the observed system and network configurations and physical access controls verified that all physical and logical CA system components are separated from key-distribution systems: <Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>28-3 Each CA operator must develop a certification practice statement (CPS). (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content.)</p> <ul style="list-style-type: none"> The CPS must be consistent with the requirements described within this document. The CA must operate in accordance with its CPS. <p>Note: This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific, single document or a collection of specific documents.</p>			
CA/RA	28-3.a Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document.	Documented certification practice statement (CPS) examined:	<Report Findings Here>
CA/RA	28-3.b Examine documented operating procedures to verify they are defined in accordance with the CPS.	Documented operating procedures examined:	<Report Findings Here>
CA/RA	28-3.c Interview personnel and observe CA processes to verify that CA operations are in accordance with its CPS.	Personnel interviewed:	<Report Findings Here>
		Describe how the observed CA processes verified that CA operations are in accordance with its CPS:	
		<Report Findings Here>	
<p>28-4 Each CA operator must develop a certificate policy. (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content.)</p>			
CA/RA	28-4 Examine documented certificate policy to verify that the CA has one in place.	Documented certificate policy reviewed:	<Report Findings Here>
<p>28-5 Documented procedures exist and are demonstrably in use by CAs to validate the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key where the certificate request is not generated within the same secure room meeting the requirements of the Level 3 environment defined below. These procedures must include at a minimum, two or more of the following for KDH certificate requests:</p> <ul style="list-style-type: none"> Verification of the certificate applicant's possession of the associated private key through the use of a digitally signed certificate request pursuant to PKCS #10 or another cryptographically-equivalent demonstration; Determination that the organization exists by using at least one third-party identity-proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization; Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant to confirm that the organization has authorized the certificate application, confirmation of the employment of the representative submitting the certificate application on behalf of the certificate applicant, and confirmation of the authority of the representative to act on behalf of the certificate applicant; Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant's representative to confirm that the person named as representative has submitted the certificate application. 			

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	28-5.a Examine documented procedures to verify that unless the certificate request is generated within the same secure room meeting the requirements of the Level 3 environment, they include validating the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.	Documented procedures examined:	<Report Findings Here>
CA/RA	28-5.b Observe certificate-issuing processes to verify that the identities of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key.	Describe how the certificate-issuing processes observed verified that the identities of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key:	
		<Report Findings Here>	
<p>28-5.1 For CA and KDH certificate-signing requests, including certificate or key-validity status changes—e.g., revocation, suspension, replacement—verification must include validation that:</p> <ul style="list-style-type: none"> • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner. 			
CA/RA	<p>28-5.1.a Examine documented procedures to verify that certificate-signing requests, including certificate or key-validity status changes, require validation that:</p> <ul style="list-style-type: none"> • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner. 	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	<p>28-5.1.b Observe certificate-signing requests, including certificate or key-validity status changes, to verify they include validation that:</p> <ul style="list-style-type: none"> • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner. 	Certificate-signing requests reviewed:	<Report Findings Here>
<p>28-5.2 RAs must retain documentation and audit trails relating to the identification of entities for all certificates issued and certificates whose status had changed for the life of the associated certificates.</p>			
CA/RA	<p>28-5.2 Examine documentation and audit trails to verify that the identification of entities is retained for the life of the associated certificates:</p> <ul style="list-style-type: none"> • For all certificates issued • For all certificates whose status had changed 	Documentation examined:	<Report Findings Here>
		Describe how the observation of audit trails verified that the identification of entities is retained for the life of the associated certificates:	
		<ul style="list-style-type: none"> • For all certificates issued • For all certificates whose status had changed 	
<p>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.</p>			
CA/RA KIF KLCP SP	<p>29-1.a Examine documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys:</p> <ul style="list-style-type: none"> • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering. 	Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	<p>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:</p> <ul style="list-style-type: none"> 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. 	<p>Personnel interviewed:</p> <p>Identify the P2PE Assessor who confirms that processes are followed to provide the following assurances prior to the loading of cryptographic keys:</p> <ul style="list-style-type: none"> 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>
<p>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:</p>			
CA/RA KIF KLCP SP	<p>29-1.1.a Examine documented procedures to verify controls are defined to protect POI devices, and other SCDs from unauthorized access up to point of deployment.</p>	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>29-1.1.b Verify that documented procedures include 29-1.1.1 through 29-1.1.3 below.</p>	Documented procedures reviewed:	<Report Findings Here>
<p>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.</p> <p>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.</p>			

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	29-1.1.1.a Examine access-control documentation and device configurations to verify that access to all POI devices and key injection/loading devices is defined and documented.	Access-control documentation reviewed:	<Report Findings Here>
		Describe how access-control documentation and device configurations observed verified that access to all POI devices and key injection/loading devices is defined and documented:	<Report Findings Here>
		<Report Findings Here>	
CA/RA KIF KLCP SP	29-1.1.1.b For a sample of POI device types and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POI devices and other SCDs is logged.	Sample of POI device types and other SCDs:	<Report Findings Here>
		Access logs reviewed:	<Report Findings Here>
		Describe how observation of authorized personnel accessing devices and access logs verified that access to all POI devices and other SCDs is logged:	
		<Report Findings Here>	
CA/RA KIF KLCP SP	29-1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD.	Describe how the implemented access controls examined verified that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD:	
		<Report Findings Here>	
29-1.1.2 Intentionally left blank.			
29-1.1.3 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.			
CA/RA KIF KLCP SP	29-1.1.3.a Examine documented authorizations for personnel with access to devices to verify that prior to deployment: <ul style="list-style-type: none"> • All personnel with access to POI devices and other SCDs are documented in a formal list authorized by management in an auditable manner. • All personnel with access to POI devices and other SCDs are authorized by management. • The authorizations are reviewed annually. 	Documented authorizations reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	29-1.1.3.b For a sample of POI device types and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in an auditable manner have access to devices.	Sample of POI device types and other SCDs reviewed:	<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>	
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.			
CA/RA KIF KLCP SP	29-1.2.a Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	29-1.2.b Observe implemented processes and interview personnel to verify that default keys or passwords are not used.	Responsible personnel interviewed:	<Report Findings Here>
29-2 Implement a documented “chain of custody” to ensure that all devices are controlled from receipt to placement into service. The chain of custody must include records to identify responsible personnel for each interaction with the devices. Note: Chain of custody includes procedures, as stated in Requirement 29-1 , that ensure that 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.			
CA/RA KIF KLCP	29-2.a Examine documented processes to verify that the chain of custody is required for devices from receipt to placement into service.	Documented processes examined:	<Report Findings Here>
CA/RA KIF KLCP	29-2.b For a sample of devices, examine documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to placement into service.	Sample of POIs and other SCDs reviewed:	<Report Findings Here>
		Documented records reviewed:	<Report Findings Here>
CA/RA KIF KLCP	29-2.c Verify that the chain-of-custody records identify responsible personnel for each interaction with the device.	Responsible personnel interviewed:	<Report Findings Here>
		Documented records reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>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:</p> <ul style="list-style-type: none"> • Transportation uses a trusted courier service (e.g., via bonded carrier). The devices are then securely stored until key-insertion occurs. • Physically secure and trackable packaging (e.g., pre-serialized, counterfeit-resistant, tamper-evident packaging) is used. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs. • A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. The SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key, and the device is further protected until deployment. • Shipped and stored containing a secret that: <ul style="list-style-type: none"> – Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and – 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 modifications. <p>Note: Unauthorized access includes that by customs officials.</p>			
CA/RA KIF KLCP SP	29-3.a Examine documented procedures to verify they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	29-3.b Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion and deployment.	Responsible personnel interviewed:	<Report Findings Here>
<p>29-4 Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or backup devices—throughout their lifecycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs, but cannot supplant the implementation of dual-control mechanisms.</p>			
CA/RA KIF KLCP SP	29-4.a Examine documented procedures to verify that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	29-4.b Interview responsible personnel and physically verify the dual-control mechanism used to prevent substitution or tampering of HSMs—both in service and spare or back-up devices—throughout their life cycle.	Responsible personnel interviewed: 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>
<p>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.</p> <p>Note: Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.</p>			
CA/RA KIF KLCP SP	29-4.1.a Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KLCP SP	29-4.1.b For a sample of received devices, examine sender documentation sent by a different communication channel than the device's shipment (e.g., the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.	Sample of received devices:	<Report Findings Here>
		Sender documentation/record of serial number validations reviewed:	<Report Findings Here>
<p>29-4.2 The security policy enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required to support specified functionality must be disabled before the equipment is commissioned.</p> <p>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.</p>			
CA/RA KIF KLCP SP	29-4.2.a Obtain and examine the defined security policy to be enforced by the HSM.	Documented security policy examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KLCP SP	29-4.2.b Examine documentation of the HSM configuration settings from past commissioning events to determine that the functions and commands enabled are in accordance with the security policy.	HSM configuration settings documentation examined:	<Report Findings Here>
CA/RA KIF KLCP SP	29-4.2.c For a sample of HSMs, examine the configuration settings to determine that only authorized functions are enabled.	Sample of HSMs reviewed:	<Report Findings Here>
		Describe how the HSM configuration settings observed verified that only authorized functions are enabled:	
		<Report Findings Here>	
29-4.2.d Not used in P2PE			
29-4.2.e Not used in P2PE			
CA/RA KIF KLCP SP	29-4.2.f Examine documentation to verify: <ul style="list-style-type: none"> • Configuration settings are defined, signed and dated by personnel responsible for implementation. • It includes identifying information for the HSM, such as serial number and/or asset identifiers. • The documentation is retained and updated anytime configuration setting impacting security occur for each affected HSM. 	Documentation examined:	<Report Findings Here>
29-4.3 When HSMs are connected to online systems, controls are in place to prevent the use of an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Note: Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.			
CA/RA KIF KLCP SP	29-4.3 Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.	Describe how the HSM configurations examined and processes observed verified that HSMs are not enabled in a sensitive state when connected to online systems:	
		<Report Findings Here>	
29-4.4 Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised. Processes must include :			
CA/RA KIF KLCP SP	29-4.4. Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify the integrity of the device and include requirements specified at 29-4.4.1 through 29-4.4.4 below.	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
29-4.4.1 Running self-tests to ensure the correct operation of the device.			
CA/RA KIF KLCP SP	29-4.4.1 Examine records of device inspections and test results to verify that self-tests are run on devices to ensure the correct operation of the device.	Records of device inspections examined:	<Report Findings Here>
		Describe how the records of device inspections and test results examined verified that self-tests are run on devices to ensure the correct operation of the device:	
		<Report Findings Here>	
29-4.4.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.			
CA/RA KIF KLCP SP	29-4.4.2 Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised.	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the inspection processes observed verified that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised:	
		<Report Findings Here>	
29-4.4.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed			
CA/RA KIF KLCP SP	29-4.4.3 Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the inspection processes observed verified that processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed:	
		<Report Findings Here>	
29-4.4.4 Maintaining records of the tests and inspections, and retaining records for at least one year.			
CA/RA KIF KLCP SP	29-4.4.4.a Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.	Records of inspections examined:	<Report Findings Here>
		Responsible personnel interviewed:	<Report Findings Here>
CA/RA KIF KLCP SP	29-4.4.4.b Examine records of inspections to verify records are retained for at least one year.	Records of inspections examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
29-5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.			
CA/RA KIF KLCP SP	29-5.a Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KLCP SP	29-5.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.	Sample of received devices reviewed:	<Report Findings Here>
<p>30-3 Processes must exist to ensure that key-injection operations are performed and reconciled on an inventory of pre-authorized devices. Processes must include the following:</p> <ul style="list-style-type: none"> • Each production run must be associated with a predefined inventory of identified POI devices to be injected or initialized with keys. • Unauthorized personnel must not be able to modify this inventory without detection. • All POI devices to be initialized with keys on a production run must be identified and accounted for against the inventory. • Unauthorized POI devices submitted for injection or initialized must be rejected by the injection platform and investigated. • Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices must be identified and accounted for against the inventory. <p>Note: The KIF platform must ensure that only authorized devices can ever be injected or initialized with authorized keys. Processes must prevent (1) substitution of an authorized device with an unauthorized device, and (2) insertion of an unauthorized device into a production run.</p>			
KIF KLCP	<p>30-3.a Obtain and examine documentation of inventory control and monitoring procedures. Determine that the procedures cover:</p> <ul style="list-style-type: none"> • Each production run is associated with a predefined inventory of identified POI devices to be injected or initialized with keys. • Unauthorized personnel are not able to modify this inventory without detection. • All POI devices to be initialized with keys on a production run are identified and accounted for against the inventory. • Unauthorized POI devices submitted for injection or initialized are rejected by the injection platform and investigated. • Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices are identified and accounted for against the inventory. 	Documented procedures reviewed:	<Report Findings Here>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	30-3.b Interview applicable personnel to determine that procedures are known and followed.	Applicable personnel interviewed:	<Report Findings Here>
<p>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.</p> <p>Processes must include the following:</p> <p>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.</p>			
CA/RA KIF KMCP KLCP SP	<p>31-1 Verify that documented procedures for removing SCDs from service include the following:</p> <ul style="list-style-type: none"> Procedures require that all secret and private keys, key material, and all account data stored within the device be securely destroyed. Procedures cover all devices removed from service permanently or for repair. Procedures cover requirements at 31-1.1 through 31-1.6 below. 	Documented procedures examined:	<Report Findings Here>
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes.			
CA/RA KIF KMCP KLCP SP	31-1.1.a Examine documented procedures for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	31-1.1.b Interview personnel and observe demonstration (if HSM is available) of processes for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.	Personnel interviewed:	<Report Findings Here>
		Describe how the demonstration observed verified that dual control is implemented for all critical decommissioning processes.	
		<Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
31-1.2 Keys and account data are rendered irrecoverable (e.g., zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.			
CA/RA KIF KMCP KLCP SP	31-1.2 Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material and account data are rendered irrecoverable (e.g., zeroized), or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.	Personnel interviewed:	<Report Findings Here>
		Describe how the demonstration verified that all keying material and account data are rendered irrecoverable, or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys:	
		<Report Findings Here>	
31-1.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.			
CA/RA KIF KMCP KLCP SP	31-1.3 Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable.	Personnel interviewed:	<Report Findings Here>
		Describe how the processes observed verified that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable or the devices are physically destroyed:	
		<Report Findings Here>	
31-1.4 Affected entities are notified before devices are returned.			
CA/RA KIF KMCP KLCP SP	31-1.4 Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.	Responsible personnel interviewed:	<Report Findings Here>
		Device-return records examined:	<Report Findings Here>
31-1.5 Devices are tracked during the return process.			
CA/RA KIF KMCP KLCP SP	31-1.5 Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.	Responsible personnel interviewed:	<Report Findings Here>
		Device-return records examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
31-1.6 Records of the tests and inspections are maintained for at least one year.			
CA/RA KIF KMCP KLCP SP	31-1.6 Interview personnel and observe records to verify that records of the tests and inspections are maintained for at least one year.	Personnel interviewed:	<Report Findings Here>
		Records of testing examined:	<Report Findings Here>
32-1 For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into POI devices, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:			
CA/RA KIF KMCP KLC SP	32-1.a Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into POI devices.	Documented procedures reviewed:	<Report Findings Here>
CA/RA KIF KMCP KLCP SP	32-1.b Verify that documented procedures cover requirements 32-1.1 through 32-1.5 below.	Documented procedures reviewed:	<Report Findings Here>
32-1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. Note: <i>Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords/authentication codes, or for physical access via a physical lock that requires two individuals each with a different high-security key.</i> <i>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.</i> <i>Physical keys, authorization codes, passwords/authentication codes, or other enablers must be managed so that no one person can use both the enabler(s) and the device, which can create cryptograms of known keys or key components under a key-encipherment key used in production.</i>			
CA/RA KIF KMCP KLCP SP	32-1.1 Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.	Describe how the dual-control mechanisms and device-authorization processes observed verified that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people:	
		<Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-1.2 Passwords/authentication codes used for dual control must each be of at least five numeric and/or alphabetic characters.			
SP CA/RA KIF KMCP KLCP	32-1.2 Observe password policies and configuration settings to confirm that passwords/authentication codes used for dual control must be at least five numeric and/or alphabetic characters.	Password policies reviewed:	<Report Findings Here>
		Describe how the configuration settings observed verified that passwords used for dual control must be at least five numeric and/or alphabetic characters:	
		<Report Findings Here>	
32-1.3 Dual control must be implemented for the following: <ul style="list-style-type: none"> • To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of clear-text key components; • For all access to key-loading devices (KLDs) and authenticated application-signing devices. 			
CA/RA KIF KMCP KLCP SP	32-1.3 Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: <ul style="list-style-type: none"> • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing • To enable application-signing functions • To place the device into a state that allows for the input or output of clear-text key components • For all access to KLDs and authenticated application-signing devices 	Dual-control mechanisms examined:	<Report Findings Here>
		Describe how the observation of authorized personnel performing the defined activities verified that dual control is implemented for the following: <ul style="list-style-type: none"> • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing • To enable application-signing functions • To place the device into a state that allows for the input or output of clear-text key components • For all access to KLDs and authenticated application-signing devices 	
		<Report Findings Here>	
32-1.4 Devices must not use default passwords.			
CA/RA KIF KMCP KLCP SP	32-1.4.a Examine password policies and documented procedures to confirm default passwords/authentication codes must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists.	Documented procedures and password policies reviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP SP	32-1.4.b Observe device configurations and interview device administrators to verify that HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords /authentication codes.	Device administrators interviewed:	<Report Findings Here>
		Describe how the device configurations observed verified that HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords:	
		<Report Findings Here>	
32-1.5 To detect any unauthorized use, devices are at all times within a secure room and either: <ul style="list-style-type: none"> • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected. Note: For key-injection facilities, or applicable entities providing key-management services, POI devices may be secured by storage in the dual-control access key injection room.			
CA/RA KIF KMCP KLCP SP	32-1.5.a Examine documented procedures to confirm that they require devices are at all times within a secure room and either: <ul style="list-style-type: none"> • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times. 	Documented procedures reviewed:	<Report Findings Here>
		Describe how devices are at all times within a secure room and either: <ul style="list-style-type: none"> • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times. <Report Findings Here>	
CA/RA KIF KMCP KLCP SP	32-1.5.b Interview responsible personnel and observe devices and processes to confirm that devices are at all times within a secure room and either: <ul style="list-style-type: none"> • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times. 		Responsible personnel interviewed:
		Describe how devices are at all times within a secure room and either: <ul style="list-style-type: none"> • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times. <Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>32-2.1 The certificate-processing operations center must implement a three-tier physical security boundary, as follows:</p> <ul style="list-style-type: none"> • Level One Barrier – Consists of the entrance to the facility • Level Two Barrier – Secures the entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Provides access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices 			
CA/RA	<p>32-2.1.a Examine physical security policies to verify three tiers of physical security are defined as follows:</p> <ul style="list-style-type: none"> • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices 	Documented physical security policies examined:	<Report Findings Here>
CA/RA	<p>32-2.1.b Observe the physical facility to verify three tiers of physical security are implemented as follows:</p> <ul style="list-style-type: none"> • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices 	Describe how the physical facility observed verified that three tiers of physical security are implemented as follows:	<ul style="list-style-type: none"> • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices <p><Report Findings Here></p>
Level 1 Barrier			
<p>32-2.2 The entrance to the CA facility/building must include the following controls:</p>			
<p>32-2.2.1 The facility entrance only allows authorized personnel to enter the facility.</p>			
CA/RA	<p>32-2.2.1.a Examine physical-security procedures and policies to verify they require that the facility entrance allows only authorized personnel to enter the facility.</p>	Documented physical-security procedures and policies examined:	<Report Findings Here>
CA/RA	<p>32-2.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed to enter the facility.</p>	Identify the P2PE Assessor who confirms that only authorized personnel are allowed to enter the facility:	<Report Findings Here>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
32-2.2.2 The facility has a guarded entrance or a foyer with a receptionist. No entry is allowed for visitors if the entryway is not staffed—i.e., only authorized personnel who badge or otherwise authenticate themselves can enter when entryway is unstaffed.			
CA/RA	32-2.2.2.a Examine physical-security procedures and policies to verify they require that the facility have a guarded entrance or a foyer with a receptionist or the entryway prevents access to visitors.	Documented physical-security procedures and policies reviewed:	<Report Findings Here>
CA/RA	32-2.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.	Identify the P2PE Assessor who confirms that the facility entrance has a guarded entrance or a foyer with a receptionist:	<Report Findings Here>
32-2.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.			
CA/RA	32-2.2.3.a Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.	Documented physical-security procedures and policies reviewed:	<Report Findings Here>
CA/RA	32-2.2.3.b Observe the facility entrance and observe personnel entering the facility to verify that visitors are authorized and registered in a logbook.	Identify the P2PE Assessor who confirms that visitors are authorized and registered in a logbook at the facility entrance:	<Report Findings Here>
Level 2 Barrier			
32-2.3 The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.			
CA/RA	32-2.3.a Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the Level 2 barrier/entrance.	Documented physical-security procedures and policies examined:	<Report Findings Here>
CA/RA	32-2.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.	Identify the P2PE Assessor who confirms that only authorized personnel are allowed to enter through the Level 2 barrier/entrance:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-2.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.			
CA/RA	32-2.3.1.a Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.	Documented physical-security procedures and policies examined:	<Report Findings Here>
CA/RA	32-2.3.1.b Interview personnel and observe visitors entering the environment to verify that visitors are authorized and escorted at all times within the Level 2 environment.	Personnel interviewed:	<Report Findings Here>
		Identify the P2PE Assessor who confirms that visitors entering the Level 2 environment are authorized and escorted at all times:	<Report Findings Here>
32-2.3.2 Access logs must record all personnel entering the Level 2 environment. <i>Note: The logs may be electronic, manual, or both.</i>			
CA/RA	32-2.3.2.a Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.	Documented physical-security procedures and policies examined:	<Report Findings Here>
CA/RA	32-2.3.2.b Observe personnel entering the Level 2 barrier and examine corresponding access logs to verify that all entry through the Level 2 barrier is logged.	Describe how the observation of personnel entering the Level 2 barrier and the corresponding access logs verified that all entry through the Level 2 barrier is logged:	<Report Findings Here>
		<Report Findings Here>	
32-2.4 The Level 2 entrance must be monitored by a video-recording system.			
CA/RA	32-2.4.a Observe the Level 2 entrance to verify that a video-recording system is in place.	Identify the P2PE Assessor who confirms the Level 2 entrance is monitored by a video-recording system:	<Report Findings Here>
CA/RA	32-2.4.b Examine a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.	Sample of recorded footage reviewed:	<Report Findings Here>

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
Level 3 Barrier			
32-2.5 The Level 3 environment must consist of a physically secure, dedicated room not used for any other business activities but certificate operations. Note: All certificate-processing operations must operate in the Level 3 environment.			
CA/RA	32-2.5.a Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.	Documented policies and procedures examined:	<i><Report Findings Here></i>
CA/RA	32-2.5.b Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.	Identify the P2PE Assessor who confirms that all certificate-processing systems are located within a Level 3 secure room:	<i><Report Findings Here></i>
CA/RA	32-2.5.c Observe operations and interview personnel to confirm that the Level 3 secure room is not used for any business activity other than certificate operations.	Personnel interviewed:	<i><Report Findings Here></i>
		Describe how the observation of operations verified that the Level 3 secure room is not used for any business activity other than certificate operations:	
		<i><Report Findings Here></i>	
32-2.5.1 Doors to the Level 3 secure room must have locking mechanisms.			
CA/RA	32-2.5.1 Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.	Identify the P2PE Assessor who confirms that all doors to the Level 3 environment have locking mechanisms:	<i><Report Findings Here></i>
32-2.5.2 The Level 3 environment must be enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars. For example, the Level 3 environment may be implemented within a “caged” environment.			
CA/RA	32-2.5.2.a Examine physical security documentation for the Level 3 environment to verify that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as have true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars	Physical security documentation reviewed:	<i><Report Findings Here></i>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	32-2.5.2.b Examine the physical boundaries of the Level 3 environment to verify that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars and protection from entry from below floors and above ceilings.	Describe how examination of the physical boundaries of the Level 3 environment verified that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars and protection from entry from below floors and above ceilings: <i><Report Findings Here></i>	
32-2.6 Documented procedures must exist for: <ul style="list-style-type: none"> Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA Specific access authorizations, whether logical or physical 			
CA/RA	32-2.6.a Examine documented procedures to verify they include the following: <ul style="list-style-type: none"> Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA Specific access authorizations, whether logical or physical 	Documented procedures examined:	<i><Report Findings Here></i>
CA/RA	32-2.6.b Interview responsible personnel to verify that the documented procedures are followed for: <ul style="list-style-type: none"> Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA Specific access authorizations, whether logical or physical 	Responsible personnel interviewed:	<i><Report Findings Here></i>
32-2.6.1 All authorized personnel with access through the Level 3 barrier must: <ul style="list-style-type: none"> Have successfully completed a background security check Be assigned resources (staff, dedicated personnel) of the CA operator with defined business needs and duties Note: <i>This requirement applies to all personnel with pre-designated access to the Level 3 environment.</i>			
CA/RA	32-2.6.1.a Examine documented policies and procedures to verify they require personnel authorized as having access through the Level 3 barrier to: <ul style="list-style-type: none"> Have successfully completed a background security check. Be assigned resources of the CA operator with defined business needs and duties. 	Documented policies and procedures examined:	<i><Report Findings Here></i>
CA/RA	32-2.6.1.b Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws) on CA personnel prior such personnel being authorized for access through the Level 3 barrier.	Responsible HR personnel interviewed:	<i><Report Findings Here></i>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA	32-2.6.1.c Interview a sample of personnel authorized for access through the Level 3 barrier to verify that they are assigned resources of the CA with defined business needs and duties.	Sample of personnel authorized for access through the Level 3 barrier interviewed:	<Report Findings Here>
32-2.6.2 Other personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.			
CA/RA	32-2.6.2.a Examine documented policies and procedures to verify that personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.6.2.b Interview a sample of responsible personnel to verify that personnel requiring entry to this level are accompanied by two (2) authorized and assigned resources at all times.	Sample of responsible personnel interviewed:	<Report Findings Here>
32-2.7 The Level 3 environment must require dual-control access and dual-occupancy such that the room is never occupied by one person for more than thirty (30) seconds—i.e., one person may never be in the room for more than 30 seconds alone. For example: <i>The Level 3 room is never occupied by one person except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.</i>			
CA/RA	32-2.7.a Examine documented policies and procedures to verify that the Level 3 environment requires dual-control access and dual-occupancy such that the room is never occupied by one person alone for more than thirty (30) seconds.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.7.b Observe authorized personnel accessing the Level 3 environment to verify that dual-control access and dual-occupancy is enforced such that the room is never occupied by one person alone for more than thirty (30) seconds.	Describe how the observation of authorized personnel accessing the Level 3 environment verified that dual-control access and dual-occupancy is enforced such that the room is never occupied by one person alone for more than thirty (30) seconds: <Report Findings Here>	
32-2.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated.			
CA/RA	32-2.7.1.a Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.7.1.b Observe enforcement mechanism configuration to verify it is automated.	Identify the P2PE Assessor who confirms the enforcement mechanism configuration is automated:	<Report Findings Here>

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-2.7.2 The system must enforce anti-pass-back.			
CA/RA	32-2.7.2.a Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.7.2.b Observe mechanisms in use and authorized personnel within the environment to verify that anti-pass-back is enforced by the conduct of a test.	Identify the P2PE Assessor who confirms the enforcement mechanism configuration is automated:	<Report Findings Here>
32-2.7.3 Dual occupancy requirements are managed using electronic (e.g., badge and/or biometric) systems.			
CA/RA	32-2.7.3.a Examine documented policies and procedures to verify that dual occupancy requirements are defined to be managed using electronic (e.g., badge and/or biometric) systems.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic systems.	Identify the P2PE Assessor who confirms the dual-occupancy requirements are managed using electronic systems:	<Report Findings Here>
32-2.7.4 Any time a single occupancy exceeds 30 seconds, the system must automatically generate an alarm and audit event that is followed up by security personnel.			
CA/RA	32-2.7.4.a Examine documented policies and procedures to verify that any time one person is alone in the room for more than 30 seconds, the system must automatically generate an alarm and an audit event that is followed up by security personnel.	Documented policies and procedures examined:	<Report Findings Here>
CA/RA	32-2.7.4.b Observe mechanisms in use to verify that the system automatically generates an alarm event and an audit event when one person is alone in the room for more than 30 seconds.	Describe how the observed mechanisms in use verified that the system automatically generates an alarm event and an audit event when one person is alone in the room for more than 30 seconds:	<Report Findings Here>
CA/RA	32-2.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.	Sample of audit events reviewed:	<Report Findings Here>
		Security personnel interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-2.8 Access to the Level 3 room must create an audit event, which must be logged.			
CA/RA	32-2.8 Observe authorized personnel enter the environment and examine correlating audit logs to verify that access to the Level 3 room creates an audit log event.	Correlating audit logs reviewed:	<Report Findings Here>
		Describe how the observation of authorized personnel entering the environment and correlating audit logs verified that access to the Level 3 room creates an audit log event:	
		<Report Findings Here>	
32-2.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel.			
CA/RA	32-2.8.1 Observe an invalid access attempt and examine correlating audit logs to verify that invalid access attempts to the Level 3 room create an audit log event.	Correlating audit logs reviewed:	<Report Findings Here>
		Describe how the observation of an invalid access attempt and correlating audit logs verified that invalid access attempts to the Level 3 room create an audit log event:	
		<Report Findings Here>	
32-2.9 The Level 3 environment must be monitored as follows:			
32-2.9.1 A minimum of one or more cameras must provide continuous monitoring (e.g., CCTV system) of the Level 3 environment, including the entry and exit.			
Note: Motion-activated systems that are separate from the intrusion-detection system may be used to activate recording activity.			
CA/RA	32-2.9.1.a Observe the Level 3 physical environment to verify that cameras are in place to monitor the Level 3 environment, including the entry and exit.	Identify the P2PE Assessor who confirms that cameras are in place to monitor the Level 3 environment, including the entry and exit:	<Report Findings Here>
		Describe how the monitoring system configurations observed verified that continuous monitoring is provided: <Report Findings Here>	
CA/RA	32-2.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.	Describe how the monitoring system configurations observed verified that continuous monitoring is provided: <Report Findings Here>	
CA/RA	32-2.9.1.c If motion-activated systems are used for monitoring, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.	Describe how the configurations observed for motion-activated systems verified that they are separate from the intrusion-detection system:	
		<Report Findings Here>	

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-2.9.2 The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.			
CA/RA	32-2.9.2 Examine monitoring system configurations to verify; <ul style="list-style-type: none"> • The system records to time-lapse VCRs or similar mechanisms. • A minimum of five frames are recorded every three seconds. 	Describe how the monitoring system configurations observed verified that: <ul style="list-style-type: none"> • The system records to time-lapse VCRs or similar mechanisms. • A minimum of five frames are recorded every three seconds. 	
<i><Report Findings Here></i>			
32-2.9.3 Continuous or motion-activated, appropriate lighting must be provided for the cameras. Note: <i>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).</i>			
CA/RA	32-2.9.3.a Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for each camera monitoring the environment.	Identify the P2PE Assessor who confirms that continuous or motionactivated lighting is provided for each camera monitoring the Level 3 physical environment:	<i><Report Findings Here></i>
CA/RA	32-2.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.	Sample of captured footage reviewed:	<i><Report Findings Here></i>
32-2.9.4 Surveillance cameras must be configured to prevent the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data. Cameras must not be able to be remotely adjusted to zoom in or otherwise observe the aforementioned.			
CA/RA	32-2.9.4.a Observe each camera locations in the Level 3 environment to verify they are not set to monitor computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.	Identify the P2PE Assessor who confirms that observed camera locations in the Level 3 environment are not set to monitor computer screens, keyboards, PIN pads, or other systems that may expose sensitive data:	<i><Report Findings Here></i>
CA/RA	32-2.9.4.b Examine a sample of captured footage to verify it does not allow for the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.	Sample of captured footage reviewed:	<i><Report Findings Here></i>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-2.9.5 Personnel with access to the Level 3 environment must not have access to the media (e.g., VCR tapes, digital-recording systems, etc.) containing the recorded surveillance data.			
CA/RA	32-2.9.5.a Examine documented access policies and procedures to verify that personnel with access to the Level 3 environment are not permitted to have access to the media containing recorded surveillance data for that environment.	Documented access policies and procedures examined:	<i><Report Findings Here></i>
CA/RA	32-2.9.5.b Examine Level 3 access lists as well as access controls to the media containing surveillance data, to verify that personnel with access to the Level 3 environment do not have access to the media containing recorded surveillance data.	Describe how the Level 3 access lists and access controls to the media containing surveillance data examined verified that personnel with access to the Level 3 environment do not have access to the media containing recorded surveillance data: <i><Report Findings Here></i>	
32-2.9.6 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 (primary and backup) to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.			
CA/RA	32-2.9.6.a 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 that at least the most recent 45 days of images are securely archived:	<i><Report Findings Here></i>
CA/RA	32-2.9.6.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 the system configurations observed verified that where digitalrecording mechanisms are in use, the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period: <i><Report Findings Here></i>	
32-2.9.7 CCTV images must be backed up daily. The backup recording must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users (personnel accessing the secure room) and administrators of the system. Alternatively, backups may be stored in other facilities via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements.			
CA/RA	32-2.9.7 Examine backup techniques utilized to ensure that: <ul style="list-style-type: none"> • Backups are securely stored in a separate location from the primary. • Ensure that segregation is maintained between users and administrators of the system. 	Describe how the observed backup techniques verified that: <ul style="list-style-type: none"> • Backups are securely stored in a separate location from the primary. • Ensure that segregation is maintained between users and administrators of the system. <i><Report Findings Here></i>	

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-3 The environment must have continuous (24/7) intrusion-detection systems in place, which protect the secure room by motion detectors when unoccupied.			
CA/RA	32-3.a Examine security policies and procedures to verify they require: <ul style="list-style-type: none"> • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment • Motion detectors must be active when the environment is unoccupied. 	Documented security policies and procedures examined:	<Report Findings Here>
CA/RA	32-3.b Examine intrusion-detection system configurations to verify: <ul style="list-style-type: none"> • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place • Motion detectors are active when the environment is unoccupied. 	Describe how the observed intrusion-detection system configurations verified that: <ul style="list-style-type: none"> • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place. • Motion detectors are active when the environment is unoccupied 	<Report Findings Here>
32-3.1 Any windows in the secure room must be locked and protected by alarmed sensors.			
CA/RA	32-3.1.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 secure areas are locked and protected by alarmed sensors:	<Report Findings Here>
CA/RA	32-3.1.b Examine configuration of window sensors to verify that the alarm mechanism is active.	Identify the P2PE Assessor who confirms the configuration of window sensors verified that the alarm mechanism is active:	<Report Findings Here>
CA/RA	32-3.1.c Test at least one window (if they can be opened) to verify that the alarms function appropriately.	Describe how the testing of at least one window verified that the alarms function appropriately:	<Report Findings Here>
32-3.2 Any windows or glass walls must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.			
CA/RA	32-3.2 Observe all windows and glass walls in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	Describe how observation of the windows and glass walls in the secure areas verified that they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-3.3 The intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have performed an authenticated exit of the secure room. The system must be configured to activate within 30 seconds.			
CA/RA	32-3.3.a Examine security system configurations to verify: <ul style="list-style-type: none"> The intrusion-detection system(s) is connected to the alarm system. The intrusion-detection system(s) is automatically activated every time all authorized personnel have exited the secure room. 	Describe how the observed security system configurations verified that: <ul style="list-style-type: none"> The intrusion-detection system(s) is connected to the alarm system. The intrusion-detection system(s) is automatically activated every time all authorized personnel have exited the secure area. <Report Findings Here>	
CA/RA	32-3.3.b Verify the IDS and alarms function correctly via: <ul style="list-style-type: none"> Having all authorized personnel who badged or otherwise authenticated into the area exit and one person remain behind even though they have badged out Having all but one authorized person who badged or otherwise authenticated into the system badge out and exit. 	Describe how observing all authorized personnel who badged or otherwise authenticated into the area exit and one person remain behind even though they have badged out verified that IDS and alarms function correctly: <Report Findings Here> Describe how observing all but one authorized person who badged or otherwise authenticated into the system badge out and exit verified that IDS and alarms function correctly: <Report Findings Here>	
32-3.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.			
CA/RA	32-4.a Examine security policies and procedures to verify they require all non-CA personnel to sign an access logbook when entering the Level 3 environment.	Documented security policies and procedures reviewed:	<Report Findings Here>
CA/RA	32-4.b On the escorted entry into the secure room, observe that all non-CA personnel appropriately sign the access logbook.	Identify the P2PE Assessor who confirms that upon escorted entry into the secure area, all personnel appropriately sign the access logbook and all escorted visitors are required to sign the access logbook:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>32-4.1 The access log must include the following details:</p> <ul style="list-style-type: none"> Name and signature of the individual Organization Date and time in and out Reason for access or purpose of visit For visitor access, the initials of the person escorting the visitor 			
CA/RA	<p>32-4.1 Examine the access logbook to verify it contains the following information:</p> <ul style="list-style-type: none"> Name and signature of the individual Organization Date and time in and out Reason for access or purpose of visit For visitor access, the initials of the person escorting the visitor 	<p>Identify the P2PE Assessor who confirms the access logbook contains the following:</p> <ul style="list-style-type: none"> Name and signature of the individual Organization Date and time in and out Reason for access or purpose of visit For visitor access, the initials of the person escorting the visitor 	<Report Findings Here>
<p>32-4.2 The logbook must be maintained within the Level 3 secure environment.</p>			
CA/RA	<p>32-4.2 Observe the location of the access logbook and verify that it is maintained within the Level 3 secure environment.</p>	<p>Identify the P2PE Assessor who confirms the location of the access logbook is maintained within the Level 3 secure environment:</p>	<Report Findings Here>
<p>32-5 All access-control and monitoring systems (including intrusion-detection systems) are powered through an uninterruptible power source (UPS).</p>			
CA/RA	<p>32-5 Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems, including intrusion-detection systems, are powered through the UPS.</p>	<p>Describe how the observed UPS system configurations verified that all access-control and monitoring systems, including intrusion-detection systems, are powered through the UPS:</p> <p><Report Findings Here></p>	
<p>32-6 All alarm events must be documented.</p>			
CA/RA	<p>32-6.a Examine security policies and procedures to verify they require that all alarm events be logged.</p>	<p>Documented security policies and procedures examined:</p>	<Report Findings Here>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
CA/RA	32-6.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.	Documented alarm events reviewed:	<Report Findings Here>
32-6.1 An individual must not sign off on an alarm event in which they were involved.			
CA/RA	32-6.1.a Examine documented procedures for responding to alarm events to verify that the procedure does not permit a person who was involved in an alarm event to sign-off on that alarm event.	Documented procedures examined:	<Report Findings Here>
CA/RA	32-6.1.b Determine who is authorized to sign off on alarm events.	Identify the P2PE Assessor who determined who is authorized to sign off on alarm events:	<Report Findings Here>
CA/RA	32-6.1.c For a sample of documented alarm events, examine the record to verify that personnel authorized to sign off on alarm events were not also the cause of that event.	Sample of documented alarm events reviewed:	<Report Findings Here>
		Alarm event records reviewed:	<Report Findings Here>
32-6.2 The use of any emergency entry or exit mechanism must cause an alarm event.			
CA/RA	32-6.2.a Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.	Describe how the observed security system configurations verified that an alarm event is generated upon use of any emergency entry or exit mechanism:	
		<Report Findings Here>	
CA/RA	32-6.2.b Conduct a test to verify the mechanisms work appropriately.	Describe the testing performed that verified the mechanisms work appropriately:	
		<Report Findings Here>	
32-6.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.			
CA/RA	32-6.3.a Examine documented procedures to verify they require that all alarms for physical intrusion must be responded to within 30 minutes by personnel assigned security duties.	Documented procedures examined:	<Report Findings Here>
CA/RA	32-6.3.b Examine a sample of alarm events and interview personnel assigned with security-response duties to verify that alarms for physical intrusion are responded to within 30 minutes.	Sample of alarm events reviewed:	<Report Findings Here>
		Personnel assigned with security-response duties interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA	32-6.3.c Conduct a test to verify the appropriate response occurs.	Describe the testing performed that verified the appropriate response occurs: <Report Findings Here>	
<p>32-7 A process must be implemented for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs. It must be ensured that synchronization errors between CCTV, intrusion detection, and access control cannot exceed one minute.</p> <p>Note: This may be done by either automated or manual mechanisms.</p>			
CA/RA	32-7.a Examine documented procedures to verify that mechanisms are defined (may be automated or manual) for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs.	Documented procedures examined:	<Report Findings Here>
CA/RA	32-7.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.	Describe how the observed system configurations for access, intrusion-detection, and monitoring (camera) systems verified that time and date stamps are synchronized: <Report Findings Here>	
CA/RA	32-7.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 reviewed:	<Report Findings Here>
<p>32-7.1 If a manual synchronization process is used, synchronization must occur at least quarterly; events must be recorded, and variances documented; and documentation of the synchronization must be retained for at least a one-year period.</p>			
CA/RA	32-7.1.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>
CA/RA	32-7.1.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>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
32-8 Distributed functionality of the KIF that is used for generation and transfer of keys must communicate via mutually authenticated channels. All key transfers between distributed KIF functions must meet the requirements of Control Objective 3 .			
32-8.1 The KIF must ensure that keys are transmitted between KIF components in accordance with Control Objective 3 .			
KIF KMCP KLCP	32-8.1.a Examine documented procedures for key conveyance or transmittal to verify that keys used between KIF components are addressed in accordance with applicable criteria in Control Objective 3 .	Documented procedures examined:	<Report Findings Here>
KIF KMCP KLCP	32-8.1.b Interview responsible personnel and observe conveyance processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the conveyance processes observed verified that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components:	
		<Report Findings Here>	
32-8.2 The KIF must implement mutually authenticated channels for communication between distributed KIF functions—e.g., between a host used to generate keys and a host used to distribute keys.			
KIF KMCP KLCP	32-8.2 Examine documented procedures to confirm they specify the establishment of a channel for mutual authentication of the sending and receiving devices.	Documented procedures examined:	<Report Findings Here>
32-8.3 The KIF must ensure that injection of enciphered secret or private keys into POI devices meets the requirements of Control Objective 4 .			
32-8.4 The channel for mutual authentication is established using the requirements of Control Objective 4 .			
KIF KLCP	32-8.4.a Examine documented procedures for key loading to hosts and POI devices to verify that they are in accordance with applicable criteria in Control Objective 4 .	Documented procedures examined:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	32-8.4.b Interview responsible personnel and observe key-loading processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.	Responsible personnel interviewed:	<Report Findings Here>
		Identify the P2PE Assessor who confirms that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components:	<Report Findings Here>
32-8.5 The KIF must implement a mutually authenticated channel for establishment of enciphered secret or private keys between POI devices and an HSM at the KIF.			
KIF KLCP	32-8.5 Examine documented procedures to confirm they specify the establishment of a mutually authenticated channel for establishment of enciphered secret or private keys between sending and receiving devices—e.g., POI devices and HSMs.	Documented procedures examined:	<Report Findings Here>
32-8.6 Mutual authentication of the sending and receiving devices must be performed. <ul style="list-style-type: none"> • KIFs must validate authentication credentials of a POI device prior to any key transport, exchange, or establishment with that device. • POI devices must validate authentication credentials of KDHS prior to any key transport, exchange, or establishment with that device. • When a KLD is used as an intermediate device to establish keys between POI devices and a KIF HSM it must not be possible to insert an unauthorized SCD into the flow without detection. 			
KIF KLCP	32-8.6 Interview responsible personnel and observe processes for establishment of enciphered secret or private keys between sending and receiving devices to verify: <ul style="list-style-type: none"> • KIFs validate authentication credentials of a POI device prior to any key transport, exchange, or establishment with that device. • POI devices validate authentication credentials of KLDs prior to any key transport, exchange, or establishment with that device. • When a KLD is used as an intermediate device to establish keys between POI devices and a KIF HSM, it is not possible to insert an unauthorized SCD into the flow without detection. 	Responsible personnel interviewed:	<Report Findings Here>
		Describe how the processes observed verified that: <ul style="list-style-type: none"> • KIFs validate authentication credentials of a POI prior to any key transport, exchange, or establishment with that device. • POI devices validate authentication credentials of KLDs prior to any key transport, exchange, or establishment with that device. • When a KLD is used as an intermediate device to establish keys between POIs and a KIF HSM, it is not possible to insert an unauthorized SCD into the flow without detection. 	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>32-8.7 Mechanisms must exist to prevent a non-authorized host from injecting keys into POI devices or an unauthorized POI device from establishing a key with a legitimate KIF component.</p>			
KIF KLCP	<p>32-8.7 Examine documented procedures to confirm they define mechanisms to prevent an unauthorized host from performing key transport, key exchange, or key establishment with POI devices.</p>	Documented procedures examined:	<Report Findings Here>
<p>32-9 The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD.</p> <p>The secure room for key injection must include the following:</p> <ul style="list-style-type: none"> • Effective 1 January 2021, the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. Only encrypted key injection shall be allowed for POI v3.0 and higher devices. • Effective 1 January 2023, the same restriction applies to entities engaged in key injection of devices for which they are the processors. <p>Note: This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the PCI PTS POI Security Requirements. It does apply to all other methods of loading of clear-text keying material for POI v3.0 and higher devices.</p>			
<p>32-9.1 The secure room must have walls made of solid materials. In addition, if the solid walls do not extend from the real floor to the real ceiling, the secure room must also have extended walls from the real floor to the real ceiling using sheetrock or wire mesh.</p> <p>Note: In KIF environments where Level 1 and Level 2 physical barrier controls are in place and confirmed, the secure room may be implemented within a “caged” environment. A caged environment is an enclosed secure room that meets the criteria of Requirement 32 but is not made of solid walls. Refer to applicable requirements within this Domain for additional information on Level 1 and Level 2 physical barrier controls. All other criteria stated in Requirements 13-9 and 32-9 relating to clear-text secret and/or private keys and/or their components existing in unprotected memory outside the secure boundary of an SCD for loading keys apply.</p>			
KIF KLCP	<p>32-9.1 Inspect the secure room designated for key injection to verify that it is constructed with extended walls from the real floor to the real ceiling using sheetrock or wire mesh.</p>	Identify the P2PE Assessor who confirms that the secure area designated for key injections is constructed with extended walls from the real floor to the real ceiling using sheetrock or wire mesh:	<Report Findings Here>
<p>32-9.2 Any windows into the secure room must be locked and protected by alarmed sensors.</p>			
KIF KLCP	<p>32-9.2.a Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.</p>	Identify the P2PE Assessor who confirms all windows in the secure room are locked and protected by alarmed sensors:	<Report Findings Here>

<i>Key Management – Reporting</i>			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	32-9.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.	Identify the P2PE Assessor who confirms the configuration of window sensors verified that the alarm mechanism is active:	<Report Findings Here>
32-9.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.			
KIF KLCP	32-9.3 Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	Describe how the observation of windows and glass walls in the secure areas verified that they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area:	<Report Findings Here>
32-9.4 A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.			
KIF KLCP	32-9.4 Inspect the secure room to verify that it is only accessed through a solid-core or a steel door, with door hinges that cannot be removed from outside the room.	Identify the P2PE Assessor who confirms that the secure area is only accessed through a solid-core or a steel door, with door hinges that cannot be removed from outside of the room:	<Report Findings Here>
32-9.5 An electronic access control system (e.g., badge and/or biometrics) must be in place that enforces:			
<ul style="list-style-type: none"> • Dual-access requirements for entry into the secure room, and • Anti-pass-back requirements. 			
KIF KLCP	32-9.5 Observe authorized personnel entering the secure room to verify that a badge-control system is in place that enforces the following requirements: <ul style="list-style-type: none"> • Dual-access for entry to the secure room • Anti-pass-back 	Describe how the observation of authorized personnel entering the secure area verified that a badge-control system is in place that enforces the following requirements: <ul style="list-style-type: none"> • Dual-access for entry to the secure area • Anti-pass-back 	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>32-9.6 The badge-control system must support generation of an alarm when one person remains alone in the secure room for more than 30 seconds. Note: Examples of alarm-generation mechanisms include but are not limited to motion detectors, login/logout controls, biometrics, badge sensors, etc.</p>			
KIF KLCP	<p>32-9.6 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.</p>	<p>Describe how the observation of authorized personnel entering the secure area verified that a badge-control system is in place that enforces the following requirements:</p> <ul style="list-style-type: none"> • Dual-access for entry to the secure area • Anti-pass-back <p><Report Findings Here></p>	
<p>32-9.7 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. The recording must continue for at least a minute after the last pixel of activity subsides.</p>			
KIF KLCP	<p>32-9.7 Inspect CCTV configuration and examine a sample of recordings to verify that CCTV monitoring is in place on a 24/7 basis.</p>	Sample of CCTV recordings reviewed:	<Report Findings Here>
		<p>Describe how the CCTV configurations observed verified that CCTV monitoring is in places on a 24/7 basis:</p> <p><Report Findings Here></p>	
<p>32-9.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.</p>			
KIF KLCP	<p>32-9.8 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.</p>	Monitoring personnel interviewed:	<Report Findings Here>
		<p>Describe how the observed configuration of monitoring systems verified that monitoring is supported on a continuous (24/7) basis and alarms can be resolved by authorized personnel:</p> <p><Report Findings Here></p>	
<p>32-9.9 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 key-injection secure room.</p>			
KIF KLCP	<p>32-9.9.a Inspect location of the CCTV server and digital-storage to verify they are located in a secure location that is separate from the key-injection secure room.</p>	Identify the P2PE Assessor who confirms the location of the CCTV server and digital-storage are located in a secure area that is separate from the key-injection area:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
KIF KLCP	32-9.9.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 key-injection secure room do not have access to the CCTV server/storage secure location.	Identify the P2PE Assessor who identified all personnel with access to the CCTV server/storage area and the key-injection area, and who confirms that personnel with access to the keyinjection area do not have access to the CCTV server/storage area:	<Report Findings Here>
32-9.10 The CCTV cameras must be positioned to monitor: <ul style="list-style-type: none"> • The entrance door, • SCDs, both pre and post key injection, • Any safes that are present, and • The equipment used for key injection. 			
KIF KLCP	32-9.10 Inspect CCTV positioning and examine a sample of recordings to verify that CCTV cameras are positioned to monitor: <ul style="list-style-type: none"> • The entrance door, • SCDs, both pre and post key injection, • Any safes that are present, and • The equipment used for key injection. 	Sample of recordings reviewed:	<Report Findings Here>
		Identify the P2PE Assessor who confirms that CCTV cameras are positioned to monitor the entrance door, SCDs (both pre and post key injection), any safes that are present, and the equipment used for key injection:	<Report Findings Here>
32-9.11 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.			
KIF KLCP	32-9.11 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.	Sample of recordings reviewed:	<Report Findings Here>
		Identify the P2PE Assessor who confirms that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>32-9.12 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.</p>			
KIF KLCP	<p>32-9.12.a Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.</p>	Identify the P2PE Assessor who confirms that at least the most recent 45 days of images are securely archived:	<Report Findings Here>
KIF KLCP	<p>32-9.12.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.</p>	Describe how the system configurations observed verified that where digital-recording mechanisms are in use, 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>	
<p>33-1 Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed on account-data processing devices before they are placed into service, as well as devices being decommissioned.</p>			
CA/RA KIF KLCP SP	<p>33-1.a Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for account-data processing devices placed into service, initialized, deployed, used, and decommissioned.</p>	Documented procedures examined:	<Report Findings Here>
CA/RA KIF KLCP SP	<p>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.</p>	Documented records reviewed:	<Report Findings Here>
<p>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.</p>			
KIF KMCP KLCP SP	<p>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.</p>	Documented key-management policies and procedures examined:	<Report Findings Here>

Key Management – Reporting			
Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor’s Findings	
KIF KMCP KLCP SP	5A-1.1.b Observe key-management operations and devices to verify that all cryptographic algorithms and key sizes are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	Describe how observed key-management operations and devices verified that all cryptographic algorithms and key sizes are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms:	
		<Report Findings Here>	
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., <i>NIST Special Publication 800-57</i>). See Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.			
KIF KMCP KLC SP	5A-1.2.a Examine documented key-management procedures to verify: <ul style="list-style-type: none"> • Crypto-periods are defined for every type of key in use. • Crypto-periods are based on industry best practices and guidelines (e.g., <i>NIST Special Publication 800-57</i>). • 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>
KIF KMCP KLCP SP	5A-1.2.b Through observation of key-management operations and inspection of SCDs, verify that crypto-periods are defined for every type of key in use.	SCDs inspected:	<Report Findings Here>
		Describe how the observed key-management operations and the inspected SCDs verified that crypto-periods are defined for every type of key in use:	
		<Report Findings Here>	
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.			
KIF KMCP KLCP SP	5A-1.3.a Verify documentation exists describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution.	Documentation reviewed:	<Report Findings Here>
KIF KMCP KLCP SP	5A-1.3.b Observe architecture and key-management operations to verify that the documentation reviewed in 5A-1.3.a is demonstrably in use for all key-management processes.	Describe how architecture and key-management operations verified that the documentation reviewed in 5A-1.3.a is demonstrably in use for all key-management processes:	
		<Report Findings Here>	

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<p>5A-1.3.1 Maintain documentation of all cryptographic keys managed as part of the P2PE solution, including:</p> <ul style="list-style-type: none"> • 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 		
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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:	<i><Report Findings Here></i>
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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:	<i><Report Findings Here></i>
		Personnel interviewed:	<i><Report Findings Here></i>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>NIST SP800-22</i>) 		
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>NIST SP800-22</i>) 	Documented key-management policies and procedures reviewed:	<i><Report Findings Here></i>
KIF KMCP KLCP SP	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>NIST SP800-22</i>) 	Documentation reviewed:	<i><Report Findings Here></i>
		Personnel interviewed:	<i><Report Findings Here></i>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
<p>Note: This section (5I-1.1) is ONLY applicable for P2PE component providers undergoing an assessment for subsequent PCI listing of the component provider's Key Management Services. This section is not applicable to, and does not need to be completed by, P2PE solution providers (or merchants as solution providers) that include key-management functions in their P2PE solution assessment (whether those functions are performed by the solution provider or are outsourced to non-PCI listed third parties).</p>			
<p>5I-1.1 Track status of the deployed key-management services for POIs and HSMs, and provide reports to solution provider annually and upon significant changes, including at least the following:</p> <ul style="list-style-type: none"> • Types/models of POIs and/or HSMs for which keys have been injected • For each type/model of POI and/or HSM: • Number of devices • Type of key(s) injected • Key-distribution method • Details of any known or suspected compromised keys, per 22-1 <p>Note: Adding, changing, or removing POI and/or HSM types, or critical key-management methods 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.</p>			
CA/RA KIF KMCP KLCP	<p>5I-1.1.a Review component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel to confirm that the following processes are documented and implemented:</p>	Documented component provider procedures reviewed:	<Report Findings Here>
	<ul style="list-style-type: none"> • Types/models of POIs and/or HSMs for which keys have been injected • For each type/model of POI and/or HSM: • Number of devices • Type of key injected • Key-distribution method • Details of any known or suspected compromised keys, per 22-1 	Responsible component provider personnel interviewed:	<Report Findings Here>

Key Management – Reporting

Applies to	Requirements and Testing Procedures	Reporting Instructions and Assessor's Findings	
CA/RA KIF KMCP KLCP	<p>5I-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:</p> <ul style="list-style-type: none"> • Types/models of POIs for which keys have been injected • For each type/model of POI: • Number of POI devices • Type of key injected • Key-distribution method • Details of any known or suspected compromised keys, per 22-1 	Solution provider reports reviewed:	<i><Report Findings Here></i>