Payment Card Industry (PCI)
Point-to-Point Encryption

Solution Requirements and Testing Procedures

Version 2.0

June 2015

Document Changes

Date	Version	Description
14 September 2011	1.0	Initial release of *PCI Point-to-Point Encryption: Solution Requirements – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware).*
April 2012	1.1	Updated release of PCI P2PE Solution Requirements to incorporate Testing Procedures and additional guidance and content. For complete information, see *PCI P2PE Solution Requirements and Testing Procedures: Summary of Changes from PCI P2PE Initial Release.*
June 2014	2.0	Update from P2PE v1.1: For complete information, see the *Point-to-Point Encryption Standard – Summary of Changes from P2PE v.1.1 to v2.0.*

Table of Contents

Introduction: Solution Requirements for Point-to-Point Encryption

Purpose of this Document

This document, *Point-to-Point Encryption: Solution Requirements and Testing Procedures,* defines both requirements and testing procedures for Point-to-Point Encryption *(*P2PE) solutions. The objective of this standard is to facilitate the development, approval, and deployment of PCI-approved P2PE solutions that will increase the protection of account data by encrypting that data from the point of interaction within the encryption environment where account data is captured through to the point of decrypting that data inside the decryption environment, effectively removing clear-text account data between these two points.

The requirements contained within this standard are intended for P2PE solution providers and other entities that provide P2PE components or P2PE applications for use in P2PE solutions, as well as P2PE assessors evaluating these entities. Additionally, merchants benefit from using P2PE solutions due to increased protection of account data and subsequent reduction in the presence of clear-text account data within their environments.

Types of Solution Providers

P2PE Solution Provider:

A P2PE solution provider is an entity with a third-party relationship with respect to its merchant customers (e.g., a processor, acquirer, or payment gateway) that has overall responsibility for the design and implementation of a specific P2PE solution, and manages P2PE solutions for its merchant customers. The solution provider has overall responsibility for ensuring that all P2PE requirements are met, including any P2PE requirements performed by third-party organizations on behalf of the solution provider (e.g., certification authorities and key-injection facilities).

Merchant as a Solution Provider/Merchant-managed Solution

The terms “merchant as a solution provider” and “merchant-managed solution” apply to merchants who choose to manage their own P2PE solutions on behalf of their own merchant encryption environments rather than outsourcing the solution to a third-party P2PE solution provider. Domain 4 defines the separation needed between encryption environments where the encrypting POI devices are physically located and the merchant’s account data decryption environment (and other merchant cardholder data environments) for a merchant-managed solution. ***Domain 4 is only applicable for merchant-managed solutions (MMS)***. In addition to meeting requirements specified in Domain 4, merchants acting as their own solution providers have the same responsibilities of solution providers mentioned throughout this document and are in scope for all other P2PE requirements (in Domains 1, 2, 3, 5 and 6).

For merchant-managed solutions, where the term “merchant” is used in Domains 1, 3, 5, and 6 of this document, those requirements refer to the merchant’s encryption environments and represent requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.

P2PE at a Glance – Overview of Domains and Requirements

The table below presents the six P2PE solution domains that represent the core areas where security controls need to be applied and validated.

This table provides an overview of each domain and its associated high-level requirements. Each requirement identified here has corresponding sub-requirements and validation procedures, which are presented in detail beginning at Domain 1: Encryption Device and Application Management.

Domain	Overview	P2PE Validation Requirements
Domain 1: **Encryption Device and Application Management**	The secure management of the PCI-approved POI devices and the resident software.	**1A** Account data must be encrypted in equipment that is resistant to physical and logical compromise. **1B** Logically secure POI devices. **1C** Use P2PE applications that protect PAN and SAD. **1D** Implement secure application-management processes. **1E** Component providers *ONLY*: report status to solution providers.
Domain 2: **Application Security**	The secure development of payment applications designed to have access to clear-text account data intended solely for installation on PCI-approved POI devices.	**2A** Protect PAN and SAD. **2B** Develop and maintain secure applications. **2C** Implement secure application-management processes.
Domain 3: **P2PE Solution Management**	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the *P2PE Instruction Manual* (PIM).	**3A** P2PE solution management. **3B** Third-party management. **3C** Creation and maintenance of *P2PE Instruction Manual* for merchants.

Domain	Overview	P2PE Validation Requirements
Domain 4: **Merchant-managed Solutions** *Note that this domain is not applicable to third-party solution providers.*	Separate duties and functions between merchant encryption and decryption environments.	**4A** Restrict access between the merchant decryption environment and all other networks/systems. **4B** Restrict traffic between the encryption environment and any other CDE. **4C** Restrict personnel access between the encryption environment and the merchant decryption environment.
Domain 5: **Decryption Environment**	The secure management of the environment that receives encrypted account data and decrypts it.	**5A** Use approved decryption devices. **5B** Secure the decryption environment. **5C** Monitor the decryption environment and respond to incidents. **5D** Implement secure, hybrid decryption processes. **5E** Component providers *ONLY*: report status to solution providers.
Domain 6: **P2PE Cryptographic Key Operations and Device Management**	Establish and administer key-management operations for account-data encryption POI devices and decryption HSMs.	**6A** Account data is processed using algorithms and methodologies that ensure they are kept secure. **6B** Account data keys and key-management methodologies 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. **6C** Keys are conveyed or transmitted in a secure manner. **6D** Key loading is handled in a secure manner. **6E** Keys are used in a manner that prevents or detects their unauthorized usage. **6F** Keys are administered in a secure manner. **6G** Equipment used to process account data and keys is managed in a secure manner. **6H** For hybrid decryption solutions: Implement secure hybrid-key management. **6I** Component providers *ONLY*: report status to solution providers.

Definition of Secure Cryptographic Devices (SCDs) to be used in P2PE Solutions

Secure cryptographic devices (SCDs) are used for the encryption and decryption of account data, as well as for the storage and management of cryptographic keys. SCDs include but are not limited to key-loading devices (KLDs), point-of-interaction (POI) encryption devices, and hardware security modules (HSMs). An SCD used for the acceptance and encryption of account data at the point of sale is required to be a PCI-approved POI device, which is a device evaluated and approved via the PCI PTS program and includes SRED (secure reading and exchange of data). HSMs used within the decryption environment for decryption of account data and related cryptographic key operations must be approved to either FIPS PUB 140-2 (overall level 3 or higher) or the PCI HSM standard.

Note that for P2PE solutions using hybrid decryption, SCDs are used for encryption of account data as well as for storage and management of cryptographic keys, but are not required for decryption of account data.

P2PE Solutions: Hardware Decryption or Hybrid Decryption

For PCI P2PE solutions, the encryption environment at the point of merchant acceptance consists exclusively of hardware encryption done within PCI-approved POI devices.

PCI P2PE decryption environments require HSMs for *all* management of cryptographic keys, and that HSMs be used for decryption of account data (hardware decryption), or optionally account data decryption can occur outside of an HSM in non-SCD "Host Systems" (hybrid decryption) meeting additional hybrid decryption requirements specified in Domains 5 and 6, in sections **5D** and **6H** respectively.

Note that hybrid decryption is NOT an option for merchant-managed solutions.

Elimination of prior terms "Hardware/Hardware" and "Hardware/Hybrid"

Previous releases of the P2PE standards utilized the terms "hardware/hardware" and "hardware/hybrid" to delineate between two potential decryption environments, as evidenced by two previous separately published standards. These terms will not be used going forward in this release because this release encompasses both decryption environment scenarios

SCD Domain Applicability

P2PE solutions require the use of various types of SCDs. To assist in evaluating these device types, the following matrix indicates the domains each SCD type must be assessed to:

	SCD Type and Usage		
Domain	**PCI-Approved POI Device for Account-Data Encryption**	**FIPS 140-2 Level 3 or PCI Approved HSM for Account-Data Decryption**	**SCD for Cryptographic Key Injection or Key Operations**
Domain 1: **Encryption Device and Application Management**	Applicable	N/A	N/A
Domain 2: **Application Security**	N/A	N/A	N/A
Domain 3: **P2PE Solution Management**	N/A	N/A	N/A
Domain 4: **Merchant-managed Solutions**	N/A	N/A	N/A
Domain 5: **Decryption Environment** [1]	N/A	Applicable	N/A
Domain 6: **P2PE Cryptographic Key Operations and Device Management**[1] (Includes Annexes)	Applicable	Applicable	Applicable

[1] For hybrid decryption environments, note that while account data decryption is performed in a Host System that meets requirements specified in Domains 5 (Section 5D) and 6 (Section 6H), cryptographic key injection and key management must still be performed in a FIPS 140-2 Level 3 HSM or a PCI-approved HSM.

P2PE Solutions and Use of Third Parties and/or P2PE Component Providers

A given P2PE solution may be entirely performed and managed by a single solution provider or by a merchant acting as its own solution provider; or certain services may be outsourced to third parties who perform these functions on behalf of the solution provider. All third parties that perform P2PE functions on behalf of a P2PE solution provider must be validated per applicable P2PE solution requirements, and such entities have the option of becoming P2PE component providers.

A **"P2PE component provider"** is an entity that provides a service assessed to a specific set of P2PE requirements and which results in a P2PE component provider listing on the PCI SSC website. P2PE component providers' services are performed on behalf of other P2PE solution providers for use in P2PE solutions.

There are two options for third-party entities performing functions on behalf of solution providers to validate compliance:

1. Undergo a P2PE assessment of relevant P2PE requirements on their own and submit the applicable P2PE Report of Validation (P-ROV) to PCI SSC for review and acceptance. Upon acceptance, the P2PE component is listed on PCI SSC's list of *Validated P2PE Components*. Or:
2. Have their services reviewed during the course of each of their solution-provider customers' P2PE assessments.

Accordingly, a solution can be reviewed via one of the following scenarios:

1. The solution provider can perform all domains (*excluding* Domain 4) in their entirety.
   - A merchant as a solution provider can perform all domains (*including* Domain 4) in their entirety.
2. A solution provider (or a merchant as a solution provider) can outsource functions and have them assessed as part of the solution provider's P2PE assessment.
3. A solution provider (or a merchant as a solution provider) can outsource certain P2PE functions (see upper sidebar) to PCI-listed P2PE component providers and report use of the PCI-listed P2PE component(s) in their P2PE Report on Validation (P-ROV).

Via requirements specified in Domain 3, solution providers (or merchants as solution providers) must manage the overall P2PE solution and any third parties used to perform P2PE functions on their behalf, whether those third parties are separately listed by PCI SSC as P2PE component providers or are assessed as part of the solution provider's P2PE assessment.

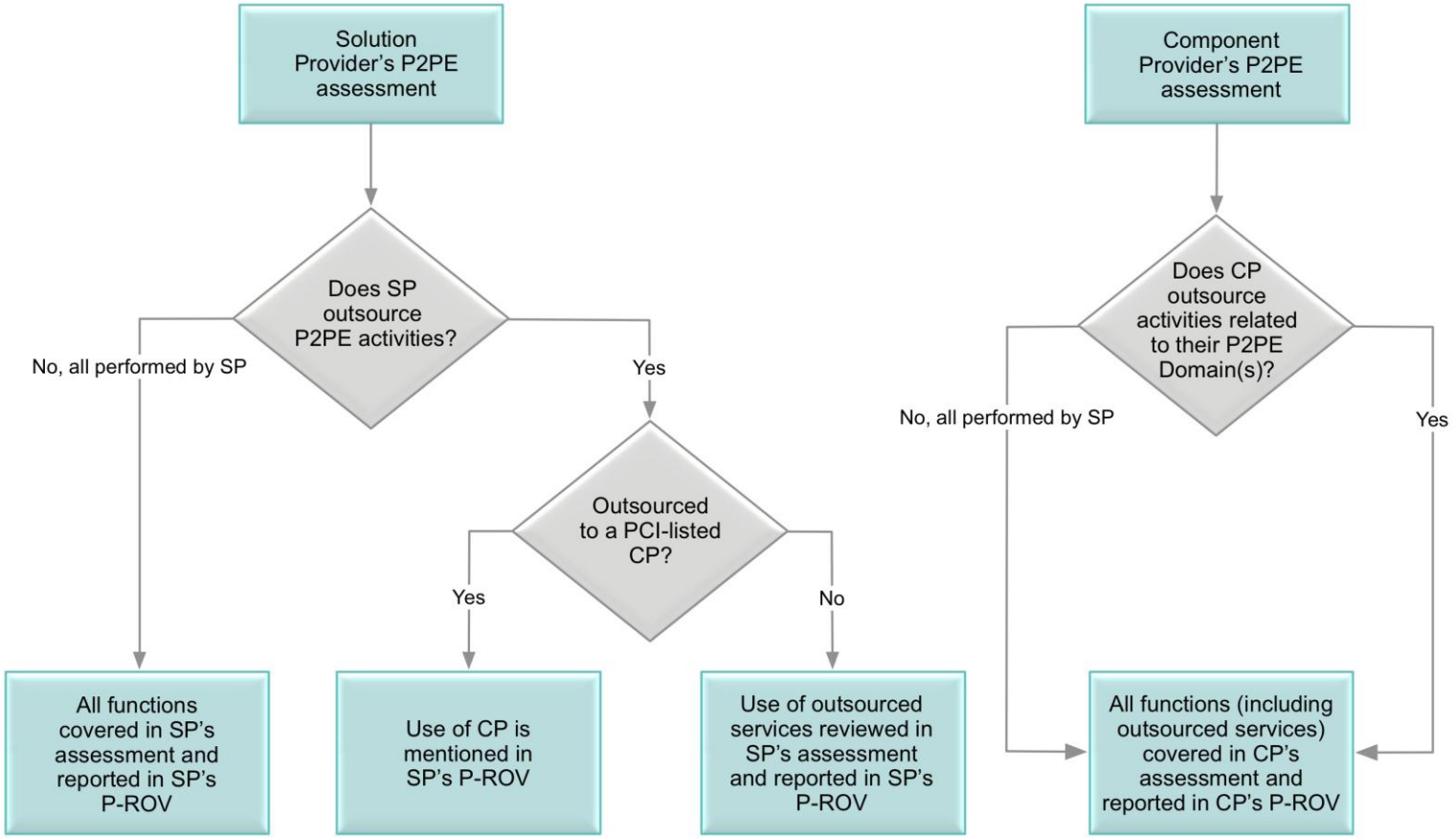
P2PE component providers may optionally be assessed for the following services:

- *Encryption-management services (Domains 1 & 6 including Annex A as applicable)*
- *Decryption-management services (Domains 5 & 6 including Annex A as applicable),*
- *Key-Injection facility services (Annex B of Domain 6)*
- *Certification Authority/Registration Authority services (Domain 6 Annex A, Part A2)*

Note that P2PE component providers are allowed to outsource elements of their respective P2PE domain(s); however, they are still ultimately responsible for ensuring all P2PE requirements for the applicable domain(s) are met. Only entities meeting all P2PE requirements for the domain(s) related to services they are offering are eligible for being listed on the PCI SSC's list of Validated P2PE Components*, whether these requirements are met directly or via outsourcing. Companies only meeting a partial set of domain requirements are not eligible for PCI SSC's listing.*

The following diagram summarizes relationships between solution providers, component providers, and other third parties performing P2PE functions on behalf of P2PE solution and/or component providers, and coverage/reporting of the applicable P2PE requirements.

P2PE Assessments: Solution Providers, Component Providers, and other Third Parties



SP – Solution Provider
CP – Component Provider
P-ROV – P2PE Report on Validation

Refer to the P2PE Program Guide for specific requirements relative to assessing and listing of P2PE component providers.

P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software

All P2PE applications and P2PE non-payment software intended for use on a PCI-approved POI device as part of a P2PE solution must be assessed either to Domain 2 or applicable requirements in Domain 1, respectively. P2PE applications may be included on PCI SSC's list of *Validated P2PE Applications*, for example, if that application may be used in more than one P2PE solution.

A **"P2PE application"** is any software or other files *with access to clear-text account data* that is intended to be loaded onto a PCI-approved POI device and used as part of a P2PE solution.

Note: *P2PE applications and P2PE non-payment software do not meet the PTS definition of "firmware" and are not reviewed as part of the PTS POI assessment. Additionally, software meeting the PTS definition of "firmware" is not reassessed during a P2PE assessment (PTS firmware is not considered a P2PE payment application, nor is it P2PE non-payment software).*

There are two approaches for an application vendor to have a P2PE application assessed for use in a P2PE solution (note that in both cases, a PA-QSA (P2PE) performs the assessment per Domain 2 requirements):

1. Undergo an independent assessment to all Domain 2 requirements:
   - Submit the application P2PE Report on Validation (P-ROV) to PCI SSC for review and acceptance, and
   - Upon acceptance, the P2PE application is listed on PCI SSC's list of *Validated P2PE Applications*.
2. Undergo an assessment to all Domain 2 requirements as part of the full assessment of the P2PE solution(s) in which the application will be used:
   - Submit the application P-ROV to PCI SSC along with the solution P-ROV.

   Note that application vendors using option 2 may optionally have their applications separately listed in PCI SSC's list of Validated P2PE Applications. Applications that are not PCI-listed are only validated for use in the P2PE solution(s) with which they were assessed. For example, this may be applicable when the application is unique and/or customized for only one solution.

"P2PE non-payment software" is any software or other files with *no access to clear-text account data* that is intended to be loaded onto a PCI-approved POI device and used as part of a P2PE solution.

- P2PE non-payment software is assessed only per designated P2PE Domain 1 Requirements at **1C-2** during the assessment of the P2PE solution(s) in which the application will be used. *Note that this software is not subject to P2PE Domain 2 Requirements.*
- P2PE non-payment software is not eligible for PCI-listing.

Refer to the P2PE Program Guide for specific requirements relative to assessing and listing P2PE applications.

Alignment of P2PE Requirements with Entities Offering P2PE Services

P2PE Domains are arranged in functional groupings of relevant P2PE requirements, to align with functions and services performed by P2PE solution providers and (if applicable) P2PE component providers and P2PE application vendors. The P2PE Domains define the relevant P2PE requirements for entities performing various P2PE functions as follows:

P2PE Domain	Entity Undergoing P2PE Validation
Domain 1: **Encryption Device and Application Management**	• Solution provider *OR* • Merchant as a solution provider *OR* • Encryption-management services component provider
Domain 2: **Application Security**	• Solution provider *OR* • Merchant as a solution provider *OR* • P2PE application vendor
Domain 3: **P2PE Solution Management**	• Solution provider *OR* • Merchant as a solution provider
Domain 4: **Merchant-managed Solutions** [2]	• Merchant as a solution provider
Domain 5: **Decryption Environment**	• Solution provider *OR* • Merchant as a solution provider *OR* • Decryption-management services component provider
Domain 6: **P2PE Cryptographic Key Operations and Device Management** (Includes Annexes)	• Solution provider *OR* merchant as a solution provider *AND/OR* • Encryption-management or decryption-management services component provider *AND/OR* • KIF or CA/RA services component provider[3]

[2] Note that for merchant-managed solutions, the "merchant as a solution provider" is responsible for all solution provider roles above (in addition to Domain 4).

[3] Please refer to table entitled *Applicability of Domain 6 and Annexes to P2PE Solution Providers and Component Providers* in the Overview section of Domain 6 for more details.

Note that the solution provider (or merchant as a solution provider) assumes ultimate responsibility for its P2PE solution regardless of whether or how many third parties provide P2PE services on behalf of the P2PE solution provider.

The following example P2PE domain responsibility scenarios are included in Appendix A to illustrate various possible roles of P2PE solution providers, P2PE component providers, P2PE application vendors, and the applicability of the P2PE domains (and subsequently the relevant requirements) for these entities that may contribute to a given P2PE solution. These scenarios are for illustration purposes only and are not meant to show every possible scenario

1. Solution provider uses a third-party POI application and manages all other solution functions.
2. Solution provider uses a third-party POI application and outsources all other solution functions.
3. Solution provider writes its own POI application(s), outsources decryption management, and manages all other solution functions.
4. Solution provider uses a third-party POI application(s), outsources device and decryption management, and manages all other solution functions.
5. Solution provider uses a third-party POI application(s), outsources to a KIF, and manages all other solution functions.
6. Solution provider outsources KIF and CA/RA functions, and manages all other solution functions.
7. Merchant-managed solution (MMS) – Merchant as the solution provider manages all functions of the solution, including writing own POI applications.
8. Merchant-managed solution (MMS) – Merchant as the solution provider uses a third-party POI application, outsources device management and KIF functions, and manages all other solution functions.
9. Merchant-managed solution (MMS) – Merchant as the solution provider outsources decryption management and manages all other functions of the solution.

Scope of Assessment for P2PE Solutions

The scope of a P2PE solution assessment covers the six P2PE domains either as part of a solution provider's full P2PE assessment, or as the cumulative result of one or more independently assessed (and PCI-listed) P2PE components or P2PE applications. See the "P2PE Solutions and use of Third Parties and/or of P2PE Component Providers" and "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software" "sections above for more information.

Here is a high-level summary of the six P2PE domains:

Domain 1 – Security requirements for the encryption environment including those for:	▪ All PCI-approved POI devices included in the P2PE solution (for the merchant to use for payment acceptance). ▪ Integration of all software onto POI devices • P2PE payment applications (subject to a Domain 2 assessment) • P2PE non-payment software (those with no access to clear-text account data—e.g., a loyalty or advertising application)
Domain 2 – Security requirements for P2PE applications	▪ For software with access to clear-text account data intended for use on POI devices.
Domain 3 – For P2PE solution management	***Note:*** *This domain cannot be outsourced to a third party or a P2PE component provider and MUST be performed by the P2PE solution provider (or merchant as a solution provider).* ▪ The solution provider's overall management of the P2PE solution including any third-party relationships, communications between various P2PE entities, and/or use of P2PE component providers. ▪ The merchant-focused *P2PE Instruction Manual (PIM)* that the solution provider prepares for and distributes to merchants (for their encryption environments), including completion of the PCI-provided *PIM Template*.
Domain 4 – For merchant as a solution provider *ONLY:*	▪ Specifies requirements for the separation between the merchant encryption environment(s) and the merchant decryption environment.
Domain 5 – Security requirements for the decryption environment, which include:	▪ Management of all system components located within or connected to the decryption environment, including those used for decryption of account data, and ▪ Maintenance of PCI DSS compliance for the decryption environment.
Domain 6 – P2PE Key-Management Operations	▪ Secure key management—including all HSMs, key-loading devices, etc.—used by the solution provider or third party for cryptographic-key operations performed in support of account-data encryption POI devices (Domain 1) and decryption HSMs (Domains 5).

Relationship between P2PE and other PCI Standards (PCI DSS, PA-DSS, PTS POI, and PIN)

Various P2PE requirements are based on elements of—or share similarities with—other PCI standards, as follows:

- POI devices (for account data encryption) are approved per PCI PIN Transaction Security (PTS) Point of Interaction (POI) requirements.
- HSMs in the decryption environment used for account-data decryption and related cryptographic-key operations are approved per PCI PTS HSM (or FIPS 140-2 level 3).
- Cryptographic-key operations for both encryption and decryption environments using key-management practices derived from the PTS PIN Security Standard.
- Applications on POI devices with access to clear-text data meet requirements derived from the Payment Application Data Security Standard (PA-DSS).
- The decryption environment is PCI DSS compliant.

Please note that this standard for point-to-point encryption solutions does not supersede the PCI Data Security Standard, PCI PIN Security Requirements, or any other PCI Standards, nor do these requirements constitute a recommendation from the Council or obligate merchants, service providers, or financial institutions to purchase or deploy such solutions. As with all other PCI standards, any mandates, regulations, or rules regarding these requirements are provided by the participating payment brands.

For Assessors: Sampling for P2PE Solutions

After considering the overall scope and complexity of the P2PE environment being assessed, the assessor may independently select representative samples of certain system components in order to assess P2PE requirements.

Selected samples must be representative of all variations or types of a particular system component. Samples must be of sufficient size to provide the assessor with assurance that controls are implemented as expected across the entire population.

Sampling of system components for assessment purposes does not reduce the scope of the solution-provider environment or the applicability of P2PE requirements. Whether or not sampling is to be used, P2PE requirements apply to the entire solution-provider environment. If sampling is used, each sample must be assessed against all applicable P2PE requirements. Sampling of the P2PE requirements themselves is not permitted.

Any sampling of POI devices and their applications, cryptographic keys, and key components must follow these principles:

- POI devices and applications/software must include every unique combination of hardware, firmware, and versions and configurations of both P2PE applications and P2PE non-payment software used by the solution.
- Samples of keys / key components must include all key types and/or functions.

Note that all HSMs (or Host Systems used in hybrid decryption) used for account data decryption must be reviewed to verify their secure configuration and therefore cannot be sampled.

For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size,
- Document any standardized processes and controls used to determine sample size,
- Document how it was verified that the standardized processes/controls ensure consistency and apply to all items in the population, and
- Explain how the sample is appropriate and representative of the overall population.

Assessors must revalidate the sampling rationale for each assessment. If sampling is to be used, different samples must be selected for each assessment.

Multiple Acquirers

The P2PE standard outlines the technology and processes needed to ensure the security of a solution that protects account data from the point of interaction to the point of initial decryption. In some instances, multiple acquirers or multiple solution providers may manage one or more P2PE solutions on the same merchant POI device. P2PE does not preclude these scenarios, as the business processes governing this shared environment are outside the responsibility of the PCI SSC. Vendors and merchants should be aware that in order for a P2PE solution to be listed on the PCI SSC website, each solution must be evaluated and tested, either independently or collectively. Once listed, merchants can then work with their acquirers to select a device and validated solution provider(s) that meet their multiple-acquirer needs.

P2PE Program Guide

Please refer to the P2PE Program Guide for information about the P2PE program, including the following topics:

- P2PE Report on Validation submission and acceptance processes.
- Annual renewal process for solutions included on the list of *Validated P2PE Solutions.*
- Vendor Release Agreements for vendors and providers of P2PE solutions, applications, and solution components.
- The P2PE Designated Change process for all new PCI-approved POI devices or P2PE applications added to an existing P2PE solution after validation.
- Notification responsibilities in the event a listed P2PE solution is determined to be at fault in a compromise.

PCI SSC reserves the right to require revalidation due to significant changes to the P2PE Solution Requirements and/or due to specifically identified vulnerabilities in a listed P2PE solution.

At-a-glance P2PE Workflow and Implementation Diagrams

See the following pages for these two diagrams.

Diagram	Title	Description
Diagram 1	**P2PE Solution and/or Component Validation Workflow at a Glance**	This chart shows the process for developing and validating a P2PE solution is provided below. The diagram illustrates the parties responsible for implementing requirements for each domain, and how validation of each domain and/or P2PE components can ultimately lead to a P2PE solution validation.
Diagram 2	**Example P2PE Implementation at a Glance**	This diagram illustrates a generic P2PE implementation and which domains apply to each of the areas involved. *Note that this diagram is for illustration purposes and shows only one type of scenario that may occur.*

The remainder of this document details the P2PE validation requirements and testing procedures on a domain-by-domain basis.

Diagram 1: P2PE Solution and/or Component Validation Workflow at a Glance

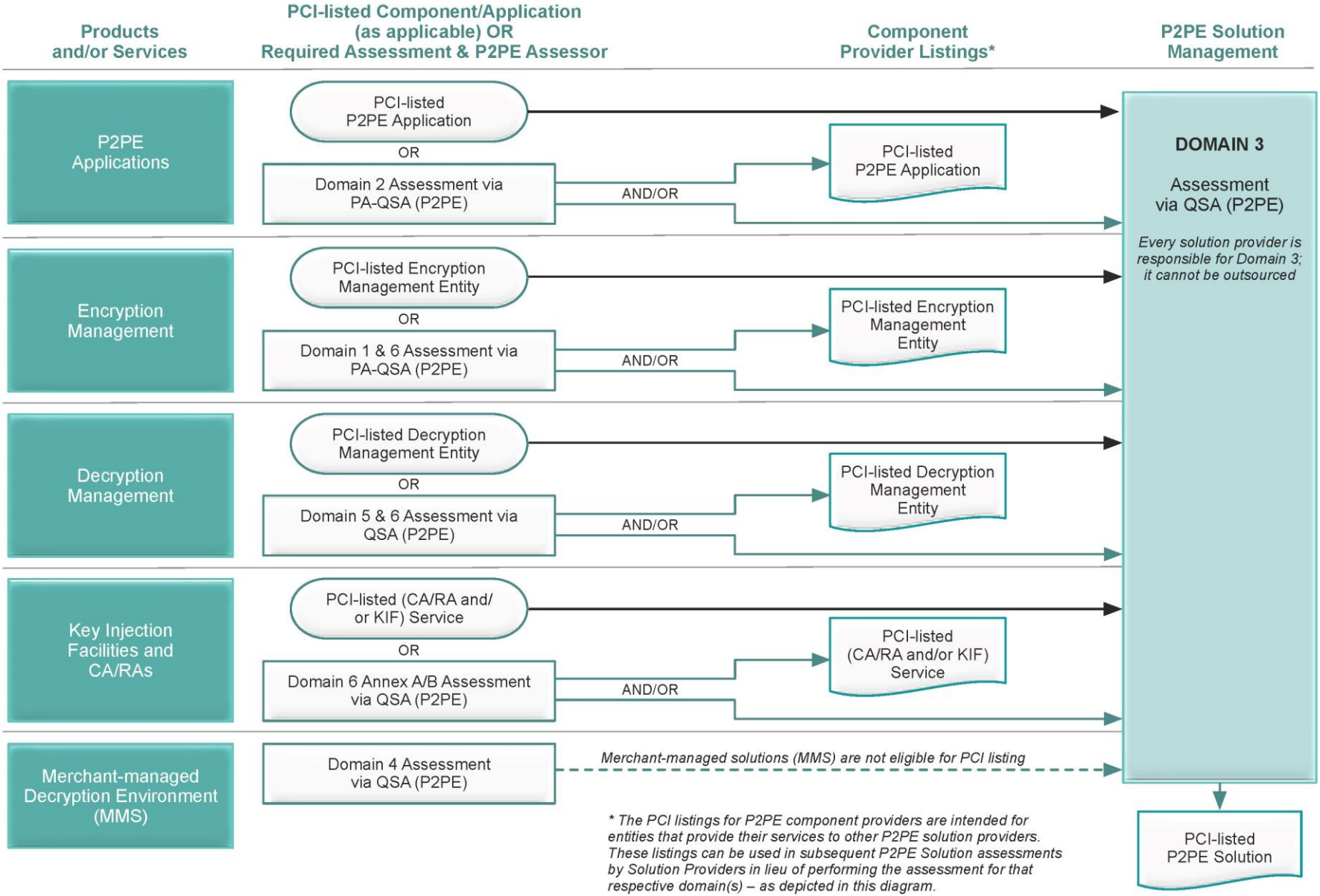
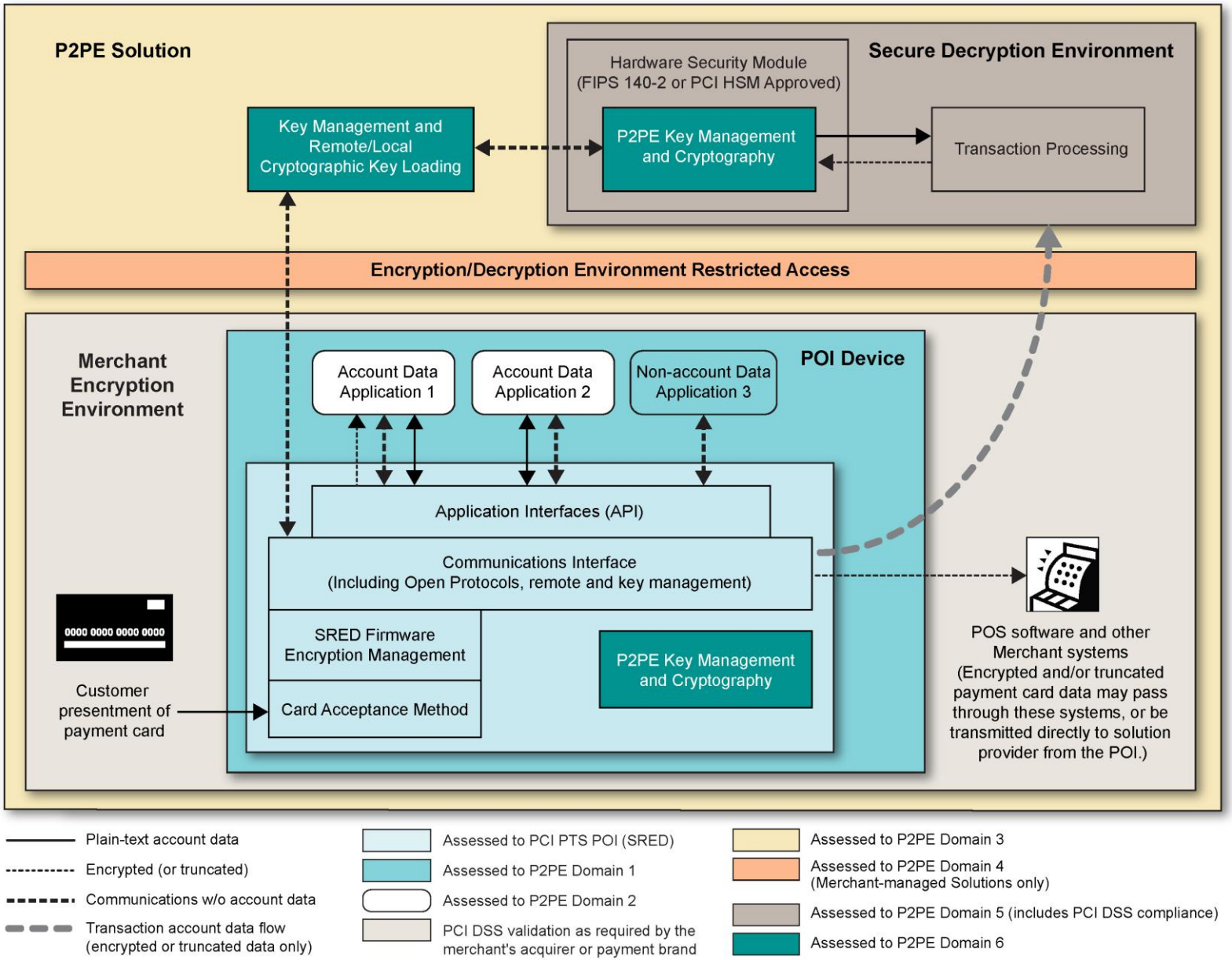


Diagram 2: Example P2PE Implementation at a Glance



Domain 1: Encryption Device and Application Management

Domain	Overview	P2PE Validation Requirements
Domain 1: **Encryption Device and Application Management**	The secure management of the PCI-approved POI devices and the resident software.	**1A** Account data must be encrypted in equipment that is resistant to physical and logical compromise. **1B** Logically secure POI devices. **1C** Use P2PE applications that protect PAN and SAD. **1D** Implement secure application-management processes. **1E** Component providers *ONLY*: report status to solution providers

Target audience: *P2PE solution providers or those who, on behalf of P2PE solution providers, manage the POI devices and their applications used in the P2PE solution.*

Overview

Domain 1 requirements encompass the use of secure point-of-interaction (POI) devices and P2PE applications and/or P2PE non-payment software. The POI device must be a PCI-approved POI device, and is typically a PIN-entry device (PED), a secure card reader (SCR), or other non-PED device that is PCI-approved. Domain 1 requirements also include the confirmation that all P2PE applications and P2PE non-payment software are properly reviewed, installed, and configured on the device.

It is not the intent of Domain 1 that solution providers actively manage POI devices when deployed at merchant locations; the intent is that the solution provider maintains knowledge of the location and status of POI devices once deployed to merchants. It may be necessary for knowledge sharing and cross-cooperation regarding the location and status of devices when different entities are responsible for managing POI devices and cryptographic keys for different functions.

Note: *All encryption devices, including POIs devices and related key-management SCDs, must additionally meet all requirements specified in Domain 6.*

Note: *Domain 1 includes the only requirements applicable to P2PE non-payment software (software on PCI-approved POI devices without access to account data). For software that* ***never has access to account data,*** *only Requirements at* ***1C-2*** *are applicable—this will validate that this software is not accessing account data, and is not bypassing or overriding any security features provided by the other approved components of the device.*

For more information, refer to the section entitled "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software."

Within this domain, the term "solution provider" refers to whichever entity is undergoing the P2PE assessment. This may be a solution provider, an encryption-management component provider, or the merchant as a solution provider.

For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 5, and 6 of this document refers to the merchant's encryption environments, and represents requirements the merchant as a solution provider is responsible for meeting for or on behalf of those merchant encryption environments.

See the "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" section for more information about validating this Domain as a solution provider, encryption-management component provider, or merchant as a solution provider.

Requirement 1A: Account data must be encrypted in equipment that is resistant to physical and logical compromise.	
Domain 1 Requirements	**Testing Procedures**
***1A-1** PCI-approved POI devices with SRED are used for transaction acceptance.*	
1A-1.1 Encryption operations must be performed using a POI device approved per the PCI PTS program (e.g., a PCI-approved PED or SCR), with SRED (secure reading and exchange of data). The PTS approval listing must match the deployed devices in the following characteristics: • Model name and number • Hardware version number • Firmware version number • SRED listed as a function provided	**1A-1.1** For each POI device type used in the solution, examine the POI device configurations and review the PCI SSC list of Approved PTS Devices to verify that all of the following POI device characteristics match the PTS listing: • Model name/number • Hardware version number • Firmware version number • SRED listed as a function provided
1A-1.1.1 The POI device's SRED capabilities must be enabled and active.	**1A-1.1.1.a** Examine the solution provider's documented procedures and interview personnel to verify that procedures are defined to ensure that SRED capabilities are enabled and active on all POI devices prior to devices being deployed to merchant encryption environments.
	1A-1.1.1.b For all POI device types used in the solution, review POI device configurations to verify that all POI device types used in the solution have SRED capabilities enabled and active (that is, the POI devices are operating in "encrypting mode") prior to devices being deployed to merchant encryption environments.
1A-1.2 POI devices must be configured to use only SRED-validated account-data capture mechanisms.	**1A-1.2.a** For all POI device types intended for use in the P2PE solution, identify and document all account-data capture interfaces.
	1A-1.2.b For each POI device type used in the solution, examine the device configuration to verify that it is configured by default to use only SRED-validated account-data capture mechanisms for accepting and processing P2PE transactions.

Requirement 1A: Account data must be encrypted in equipment that is resistant to physical and logical compromise.	
Domain 1 Requirements	**Testing Procedures**
1A-1.2.1 All capture mechanisms on the POI device must be SRED-validated, or must be disabled or otherwise prevented from being used for P2PE transactions such that they cannot be enabled by the merchant.	**1A-1.2.1.a** Examine POI configuration and deployment procedures to verify they include either: • Disabling all capture mechanisms that are not SRED validated, or • Implementing configurations that prevent all non-SRED validated capture mechanisms from being used for P2PE transactions.
	1A-1.2.1.b Verify that the documented procedures include ensuring that all non-SRED-validated capture mechanisms are disabled or otherwise prevented from being used for P2PE transactions prior to devices being deployed to merchant encryption environments.
	1A-1.2.1.c For all POI device types, verify: • All non-validated capture mechanisms are either disabled or configured to prevent their use for P2PE transactions, prior to devices being deployed to merchant encryption environments. • Disabled capture mechanisms cannot be enabled by the merchant, and/or the configurations that prevent capture mechanisms from being used for P2PE transactions cannot be enabled by the merchant.
1A-1.3 If the POI device implements open protocols as part of the solution, the device must also be validated to the PCI PTS Open Protocols (OP) module. Open protocols include the following: • Link Layer Protocols • IP Protocols • Security Protocols • IP Services	**1A-1.3** For all POI device types that implement open protocols, examine device configurations and review the list of approved PTS devices at www.pcisecuritystandards.org, to verify that all POI devices that implement open protocols used in this solution are listed. Confirm each such device has a valid SSC listing number on the PCI SSC website under “Approved PCI PTS Devices” with “OP” listed as a “function provided”.
1A-1.4 Clear-text account data must not be disclosed to any component or device outside of the PCI-approved POI device.	**1A-1.4.a** Examine documented transaction processes and data flows to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.
	1A-1.4.b Using forensic tools and/or other data tracing methods, inspect a sample of transactions to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.

Requirement 1A: Account data must be encrypted in equipment that is resistant to physical and logical compromise.	
Domain 1 Requirements	**Testing Procedures**
***1A-2** Applications on POI devices with access to clear-text account data are assessed per Domain 2 before being deployed into a P2PE solution.*	
***Note:** Applications included in a P2PE solution but not already listed on the list of Validated P2PE Applications must undergo an assessment per Domain 2 (in addition to meeting applicable application requirements in Domain 1).*	
1A-2.1 All applications on POI devices with access to clear-text account data must be assessed according to Domain 2. The assessment must match the application in the following characteristics: • Application name • Version number	**1A-2.1.a** For applications on the PCI SSC list of *Validated P2PE Applications*, review the list and compare to applications used in the solution to verify that the applications match the P2PE application listing in the following characteristics: • Application name • Version number
	1A-2.1.b For applications not on the PCI SSC list of *Validated P2PE Applications*, review the application P-ROV(s) and verify that the applications used in the solution match the application P-ROV in the following characteristics: • Application name • Version number
1A-2.2 All applications on POI devices with access to clear-text account data must only be deployed on POI device types that are: • Confirmed per **1A-1.1** as a PTS approved device(s) • Explicitly included in the Domain 2 assessment for that application.	**1A-2.2.a**.For applications on the PCI SSC list of *Validated P2PE Applications*, review the list and verify all POI device types the application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) • Explicitly included in that application's listing
	1A-2.2.b For applications not on the PCI SSC list of *Validated P2PE Applications*, review the application P-ROV and verify the POI device types the application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) • Explicitly included in that P-ROV as assessed for that application.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
***1B-1** Solution provider ensures that logical access to POI devices deployed at merchant encryption environment(s) is restricted to authorized personnel.*	
1B-1.1 Solution provider must ensure merchant logical access to POI devices, if needed, is restricted as follows: • Be read-only • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear-text PAN • Cannot view or access SAD • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear-text PAN and/or SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms	**1B-1.1.a** Examine documented POI device configuration procedures and account privilege assignments to verify that merchant logical access to POI devices is restricted as follows: • Be read-only • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear-text PAN • Cannot view or access SAD. • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear-text PAN and/or SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms
	1B-1.1.b For a sample of all POI devices used in the solution, logon to the device using an authorized test merchant account. Verify that merchant-account logical access meets the following: • Be read-only • Only view transaction-related data • Cannot view or access cryptographic keys • Cannot view or access clear-text PAN • Cannot view or access SAD. • Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear-text PAN and/or SAD • Cannot enable disabled device interfaces or disabled data-capture mechanisms
	1B-1.1.c Observe a sample of POI device configurations and interview responsible personnel to verify that the defined merchant-access requirements are configured for all devices used in the solution.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
1B-1.1.1 Where there is a legal or regulatory obligation in a region for merchants to print full PAN on merchant receipts, it is allowable for the merchant to have access to full PAN for this purpose but *ONLY* if the following are met: • The solution provider must document which payment application(s) facilitates printing of PANs for merchants. • The P2PE application that facilitates this is confirmed per **1A-2.1** as assessed to Domain 2 and on PCI SSC's list of *Validated P2PE Applications*. *Note that Domain 2 (at **2A-3.1.2**) and Domain 3 (at **3A-1.3**) also include requirements that must be met for any P2PE application and P2PE solution provider, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*	**1B-1.1.1.a** Review solution provider's documentation about the legal/regulatory obligation that requires merchants to have access to full PANs for receipt printing purposes to verify that the documentation specifies which payment application(s) facilitates printing of PANs for merchants.
	1B-1.1.1.b Review applications confirmed at **1A-2.1** to verify the application(s) that facilitates printing of full PANs on merchant receipts is on PCI SSC's list of *Validated P2PE Applications.*
1B-1.2 All solution-provider personnel with logical access to POI devices deployed in merchant encryption environments must be documented in a formal list and authorized by solution provider management. The list of authorized personnel is reviewed at least annually.	**1B-1.2.a** Examine documented authorizations to verify: • All personnel with access to devices are documented in a formal list. • All personnel with access to devices are authorized by management. • The list of authorized personnel is reviewed at least annually.
	1B-1.2.b For a sample of all POI device types, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to POI devices.
1B-1.2.1 Solution provider personnel with logical access to POI devices deployed in merchant encryption environments must be granted based on least privilege and need to know.	**1B-1.2.1a** Examine documented access-control policies and procedures to verify that solution provider personnel with logical access to POI devices deployed at merchant encryption environments is assigned according to least privilege and need to know.
	1B-1.2.1.b For a sample of all POI devices and personnel, observe configured accounts and permissions, and interview responsible personnel to verify that the level of logical access granted is according to least privilege and need to know.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
***1B-2** Solution provider secures any remote access to POI devices deployed at merchant encryption environments.*	
1B-2.1 Solution provider's authorized personnel must use two-factor or cryptographic authentication for all remote access to merchant POI devices. ***Note:** This includes remote access to POI devices via a terminal management system (TMS) or other similar systems.*	**1B-2.1.a** Examine documented procedures to verify that either two-factor or cryptographic authentication must be used for all remote access to POI devices.
	1B-2.1.b Observe remote-access mechanisms and controls to verify that either two-factor or cryptographic authentication is configured for all remote access to POI devices.
	1B-2.1.c Interview personnel and observe actual remote connection attempts to verify that either two-factor or cryptographic authentication is used for all remote access to POI devices.
1B-2.2 POI devices must be configured to ensure that remote access is only permitted from the solution provider's authorized systems.	**1B-2.2.a** Examine documented device-configuration procedures and interview personnel to verify that devices must be configured to permit remote access only from the solution provider's authorized systems.
	1B-2.2.b For all devices used in the solution, observe a sample of device configurations to verify that remote access is permitted only from the solution provider's authorized systems.
1B-2.3 POI devices must be configured such that merchants do not have remote access to the merchant POI devices.	**1B-2.3.a** Examine documented POI-configuration procedures and interview personnel to verify that devices must be configured to ensure merchants do not have remote access to the POI devices.
	1B-2.3.b For all devices used in the solution, observe a sample of device configurations to verify that merchants do not have remote access to the POI devices.
1B-2.4 Solution provider must implement secure identification and authentication procedures for remote access to POI devices deployed at merchant encryption environments, including:	**1B-2.4.a** Examine documented identification and authentication procedures to verify secure identification and authentication procedures are defined for remote access to POI devices deployed at merchant encryption environments.
	1B-2.4.b Verify documented procedures include requirements specified at **1B-2.4.1** through **1B-2.4.3**.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
1B-2.4.1 Individual authentication credentials for all authorized solution-provider personnel that are unique for each merchant. ***Note:*** *If a centralized terminal-management system (TMS) is utilized to manage multiple merchant accounts, it is acceptable for the TMS system to only require unique access for each authorized solution-provider employee accessing the TMS instead of requiring unique access per merchant.*	**1B-2.4.1** Examine device configurations and authentication mechanisms to verify that all authorized solution-provider personnel have individual authentication credentials that are unique for each merchant (or if applicable, per centralized TMS).
1B-2.4.2 Tracing all logical access to POI devices by solution-provider personnel to an individual user.	**1B-2.4.2.a** Examine POI device configurations and authentication mechanisms to verify that all logical access to POI devices can be traced to an individual user.
	1B-2.4.2.b Observe authorized logical accesses and examine access records/logs to verify that all logical access is traced to an individual user.
1B-2.4.3 Maintaining audit logs of all logical access to POI devices, and retaining access logs for at least one year.	**1B-2.4.3.a** Observe authorized logical accesses and examine access records/logs to verify that an audit log of all logical access to devices is maintained.
	1B-2.4.3.b Examine access records/logs to verify that access logs are retained for at least one year.
1B-3 *The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	
1B-3.1 Secure update processes must be implemented for all firmware and software updates, including: • Integrity check of update • Authentication of origin of the update	**1B-3.1.a** Examine documented procedures to verify secure update processes are defined for all firmware and software updates, and include: • Integrity checks of update • Authentication of origin of the update

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
	1B-3.1.b Observe a sample of firmware and software updates, and interview personnel to verify: • The integrity of the update is checked • The origin of the update is authenticated
1B-3.2 An up-to-date inventory of POI device system builds must be maintained and confirmed at least annually and upon any changes to the build.	**1B-3.2.a** Examine documented procedures to verify they include: • Procedures for maintaining an up-to-date inventory of POI device system builds • Procedures for confirming all builds at least annually and upon any changes to the build
	1B-3.2.b Review documented inventory of devices, and examine the inventory of system builds to verify: • The inventory includes all POI device system builds. • The inventory of POI device system builds is up-to-date.
	1B-3.2.c Observe results of vulnerability assessments and interview responsible personnel to verify vulnerability assessments are performed against all POI device system builds: • At least annually and • Upon any changes to the build
1B-3.3 Critical software security updates must be deployed to POI devices in the field within 30 days of receipt from device vendors or application vendors.	**1B-3.3.a** Examine documented procedures to verify they include defined procedures for deploying critical software security updates to POI devices in the field within 30 days of receipt from device or application vendors.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
	1B-3.3.b Examine security update deployment records and device logs, and interview responsible solution provider personnel and to verify that critical security updates are deployed to devices and applications in the field within 30 days of receipt from device and application vendors. .
1B-3.4 Updates must be delivered in a secure manner with a known chain-of-trust, as defined by the vendor—e.g., in the POI device vendor's security guidance or in the P2PE application's Implementation Guide.	**1B-3.4.a** Examine documented procedures for device updates to verify they follow guidance from the device or application vendor for delivering updates in a secure manner with a known chain-of-trust.
	1B-3.4.b Observe processes for delivering updates and interview responsible personnel to verify that updates are delivered in a secure manner with a known chain-of-trust, and following guidance from the device or application vendor.
1B-3.5 The integrity of patch and update code must be maintained during delivery and deployment, as defined by the vendor—e.g., in the POI device vendor's security guidance or in the P2PE application's Implementation Guide.	**1B-3.5.a** Examine documented procedures for device updates to verify they follow guidance from the device or application vendor to maintain the integrity of all patch and update code during delivery and deployment.
	1B-3.5.b Observe processes for delivering updates and interview responsible personnel to verify that the integrity of patch and update code is maintained during delivery and deployment, and according to guidance from the device or application vendor.
	1B-3.5.c Observe authorized personnel attempt to run the update process with arbitrary code to verify that the system will not allow the update to occur.
***1B-4** Solution provider implements procedures to secure account data when troubleshooting*	
1B-4.1 Any PAN and/or SAD used for debugging or troubleshooting purposes must be securely deleted. These data sources must be collected in limited amounts and collected only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.	**1B-4.1.a** Examine the solution provider's procedures for troubleshooting customer problems and verify the procedures include: • PAN and/or SAD is never output to merchant environments • Collection of PAN and/or SAD only when needed to solve a specific problem • Storage of such data in a specific, known location with limited access • Collection of only a limited amount of data needed to solve a specific problem • Encryption of PAN and/or SAD while stored • Secure deletion of such data immediately after use
	1B-4.1.b For a sample of recent troubleshooting requests, observe data collection and storage locations, and interview responsible personnel to verify the procedures identified at **1B-4.1.a** were followed.

Requirement 1B: Secure logical access to POI devices.	
Domain 1 Requirements	**Testing Procedures**
***1B-5** The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).*	
1B-5.1 Any changes to critical functions of POI devices must be logged—either on the device or within the remote-management systems of the P2PE solution provider. ***Note:** Critical functions include application and firmware updates as well as changes to security-sensitive configuration options, such as whitelists or debug modes.*	**1B-5.1.a** Examine device and/or system configurations to verify that any changes to the critical functions of the POI devices are logged, including: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)
	1B-5.1.b Observe authorized personnel perform authorized changes on POI devices, as follows, and examine log files to verify that all such activities result in a correlating log file: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)

Requirement 1C: Use applications that protect PAN and SAD.	
Domain 1 Requirements	**Testing Procedures**
***1C-1** Applications are implemented securely, including when using shared resources and when updating applications and application functionality.*	
1C-1.1 Applications with access to account data must be installed and configured to only use external communication methods specified in the application's *Implementation Guide*. *Aligns with 2A-3.3*	**1C-1.1.a** Observe application and device configurations and interview personnel to verify that applications with access to account data are installed and configured to only use approved external communication methods, by following guidance in the application's *Implementation Guide.*
	1C-1.1.b For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution—that is, the application and device should be tested together with all other applications intended to be installed on the device)—and use an appropriate "test platform" (as necessary) provided by the application vendor to perform test transactions for all functions of the application that handle account data. Examine results of tests and verify that the application only uses approved external communication methods.

Requirement 1C: Use applications that protect PAN and SAD.	
Domain 1 Requirements	**Testing Procedures**

1C-1.2 Processes for any whitelisting functionality must include:
• Implementing whitelisting functionality in accordance with the device vendor's security guidance or the application's Implementation Guide.
• Cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
• Cryptographic authentication by the POI device's firmware
• Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.
• Approval of functionality by authorized personnel prior to implementation
• Documentation for all new installations or updates to whitelist functionality that includes the following:
  ○ Description and justification for the functionality
  ○ The identity of the authorized person who approved the new installation or updated functionality prior to release
  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data
Aligns with 2A-3.4
	1C-1.2 Review documented policies and procedures and interview personnel to verify that processes for implementing any whitelisting functionality include:
	• Following the device vendor's security guidance or the application's Implementation Guide
	• Cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
	• Cryptographic authentication of whitelisting functionality by the POI device's firmware
	• Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.
	• Approval of functionality by authorized personnel prior to implementation
	• Documentation for all new installations and updates to whitelist functionality that includes the following:
	  ○ Description and justification for the functionality
	  ○ The identity of the authorized person who approved the new installation or updated functionality prior to release
	  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data

1C-1.2.1 Any whitelisting functionality must only allow the output of clear-text account data for non-PCI payment brand account/card data.	**1C-1.2.1.a** Observe application and device configurations and interview personnel to verify that whitelisting functionality only allows for the output of non-PCI payment brand accounts/cards, by following guidance in either the device vendor's security guidance or the application's *Implementation Guide*.
	1C-1.2.1.b For all device types with whitelisting functionality, perform test transactions to verify output of clear-text account data is only enabled for non-PCI payment brand account/card data.

Requirement 1C: Use applications that protect PAN and SAD.	
Domain 1 Requirements	**Testing Procedures**
1C-1.2.2 Any new installations of, or updates, to whitelisting functionality must be: • Cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control. • Cryptographically authenticated by the POI device's firmware in accordance with the device vendor's security guidance or the application's *Implementation Guide.*	**1C-1.2.2** Observe the process for new installations of, or updates to, whitelisting functionality and interview personnel to verify they are performed as follows: • Cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control. • Cryptographically authenticated by the POI device firmware, in accordance with the device vendor's security guidance or the application's *Implementation Guide.*
1B-1.2.3 Any new installations of, or updates to, whitelisting functionality must follow change-control procedures that include: • Coverage for both new installations and updates to such functionality. • Description and justification for the functionality. • The identity of the person who approved the new installation or update prior to release. • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.	**1B-1.2.3** Review records of both new installations and updated whitelisting functionality, and confirm they include the following: • Coverage for both new installations and updates to such functionality. • Description and justification for the functionality. • The identity of the person who approved the new installation or update prior to release. • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.

Requirement 1C: Use applications that protect PAN and SAD.	
Domain 1 Requirements	**Testing Procedures**
***1C-2** All applications/software without a business need do not have access to account data.*	
***Note:** Requirements at **1C-2** are the only requirements applicable to applications or software on PCI-approved POI devices with no access to account data (e.g., a loyalty or advertising application).*	
1C-2.1 Processes must be documented and implemented to ensure that, prior to new installations or updates, applications/software without a business need do not have access to account data, including that the software: • Does not have any logical interfaces (e.g., application programming interfaces (APIs)) that allow for the storing, processing, or transmitting of account data. • Is cryptographically authenticated by the POI device's firmware. • Requires dual control for the application-signing process.	**1C-2.1** Review the solution provider's documented processes and interview responsible personnel to confirm the processes include: • Review of the application vendor's documentation to determine all logical interfaces used by the application/software. • Documenting how the solution provider confirmed that the application has no logical interfaces that allow for storing, processing, or transmitting account data • Authentication of the application by the POI device's firmware • Requiring dual control to authenticate the application • Following this process both for new installations and for updates.
1C-2.1.1 The application/software does not have any logical interfaces—e.g., application programming interfaces (APIs)—that allow for storing, processing, or transmitting account data.	**1C-2.1.1** For each POI device type and each application that does not have a business need to access account data, review the solution provider's documentation to verify it confirms that the application has no logical interfaces that allows for storing, processing, or transmitting account data.
1C-2.1.2 The application/software is authenticated within the POI device using an approved security mechanism of the POI device.	**1C-2.1.2** Interview solution-provider personnel and observe the process for new application installations or application updates to verify that applications with no need to access clear-text account data are authenticated to the device using an approved security mechanism.
1C-2.1.3 Require dual control for the application-signing process.	**1C-2.1.3** Interview solution-provider personnel and observe processes for new application installations or application updates to confirm that application signing is performed under dual control.

Requirement 1D: Implement secure application-management processes.	
Domain 1 Requirements	**Testing Procedures**
***1D-1** Integrity of applications is maintained during installation and updates.*	
1D-1.1 Processes must be documented and implemented to manage all changes to applications, including: • Following vendor guidance in the application's *Implementation Guide.* • Documented approval for all changes by appropriate personnel. • Documented reason and impact for all changes. • Functionality testing of all changes on the intended device(s). • Documented back-out procedures for application installations/updates. *Note that adding a changed application or a changed POI device to a PCI-listed P2PE Solution requires the Solution Provider to undergo an assessment per PCI's "Designated Change" process. See the P2PE Program Guide for more information.* *Aligns with **2C-2.1***	**1D-1.1.a** Review the solution provider's documented processes for implementing changes to applications, and interview solution-provider personnel, and confirm the following processes are in place: • Guidance in the *Implementation Guide* is followed. • All changes to applications include documented approval by appropriate authorized solution-provider personnel. • All changes to applications are documented as to reason and impact of the change. • Functionality testing of all changes on the intended devices is performed. • Documentation includes back-out procedures for application installations/updates.
	1D-1.1.b Review records of changes to applications and, and confirm the following: • All *Implementation Guide* requirements were followed. • Approval of the change by appropriate parties is documented. • The documentation includes reason and impact of the change. • The documentation describes functionality testing that was performed. • Documentation includes back-out procedures for application installations/updates.
1D-1.2 All new installations and updates to applications must be authenticated as follows: *Aligns with 2C-2.1*	**1D-1.2** Review the solution provider's documentation and confirm their documented processes include using the guidance in the application's *Implementation Guide* for any application installations and updates.
1D-1.2.1 All new installations and updates of applications must be cryptographically authenticated by the POI device's firmware.	**1D-1.2.1** Interview responsible personnel and observe installation and update processes to confirm that new application installations and updates are cryptographically authenticated by the POI device's firmware.

Requirement 1D: Implement secure application-management processes.	
Domain 1 Requirements	**Testing Procedures**
1D-1.2.2 All applications must be cryptographically signed (or similar) prior to installation on the POI device only by authorized personnel using dual control.	**1D-1.2.2** Confirm the following through interviews with responsible solution provider personnel and by observing an installation/update: • Cryptographic signing processes for applications are followed as specified in the *Implementation Guide*. • Cryptographic signing (or similar) is performed prior to installation only by authorized personnel using dual control. • All new installations and updates to applications are signed prior to installation on the device. • Cryptographic signing for new installations and updates to applications is done under dual control.
1D-1.3 The application must be configured to securely integrate with any device resources that may be shared with other applications. *Aligns with 2B-2.2*	**1D-1.3** Interview solution-provider personnel and observe configuration processes to determine that applications are integrated with any shared resources in accordance with the *Implementation Guide.*
1D-1.4 Processes must be in place to implement application developer guidance on key and certificate usage from the application's *Implementation Guide*. *Aligns with 2B-3.1.1*	**1D-1.4.a** Review the solution provider's documentation and confirm their documented processes include application developer key-management security guidance.
	1D-1.4.b Interview solution-provider personnel to confirm that they follow key-management security guidance in accordance with the *Implementation Guide*.
1D-2 Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.	
1D-2.1 Upon receipt from the application vendor, a current copy of the application vendor's *Implementation Guide* must be retained and distributed to any outsourced integrators/resellers used for the P2PE solution. *Aligns with 2C-3.1.3*	**1D-2.1** Interview solution-provider personnel and examine documentation (including a current copy of the *Implementation Guide* from the application vendor) to confirm the following: • The solution provider retains a current copy of the *Implementation Guide*. • The solution provider distributes the Implementation Guide to any outsourced integrators/resellers the solution provider uses for the P2PE solution upon obtaining updates from the application vendor.

Requirement 1E: Component providers ONLY: report status to solution providers	
Domain 1 Requirements	**Testing Procedures**
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain for subsequent PCI listing of the component provider's device-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 device-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).*	
1E-1 For component providers of encryption -management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	
1E-1.1 Track status of the encryption-management services and provide reports to solution provider annually and upon significant changes, including at least the following: • Types/models of POI devices. • Number of devices deployed and any change in numbers since last report. • Date of last inventory of POI device system builds. • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated.	**1E-1.1.a** Review component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel, and to confirm that the following processes are documented and implemented: • Types/models of POI devices. • Number of devices deployed and change since last report. • Date of last inventory of POI device system builds.. • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated.
	1E-1.1.b Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of POI devices. • Number of devices deployed and change since last report. • Date of last inventory of POI device system builds. • Date list of personnel with logical remote access to deployed merchant POI devices was last reviewed/updated.

Requirement 1E: Component providers ONLY: report status to solution providers	
Domain 1 Requirements	**Testing Procedures**
1E-1.2 Manage and monitor changes to encryption-management services and notify the solution provider upon occurrence of any of the following: • Critical software security updates deployed to POI devices. • Addition and/or removal of POI device types. • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change. • Adding, changing, and/or removing P2PE non-payment software on POI devices (without access to clear-text account data), including description of change. • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software. *Note that adding, changing, or removing POI device types, P2PE applications, and/or P2PE non-payment software may require adherence to PCI SSC's process for 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.*	**1E-1.2.a** Review component provider's documented procedures and interview responsible component-provider personnel, and confirm that processes include notifying the solution provider upon occurrence of the following: • Critical software security updates deployed to POI devices. • Addition and/or removal of POI device types. • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change. • Adding, changing, and/or removing P2PE non-payment software on POI devices (without access to clear-text account data), including description of change. • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software.
	1E-1.2.b Observe reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical software security updates deployed to POI devices. • Addition and/or removal of POI device types. • Adding, changing, and/or removing P2PE applications on POI devices (with access to clear-text account data), including description of change. • Adding, changing, and/or removing P2PE non-payment software (without access to clear-text account data), including description of change. • Updated list of POI devices, P2PE applications, and/or P2PE non-payment software.

Domain 2: Application Security

Domain	Overview	P2PE Validation Requirements
Domain 2: **Application Security**	The secure development of payment applications designed to have access to clear-text account data intended solely for installation on PCI-approved POI devices.	**2A** Protect PAN and SAD. **2B** Develop and maintain secure applications. **2C** Implement secure application-management processes.

Target audience: *Application vendors designing applications (that have access to clear-text account data) for use within PCI-approved POI devices as part of a P2PE solution.*

Overview

Although point-of-interaction (POI) devices are often considered as "hardware" devices, software is often added to POI devices after the PIN Transaction Security (PTS) evaluation and approval. (Such a device is referred to as a "PCI-approved POI device" after the PTS evaluation and approval is complete.) It is vital to the security of these devices—and the systems that rely on the operation of these devices—that any such software is assessed to confirm its secure operation. To this end, P2PE requirements specify both the confirmation that a PCI-approved POI device is in use and that P2PE applications and P2PE non-payment software are installed and configured on the device properly (Domain 1), as well as the independent assessment of all P2PE applications (with access to clear-text account data) that are resident within the POI device (Domain 2).

The PTS evaluation of a PCI-approved POI device includes all firmware in the device. While it may be possible for a POI device to implement all the necessary functionality for use in a P2PE solution solely within its existing PTS-approved firmware, generally the POI device will contain additional software. When used in a P2PE solution, all software (excluding the PCI-approved POI firmware) implemented on the POI device that has the potential to access clear-text account data (P2PE applications) must be assessed and confirmed to be secure per Domain 2 requirements. Conversely, applications without access to account data (P2PE non-payment software) are only required to meet requirements specified at **1C-2** and are not required to meet Domain 2 requirements.

Note that PA-DSS and P2PE are distinct PCI standards with separate requirements and programs, and validation against one of these standards does not imply or result in any validation against the other standard. The P2PE Standard does not require applications used in a P2PE solution to be validated to PA-DSS.

See the "*P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software"* section for more information about P2PE applications and software, and about validating P2PE payment applications per this domain.

Use of a "Test Platform"

To facilitate testing applications in accordance with the test procedures contained in this standard, it may be necessary for the application vendor to provide a test platform. A test platform is considered to be special test functionality that is either separate or absent from production-level code. The test platform must rely on as much underlying intended production-level functionality as possible. The test platform is only to serve the purpose of providing a test framework that allows for application functionality to be exercised outside of a P2PE production-level deployment environment in order to verify the application's compliance to the applicable P2PE requirements. For example, elevated privileges or access capabilities may need to be granted for the purpose of providing run-time visibility into various facets of the application's functionality. Other examples are providing a test function to initiate a test transaction, or simulating an ECR connection. It is at the P2PE assessor's discretion to request any test functionality deemed required to verify the application's compliance to any applicable P2PE requirements.

Domain 2 Informative Annex – Application's Implementation Guide

There are multiple requirements throughout Domain 2 covering content for the application's *Implementation Guide*, which is a required document per **2C-3.** All requirements for the *Implementation Guide* are summarized in the *Domain 2 Informative Annex*.

Requirement 2A: Protect PAN and SAD.	
Domain 2 Requirements	**Testing Procedures**
***2A-1** The application executes on a PCI-approved POI device with SRED enabled and active.*	
2A-1.1 The application must be intended for use on a device approved per the PCI PTS program (e.g., a PCI-approved PED or SCR), with SRED (secure reading and exchange of data). The PTS approval listing must match the following characteristics: • Model name and number • Hardware version number • Firmware version number • SRED listed as a function provided.	**2A-1.1** For each POI device type used by the application, examine the POI device configurations and review the PCI SSC list of Approved PTS Devices to verify that all of the following POI device characteristics match the PTS listing: • Model name/number • Hardware version number • Firmware version number • SRED listed as a function provided.
2A-1.2 The application must only use the PTS SRED-validated account-data capture mechanisms of the underlying POI device for accepting and processing P2PE transactions.	**2A-1.2** For each type of POI device being assessed as part of the application assessment, verify that the application only uses SRED-validated account data capture mechanisms.
***2A-2** The application does not store PAN and/or SAD for any longer than business processes require.*	
2A-2.1 The application vendor must document all flows and justify all uses of PAN and/or SAD input into, processed by, and output from the application.	**2A-2.1.a** Interview software personnel and examine the application's design documentation to verify it documents all flows and justifies all uses of PAN and/or SAD input into, processed by, and output from the application.
	2A-2.1.b Perform a source-code review and verify that PAN and/or SAD are only utilized according to the documentation.
2A-2.2 The application must not store PAN and/or SAD (even if encrypted) as follows: • Application must not store PAN data after the payment transaction is complete. • Application must not store SAD after authorization is complete. ***Note:** Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (e.g., offline transactions). However, at all times, SAD is not stored after authorization is complete.*	**2A-2.2.a** Examine the application's design documentation and verify it includes a description of the following: • How it uses PAN and/or SAD for its application processing. • How it ensures the application does not store PAN after the payment transaction is complete. • How it ensures the application does not store SAD after authorization is complete.
	2A-2.2.b Perform a source-code review to verify that the application is designed such that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.

Requirement 2A: Protect PAN and SAD.	
Domain 2 Requirements	**Testing Procedures**
	2A-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.
2A-2.3 The application must not retain PAN and/or SAD in working memory any longer than strictly necessary.	**2A-2.3.a** Examine the application's design documentation and verify it contains a detailed description of the function of the application, including how it ensures the application does not retain PAN and/or SAD in working memory any longer than strictly necessary.
	2A-2.3.b Perform a source-code review and verify that PAN and/or SAD is cleared from all working memory locations after use, including local variables (before exiting the function).
	2A-2.3.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application clears all working memory locations utilized for the temporal retention of PAN and/or SAD during processing.
2A-2.4 The application must securely delete any PAN and/or SAD stored during application processing.	**2A-2.4.a** Examine the application's design documentation and verify it describes the process used by the application to securely delete any PAN and/or SAD stored during application processing.
	2A-2.4.b Perform a source-code review and verify that the process provided by the application vendor renders all stored PAN and/or SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data.

Requirement 2A: Protect PAN and SAD.	
Domain 2 Requirements	**Testing Procedures**
	2A-2.4.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide.* Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the process provided by the application renders all PAN and/or SAD data irrecoverable, in accordance with industry-accepted standards for secure deletion of data, once the business process of the application is completed.
***2A-3** The application does not transmit clear-text PAN and/or SAD outside of the POI device, and only uses communication methods included in the scope of the PCI-approved POI device evaluation.*	
2A-3.1 The application must not output clear-text account data outside of the POI device. ***Note:** Output of clear-text data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process is assessed at Requirement **2A-3.4**.*	**2A-3.1.a** Examine the application's design documentation and verify it contains a description of the application's function, including that the application does not output clear-text account data outside of the POI device.
	2A-3.1.b Perform a source-code review and verify the application never outputs clear-text account data outside of the POI device.
	2A-3.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application does not output clear-text account data outside of the POI device.
2A-3.1.1 The output of any truncated PANs must adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs. ***Note:** This requirement does not supersede stricter requirements in place for displays of PAN—e.g., legal or payment card brand requirements for point-of-sale (POS) receipts.*	**2A-3.1.1.a** If the application outputs any truncated PANs, examine the application's design documentation and verify it contains a description of the application's function, including that any truncation of PANs adheres to the allowable number of digits as specified in PCI DSS and/or related FAQs.
	2A-3.1.1.b If the application outputs any truncated PANs, perform a source-code review and verify that any truncation of PANs adheres to the allowable number of digits as specified in PCI DSS and/or related FAQs that specify allowable digits.

Requirement 2A: Protect PAN and SAD.	
Domain 2 Requirements	**Testing Procedures**
	2A-3.1.1.c If the application outputs any truncated PANs, install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that any truncation of PANs adheres to the allowable number of digits as specified in PCI DSS and/or related FAQs.
2A-3.1.2 If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, this is ONLY allowable if the application includes the following: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and is not attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing. *Note that Domain 1 (at **1B.1.1**) and Domain 3 (at **3A-1.3**) also include requirements that must be met for any POI device and for a P2PE solution provider, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*	**2A-3.1.2.a** If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, examine the application's design documentation and verify it contains a description of the application's function, including that the printing of full PANs on merchant receipts is a legal/regulatory obligation.
	2A-3.1.2.b If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, perform a source-code review and verify the following: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and does not include any functionality that sends clear-text PANs to any devices attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing.
	2A-3.1.2.c If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and is not attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing.

Requirement 2A: Protect PAN and SAD.

Domain 2 Requirements	Testing Procedures
2A-3.2 The application must not facilitate, via its own logical interface(s), sharing of clear-text account data directly with other applications. ***Note:*** *The application is allowed to share clear-text account data directly with the POI device's SRED-approved firmware.*	**2A-3.2.a** Examine the application's *Implementation Guide* required at **2C-3** of this document and determine that it includes the following: • A list of all logical interfaces for the application, and the function/purpose of each. • The logical interfaces intended for sharing of clear-text account data (e.g., those used to pass clear-text data back to the approved firmware of the POI device). • The logical interfaces *not* intended for sharing of clear-text account data (e.g., those for communication with other applications). Examine the logical interfaces used to communicate with other applications and confirm that the application cannot share clear-text account data with other applications via these logical interfaces. *Note that the application may be the only POI-resident application at the time of assessment, but other assessed applications may be added to a P2PE solution at a later date; or the application may be added to a solution that includes pre-approved applications. The assessor must test this requirement with this point in mind.*
	2A-3.2.b Perform a source-code review and verify that the application cannot directly facilitate sharing of clear-text account data with other applications via its logical interfaces.
	2A-3.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the application cannot directly facilitate sharing of clear-text account data with other applications via its logical interfaces.

Requirement 2A: Protect PAN and SAD.

Domain 2 Requirements	Testing Procedures
2A-3.3 The application must only use external communication methods included in the PCI-approved POI device evaluation. *For example, the POI device may provide an IP stack approved per the PTS Open Protocols module, or the device may provide serial ports or modems approved by the PTS evaluation to communicate transaction data encrypted by its PCI PTS SRED functions.* ***Note:** Using any external communication methods not included the PCI-approved POI device evaluation will invalidate the PTS approval and such use is prohibited in P2PE solutions.*	**2A-3.3.a** Examine the POI device vendor's security guidance to determine which external communication methods are approved via the PCI-approved POI device evaluation. Review the application's design documentation and verify that it contains a description of the application's function including the following: • A list of the external communication methods included in the POI device vendor's security guidance. • A list of which approved external communication methods are used by the application. • A description of where external communications are used by the application.
Security of applications where the POI device implements Open Protocols is covered at Requirement **2B-2.1.**	**2A-3.3.b** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify it includes guidance that the use of any other method for external communication is not allowed.
	2A-3.3.c Perform a source-code review and verify that, when configured appropriately, the application only utilizes the external communication methods included in the POI device vendor's security guidance and does not implement its own external communication methods (e.g., does not implement its own IP stack).
	2A-3.3.d Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: The application uses only the external communication methods included in the POI device vendor's security guidance for all external communications.

Requirement 2A: Protect PAN and SAD.

Domain 2 Requirements	Testing Procedures

2A-3.4 Any whitelisting functionality implemented by the application must include guidance in the application's *Implementation Guide* that includes the following:
• How to configure the whitelisting functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data.
• How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
• How to perform cryptographic authentication by the POI device's firmware.
• That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data.
• That such functionality must be approved by authorized personnel prior to implementation.
• That all new installations or updates to whitelist functionality must include the following:
  ○ Description and justification for the functionality.
  ○ Who approved the new installation or updated functionality prior to release.
  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data.
	2A-3.4.a For any whitelisting functionality implemented by the application, examine the application's *Implementation Guide* required at **2C-3** of this document and verify it contains details to describe any whitelisting functionality and that it provides instructions as follows:
	• How to configure the application functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data
	• How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
	• How to establish cryptographically authentication by the POI device's firmware.
	• That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data.
	• That such functionality must be approved by authorized personnel prior to implementation.
	• That documentation for all new installations or updates to whitelist functionality includes the following:
	  ○ Description and justification for the functionality.
	  ○ Who approved the new installation or updated functionality prior to release.
	  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
2B-1 *The application is developed and tested according to industry-standard software development life cycle practices that incorporate information security.*	
2B-1.1 Applications must be developed based on industry best practices and in accordance with the POI device vendor's security guidance, and information security is incorporated throughout the software development life cycle. These processes must include the following:	**2B-1.1.a** Examine the application vendor's written software development processes to verify the following: • Processes are based on industry standards and/or best practices. • Information security is included throughout the software development life cycle. • Applications are developed in accordance with all applicable P2PE requirements.
	2B-1.1.b Examine the POI device vendor's security guidance, and verify that any specified software development processes are: • Incorporated into the application developer's written software development processes. • Implemented per the POI device vendor's security guidance.
	2B-1.1.c Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it provides information from the POI device vendor's security guidance applicable to the solution provider (e.g., application configuration settings which are necessary for the application to function with the device).
	2B-1.1.d Verify each of the items at **2B-1.1.1** through **2B-1.1.3** by performing the following: • Examine written software development processes and interview software developers. • Examine testing documentation and samples of test data, observe testing processes, and interview software-testing personnel. • Examine the final application product.
2B-1.1.1 Live PANs must not be used for testing or development.	**2B-1.1.1** Live PANs are not used for testing or development.
2B-1.1.2 Development, test, and/or custom application data/accounts, user IDs, and passwords must be removed before applications are released for production or released to customers.	**2B-1.1.2** Examine written software-development procedures and interview responsible personnel to verify that development, test, and/or custom application data/accounts, user IDs, and passwords are removed before an application is released for production or released to customers.

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
2B-1.2 Application code and any non-code configuration mechanisms must be reviewed prior to every release or update. The review process includes the following:	**2B-1.2** Examine written software-development procedures and interview responsible personnel to verify the application vendor performs reviews for all application code changes and non-code configuration mechanisms as follows: • Reviews are performed by an individual, other than the code author, who is knowledgeable in code-review techniques and secure coding practices. • Changes to code that manages security-sensitive configuration options are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Code reviews ensure code is developed according to secure coding guidelines.
2B-1.2.1 Review of code changes by individuals other than the originating author, and by individuals who are knowledgeable in code-review techniques and secure coding practices.	**2B-1.2.1** Examine code review results for a sample of code changes to confirm that code reviews are performed by an individual other than the code author who is knowledgeable in code-review techniques and secure coding practices.
2B-1.2.2 Performing code reviews to ensure code is developed according to secure coding guidelines.	**2B-1.2.2** Examine code-review results for a sample of code changes to verify that code reviews ensure code is developed according to secure coding guidelines.
2B-1.2.3 Confirming that appropriate corrections are implemented prior to release.	**2B-1.2.3** Examine change control documentation for a sample of code changes to verify that appropriate corrections are implemented prior to release.
2B-1.2.4 Review and approval of review results by management prior to release.	**2B-1.2.4** Examine change control documentation for a sample of code changes to verify that review results are reviewed and approved by management prior to release.
2B-1.3 All changes to the application must follow change-control procedures. The procedures must include the following:	**2B-1.3.a** Obtain and examine the developer's change-control procedures for software modifications, and verify that the procedures require the following: • Documentation of customer impact • Documented approval of change by appropriate authorized parties • Functionality testing to verify that the change does not adversely impact the security of the device • Back-out or application de-installation procedures

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
	2B-1.3.b Examine the application's Implementation Guide required at 2C-3 of this document and verify it includes the following: • Documentation detailing the impact of all changes included in the relevant application release • Instructions detailing back-out or de-installation procedures for the application
	2B-1.3.c Examine recent application changes, and trace those changes back to related change-control documentation. Verify that, for each change examined, the following was documented according to the change-control procedures:
2B-1.3.1 Documentation of impact	**2B-1.3.1** Verify that documentation of customer impact is included in the change-control documentation for each change.
2B-1.3.2 Documented approval of change by appropriate authorized parties	**2B-1.3.2** Verify that documented approval by appropriate authorized parties is present for each change.
2B-1.3.3 Functionality testing to verify that the change does not adversely impact the security of the device.	**2B-1.3.3.a** For each sampled change, verify that functionality testing was performed to verify that the change does not adversely impact the security of the device.
	2B-1.3.3.b Verify that all changes (including patches) are tested per secure coding guidance before being released.
2B-1.3.4 Back-out, rollback, or application de-installation procedures.	**2B-1.3.4** Verify that back-out, rollback, or application de-installation procedures are prepared for each change.
2B-1.4 Applications must be developed according to industry best practices for secure coding techniques, including (but not limited to): • Developing with least privilege. • Developing with fail-safe exception handling. • Developing with defensive (protective) techniques regarding the logical input interfaces of the application.	**2B-1.4** Examine software development processes and interview software developers to verify that secure coding techniques are defined and include: • Developing with least privilege. • Developing with fail-safe defaults. • Developing with defensive (protective) techniques regarding the logical input interfaces of the application.
2B-1.4.1 Application development processes must include prevention of common coding vulnerabilities.	**2B-1.4.1.a** Obtain and review software development processes for applications. Verify the process includes prevention of common coding vulnerabilities relevant to the programming languages and platforms in use.

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
	2B-1.4.1.b Verify that applications are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit vulnerabilities relevant to the application (an example of such a vulnerability would include buffer overflows).
2B-1.4.2 Application risk-assessment techniques (e.g., (application threat-modeling) must be used to identify potential application-security design flaws and vulnerabilities during the software-development process. Risk-assessment processes include the following: • Coverage of all functions of the application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within the application that interact with account data, as well as any process-oriented outcomes that could lead to the exposure of account data. • A list of potential threats and vulnerabilities resulting from account-data flow analyses and assigned risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of application risk-assessment results for management review and approval.	**2B-1.4.2** Examine written software development procedures and interview responsible personnel to verify the vendor uses application risk-assessment techniques as part of the software development process, and that the processes include: • Coverage of all functions of the application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within applications that interact with account data, as well as any process-oriented outcomes that could lead to the exposure of account data. • A list of potential threats and vulnerabilities resulting from account-data flow analyses, and assigned risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of application risk-assessment results for management review and approval.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
2B-1.5 Application vendor must provide training in secure development practices to application developers, as applicable for the developer's job function and technology used, e.g.: • Secure application design. • Secure coding techniques to avoid common coding vulnerabilities (e.g., vendor guidelines, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.). • Managing sensitive data in memory. • Code reviews. • Security testing (e.g., penetration testing techniques). • Risk-assessment techniques. ***Note:*** *Training for application developers may be provided in-house or by third parties. Examples of how training may be delivered include on-the-job, instructor-led, and computer-based.*	**2B-1.5.a** Verify documented software development processes require training in secure development practices for application developers, as applicable for the developer's job function and technology used.
	2B-1.5.b Interview a sample of developers to verify that they are knowledgeable in secure development practices and coding techniques, as applicable to the technology used.
	2B-1.5.c Examine records of training to verify that all application developers receive training as applicable for their job function and technology used.
2B-1.5.1 Training must be updated as needed to address new development technologies and methods used.	**2B-1.5.1** Examine training materials and interview a sample of developers to verify that training is updated as needed to address new development technologies and methods used.
2B-1.6 Secure source-control practices must be implemented to verify integrity of source-code during the development process.	**2B-1.6.a** Examine written software-development procedures and interview responsible personnel to verify the vendor maintains secure source-code control practices to verify integrity of source-code during the development process.
	2B-1.6.b Examine mechanisms and observe procedures for securing source-code to verify integrity of source-code is maintained during the development process.
2B-1.7 The application vendor must document and follow a software-versioning methodology as part of their system-development lifecycle. The methodology must follow the procedures in the P2PE Program Guide for changes to payment applications and include at least the following:	**2B-1.7.a** Examine documented software-development processes to verify they include the application vendor's versioning methodology, and that the versioning methodology must be in accordance with the P2PE Program Guide. Verify that the documented versioning methodology is required to be followed for the application, including all changes to the application.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
2B-1.7.1 The vendor's software versioning methodology must define the specific version elements used, including at least the following: • Details of how the elements of the version scheme are in accordance with requirements specified in the P2PE Program Guide. • The format of the version scheme, including number of elements, separators, character set, etc. (consisting of alphabetic, numeric, and/or alphanumeric characters). • Definition of what each element represents in the version scheme (e.g., type of change, major, minor, or maintenance release, wildcard, etc.). • Definition of elements that indicate use of wildcards. ***Note:*** *Wildcards may only be substituted for elements of the version number that represent non-security impacting changes. Refer to 2B-6.3 for additional requirements on the use of wildcards.*	**2B-1.7.1.a** Examine recent application changes, the version numbers assigned, and the change control documentation that specifies the type of application change and verify that the elements in the version number match the applicable change and the parameters defined in the documented versioning methodology.
	2B-1.7.1.b Interview a sample of developers and verify that they are knowledgeable in the version scheme, including the acceptable use of wildcards in the version number.

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
2B-1.8 The versioning methodology must indicate the type and impact of all application changes in accordance with the P2PE Program Guide, including: • Description of all types and impacts of application changes (e.g., changes that have no impact, low impact, or high impact to the application). • Specific identification and definition of changes that: ○ Have no impact on functionality of the application or its dependencies ○ Have impact on application functionality but no impact on security or P2PE requirements ○ Have impact to any security functionality or P2PE requirement. • How each type of change ties to a specific version number.	**2B-1.8.a** Examine the software vendor's documented versioning methodology to verify the version methodology includes: • Description of all types and impacts of application changes (e.g., changes that have no impact, low impact, or high impact to the application). • Specific identification and definition of changes that: ○ Have no impact on functionality of the application or its dependencies ○ Have impact on application functionality but no impact on security or P2PE requirements ○ Have impact to any security functionality or P2PE requirement. • How each type of change ties to a specific version number.
	2B-1.8.b Verify that the versioning methodology is in accordance with the P2PE Program Guide requirements.
	2B-1.8.c Interview personnel and observe processes for each type of change to verify that the documented methodology is being followed for all types of changes.
	2B-1.8.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change to verify that the version assigned to the change matches the type of change according to the documented methodology.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
2B-1.9 The versioning methodology must specifically identify whether wildcards are used and, if so, how they are used. The following must be included: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on the security of the application and/or the POI device. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Wildcard elements must not precede version elements that could represent security-impacting changes. Any version elements that appear after a wildcard element must not be used to represent security-impacting changes. ***Note:*** *Wildcards may only be used in accordance with the P2PE Program Guide.*	**2B-1.9.a** Examine the software vendor's documented versioning methodology to verify that it includes specific identification of how wildcards are used, including: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on the security of the application and/or the POI device. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Any elements to the right of a wildcard cannot be used for a security-impacting change. Version elements reflecting a security-impacting change must appear "to the left of" the first wildcard element.
	2B-1.9.b Verify that any use of wildcards is in accordance with the P2PE Program Guide requirements—e.g., elements that appear after a wildcard element cannot be used for a security impacting change.
	2B-1.9.c Interview personnel and observe processes for each type of change to verify that: • Wildcards are never used for any change that has an impact on security or any P2PE requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never be used to represent a security impacting change.
	2B-1.9.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change. Verify that: • Wildcards are not used for any change that has an impact on security or any P2PE requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are not used to represent a security impacting change.

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
2B-1.10 The vendor's published versioning methodology must be communicated to customers and integrators/ resellers.	**2B-1.10** Verify the application's *Implementation Guide* required at **2C-3** of this document includes a description of the vendor's published versioning methodology for customers and integrators/resellers, and includes the following: • Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.) • Details of how security-impacting changes will be indicated by the version scheme • Details of how other types of changes will affect the version • Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change
2B-1.11 If an internal version mapping to published versioning scheme is used, the versioning methodology must include mapping of internal versions to the external versions.	**2B-1.11.a** Examine the documented version methodology to verify it includes a mapping of internal versions to published external versions.
	2B-1.11.b Examine recent changes to confirm internal version mapping to published versioning scheme match according to the type of change.
2B-1.12 Software vendor must have a process in place to review application updates for conformity with the versioning methodology prior to release.	**2B-1.12.a** Examine documented software development processes and the versioning methodology to verify there is a process in place to review application updates for conformity with the versioning methodology prior to release.
	2B-1.12.b Interview software developers and observe processes to verify that application updates are reviewed for conformity with the versioning methodology prior to release.
2B-1.13 Software vendor must implement a process to document and authorize the final release of the application and any application updates. Documentation must include: • Signature by an authorized party to formally approve release of the application or application update. • Confirmation that secure development processes were followed by the vendor.	**2B-1.13.a** Examine documented processes to verify that final release of the application and any application updates are formally approved and documented, including a signature by an authorized party to formally approve the release and confirmation that all SDLC processes were followed.
	2B-1.13.b For a sample of recent releases of application and application updates, review approval documentation to verify it includes: • Formal approval and signature by an authorized party. • Confirmation that that all secure development processes were followed.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
***2B-2** The application is implemented securely, including the secure use of any resources shared between different applications.*	
2B-2.1 Where the application relies on the Open Protocol functionality of the POI device firmware, the application must be developed in accordance with the POI device vendor's security guidance. ***Note:** POI device vendor security guidance is intended for application developers, system integrators, and end-users of the platform to meet requirements in the PCI PTS Open Protocols module as part of a PCI-approved POI device evaluation.*	**2B-2.1.a** Examine documented processes (including design documentation) and verify the application is developed in accordance with the POI device vendor's security guidance.
	2B-2.1.b Review the application's *Implementation Guide* required at **2C-3** of this document and confirm that it includes the following in accordance with the POI device vendor's security guidance: • Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing • Any guidance that the POI device vendor intended for integrators/ resellers, solution providers, and/or end-users

2B-2.1.1 The application must not circumvent, bypass, or add additional services or protocols to the Open Protocols of the POI device firmware as approved and documented in the POI device vendor's security guidance. This includes the use of:
• Link Layer protocols
• IP protocols
• Security protocols
• IP services
 	
***Note:** The PTS POI Open Protocols module ensures that open protocols and services in POI devices do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device. The POI device vendor defines what protocols and services are supported by the device and provides guidance to their use.*
 	
Adding or enabling additional services or protocols, or failing to follow the issued POI device vendor's security guidance will invalidate the approval status of that device for that implementation.
	2B-2.1.1. Perform a source-code review and verify that the application:
	• Was developed according to the POI device vendor's security guidance with respect to the documented Open Protocols.
	• Does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the POI device firmware as approved and documented in the POI device's vendor security guidance. This includes the use of:
	  ○ Link Layer protocols
	  ○ IP protocols
	  ○ Security protocols
	  ○ IP services

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
2B-2.2 The application-development process must include secure integration with any resources shared with or between applications.	**2B-2.2.a** Review the POI device vendor's security guidance and the application's *Implementation Guide*. Confirm that the application's *Implementation Guide* required at **2C-3** of this document is in accordance with any applicable information in the POI device vendor's security guidance, and includes the following: • A list of shared resources. • A description of how the application connects to and/or uses shared resources. • Instructions for how the application should be configured to ensure secure integration with shared resources.
	2B-2.2.b Perform a source-code review and verify that any connection to, or use of, shared resources is done securely and in accordance with the POI device vendor's security guidance.
	2B-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that any connections to, or use of, shared resources are handled securely and in accordance with the POI device vendor's security guidance.
2B-2.3 Applications do not bypass or render ineffective any application segregation that is enforced by the POI device.	**2B-2.3** Perform a source-code review and verify that applications do not bypass or render ineffective any application segregation that is enforced by the POI device, in accordance with the POI device vendor's security guidance.
2B-2.4 Applications do not bypass or render ineffective any OS hardening implemented by the POI device.	**2B-2.4** Perform a source-code review and verify that applications do not bypass or render ineffective any OS hardening which is implemented by the POI device, in accordance with the device vendor's security guidance.
2B-2.5 Applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI device.	**2B-2.5** Perform a source-code review and verify that applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI device, in accordance with the device vendor's security guidance.

Requirement 2B: Develop and maintain secure applications.	
Domain 2 Requirements	**Testing Procedures**
2B-2.6 If the application provides configuration/update functionality at-the-terminal (e.g., using an on-screen menu system), the application must not bypass or render ineffective any applicable controls contained within this standard. ***Note:*** *Some applications may provide administrative or other privileged functions at the terminal, such as the ability to load whitelists or change other application configurations. Any such functions provided in this way must meet all applicable P2PE requirements.*	**2B-2.6** If the application provides configuration/update functionality at the terminal, perform a functional test of the application loaded on each applicable POI device type and verify that the application does not bypass or render ineffective any applicable controls contained within this standard.
2B-3 *The application vendor uses secure protocols, provides guidance on their use, and performs integration testing on the final application.*	
2B-3.1 The application developer's process must include full documentation, and integration testing of the application and intended platforms, including the following:	**2B-3.1** Through observation and review of the application developer's system development documentation, confirm the application developer's process includes full documentation and integration testing of the application and intended platforms, including the following:
2B-3.1.1 The application developer must provide key-management security guidance describing how cryptographic keys and certificates have to be used. *Examples of guidance include which cryptographic certificates to load, how to load account-data keys (through the firmware of the device), when to roll keys, etc.*	**2B-3.1.1** Review the application's *Implementation Guide* required at 2C-3 of this document, and confirm it includes key-management security guidance for solution providers, describing how cryptographic keys and certificates have to be used and managed.
2B-3.1.2 The application developer must perform final integration testing on the device, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform.	**2B-3.1.2** Interview application developers to confirm that final integration testing, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform, was performed.

Requirement 2B: Develop and maintain secure applications.

Domain 2 Requirements	Testing Procedures
2B-4 *Applications do not implement any encryption functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the POI device.*	
Note: *The application may provide additional encryption to existing SRED encryption, but cannot bypass or replace SRED encryption.*	
2B-4.1 The application must not encrypt clear-text account data. This means the application must not implement any encryption functions that bypass or are intended to be used instead of the approved SRED functions of the POI device.	**2B-4.1.a** Examine the application's *Implementation Guide* required at 2C-3 of this document and verify the description of the application's function includes the following: • Confirmation that the application does not perform encryption of clear-text account-data, nor does it replace the POI device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption
	2B-4.1.b Perform a source-code review to verify that any application functionality facilitating the encryption of account data utilizes the approved cryptographic algorithm(s) and associated key-management functions of the POI device's SRED firmware and is not implemented within the application itself.
	2B-4.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application does not perform encryption of account-data nor does it replace the SRED encryption performed by the underlying POI device's firmware.

Requirement 2C: Implement secure application-management processes.

Domain 2 Requirements	Testing Procedures
***2C-1** New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.*	
2C-1.1 Software developers must establish and implement a process to identify and test their applications for security vulnerabilities and implementation errors prior to every release (including updates or patches) using manual or automated vulnerability assessment processes.	**2C-1.1.a** Obtain and examine processes to identify new vulnerabilities and test applications for vulnerabilities that may affect the application. Verify the processes include the following: • Using outside sources for security vulnerability information. • Periodic testing of applications for new vulnerabilities.
	2C-1.1.b Interview responsible software vendor personnel to confirm the following: • New vulnerabilities are identified using outside sources of security vulnerability information. • All applications are tested for vulnerabilities.
2C-1.2 Software vendors must establish and implement a process to develop and deploy critical security updates to address discovered security vulnerabilities in a timely manner. ***Note:** A "critical security update" is one that addresses an imminent risk to account data.*	**2C-1.2.a** Obtain and examine processes to develop and deploy application security upgrades. Verify that processes include the timely development and deployment of critical security updates to customers.
	2C-1.2.b Interview responsible software-vendor personnel to confirm that application security updates are developed and critical security updates are deployed in a timely manner.
***2C-2** Applications are installed and updates are implemented only via trusted and cryptographically authenticated processes using an approved security mechanism evaluated for the PCI-approved POI device.*	
2C-2.1 Ensure that all application installations and updates are cryptographically authenticated as follows:	**2C-2.1** To confirm that all application installations and updates are cryptographically authenticated, verify the following:
2C-2.1.1 All application installations and updates are cryptographically authenticated using the approved security mechanisms of the POI device's firmware.	**2C-2.1.1.a** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify that it includes the following: • A description of how the application is cryptographically authenticated using the approved security mechanisms of the POI device's firmware for any application installations and updates. • Instructions for how to use the approved security mechanisms to perform application installations and updates. • A statement that application installations and updates cannot occur except by using the approved security mechanisms of the POI device's firmware.

Requirement 2C: Implement secure application-management processes.	
Domain 2 Requirements	**Testing Procedures**
	2C-2.1.1.b Perform a source-code review to verify that the application only allows installations and updates using the approved security mechanisms of the POI device's firmware.
	2C-2.1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that, by following the *Implementation Guide,* the application only allows installations and updates using the approved security mechanisms of the POI device's firmware.
	2C-2.1.1.d After the application is installed and configured in accordance with the *Implementation Guide,* attempt to perform an installation and an update using non-approved security mechanisms, and verify that the POI device will not allow the installation or update to occur.
2C-2.1.2 The application developer includes guidance for whoever signs the application, including requirements for dual control over the application-signing process.	**2C-2.1.2** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify that it includes the following: • Instructions for how to sign the application. • Instructions how to implement the dual control for the application-signing process. • A statement that all applications must be signed via the instructions provided in the *Implementation Guide.*
***2C-3** Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	
2C-3.1 The process to develop, maintain, and disseminate an *Implementation Guide* for the application's installation, maintenance, upgrades and general use includes the following:	**2C-3.1** Examine the *Implementation Guide* and related processes, and verify the guide is disseminated to all relevant application installers and users (including customers, resellers, and integrators).
2C-3.1.1 Addresses all requirements in P2PE Domain 2 wherever the *Implementation Guide* is referenced.	**2C-3.1.1** Verify the *Implementation Guide* covers all related requirements in P2PE Domain 2.

Requirement 2C: Implement secure application-management processes.	
Domain 2 Requirements	**Testing Procedures**
2C-3.1.2 Review of the *Implementation Guide* at least annually and upon changes to the application or the P2PE Domain 2 requirements, and update as needed to keep the documentation current with: • Any changes to the application (e.g., device changes/upgrades and major and minor software changes). • Any changes to the *Implementation Guide* requirements in this document.	**2C-3.1.2.a** Verify the *Implementation Guide* is reviewed at least annually and upon changes to the application or the P2PE Domain 2 requirements.
	2C-3.1.2.b Verify the *Implementation Guide* is updated as needed to keep the documentation current with: • Any changes to the application (e.g., device changes/upgrades and major and minor software changes). • Any changes to the *Implementation Guide* requirements in this document.
2C-3.1.3 Distribution to all new and existing application installers (e.g., solution providers, integrator/resellers, etc.), and re-distribution to all existing application installers every time the guide is updated.	**2C-3.1.3** Verify the *Implementation Guide* is distributed to new application installers, and re-distributed to all application installers every time the guide is updated.
2C-3.2 Develop and implement training and communication programs to ensure application installers (e.g., solution providers or integrators/resellers) know how to implement the application according to the *Implementation Guide*.	**2C-3.2** Examine the training materials and communication program, and confirm the materials cover all items noted for the *Implementation Guide* throughout P2PE Domain 2.
2C-3.2.1 Review the training materials for application installers on an annual basis and whenever new application versions are released. Update as needed to ensure materials are current with the *Implementation Guide*.	**2C-3.2.1** Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new application versions are released, and updated as needed.

Domain 2 Informative Annex: Summary of Contents for the *Implementation Guide* for P2PE Applications

This Annex summarizes required content for each application's *Implementation Guide,* as required for applications assessed to P2PE Domain 2, and describes and contains only those Domain 2 requirements that have related *Implementation Guide* topics. It is intended only as summary reference for required *Implementation Guide* contents and does not specify any additional requirements.

Domain 2 Requirement		Required Content for the *Implementation Guide*
2A-3.2	The application must not facilitate, via its own logical interface(s), sharing of clear-text account data directly with other applications.	• A list of all logical interfaces for the application, and the function/purpose of each. • The logical interfaces intended for sharing of clear-text account data (e.g., those used to pass clear-text data back to the approved firmware of the POI device) • The logical interfaces not intended for sharing of clear-text account data (e.g., those for communication with other applications)
2A-3.3	The application only uses external communication methods included in the PCI-approved POI device evaluation and has not implemented its own external communication stack.	Guidance that use of any other methods for external communications is not allowed.

Domain 2 Requirement		Required Content for the *Implementation Guide*

2A-3.4	Any whitelisting functionality implemented by the application must include guidance in the application's *Implementation Guide* that includes the following:
	• How to configure the whitelisting functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data.
	• How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
	• How to perform cryptographic authentication by the POI device's firmware
	• That review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.
	• That such functionality must be approved by authorized personnel prior to implementation
	• That documentation for all new installations or updates to whitelist functionality that includes the following:
	  ○ Description and justification for the functionality
	  ○ Who approved the new installation or updated functionality prior to release
	  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data
		Details to describe any whitelisting functionality implemented by the application as follows:
		• How to configure the application functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data
		• How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.
		• How to establish cryptographically authentication by the POI device's firmware
		• That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data.
		• That such functionality must be approved by authorized personnel prior to implementation
		• That documentation for all new installations or updates to whitelist functionality includes the following:
		  ○ Description and justification for the functionality
		  ○ Who approved the new installation or updated functionality prior to release
		  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data

Domain 2 Requirement		Required Content for the *Implementation Guide*
2B-1.1	Applications must be developed based on industry best practices and in accordance with the POI device vendor's security guidance, and information security is incorporated throughout the software development life cycle.	Information from the POI device vendor's security guidance applicable to the solution provider (e.g., application configuration settings which are necessary for the application to function with the device).
2B-1.3	All changes to the application must follow change-control procedures.	• Documentation detailing the impact of all changes included in the relevant application release • Instructions detailing back out or de-installation procedures for the application
2B-1.10	The vendor's published versioning methodology must be communicated to customers and integrators/resellers.	A description of the vendor's published versioning methodology, including the following: • Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.) • Details of how security-impacting changes will be indicated by the version scheme • Details of how other types of changes will affect the version • Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change
2B-2.1	Where the application relies on the Open Protocol functionality of the POI device firmware, the application must be developed in accordance with the POI device vendor's security guidance.	• Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing. • Any guidance that the POI device vendor intended for integrators/ resellers, solution providers, and/or end-users.
2B-2.2	The application development process must include secure integration with any shared resources.	Includes the following, in accordance with the POI device vendor's security guidance: • A list of shared resources • A description of how the device connects to and/or uses shared resources Instructions for how the application should be configured to ensure secure integration with shared resources
2B-3.1.1	The application developer must provide key-management security guidance describing how keys and certificates have to be used.	• Key-management security guidance for solution providers, describing how cryptographic keys and certificates have to be used and managed.

Domain 2 Requirement		Required Content for the *Implementation Guide*
2B-4.1	The application must not encrypt clear-text account data. This means the application must not implement any encryption functions that bypass or are intended to be used instead of the approved SRED functions of the POI device.	The description of the application's function that includes the following: • Confirmation that the application does not perform encryption of clear-text account data, nor does it replace the POI device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption
2C-2.1.1	All application installations and updates are cryptographically authenticated using the approved security mechanisms of the POI device's firmware.	• A description of how the application uses the approved security protocol of the POI device's firmware for any application installations and updates • Instructions for how to use the approved security protocol to perform application installations and updates • A statement that application installations and updates cannot occur except by using the approved security protocol of the POI device's firmware
2C-2.1.2	The application developer includes guidance for whoever signs the application, including requirements for dual control over the application-signing process.	• Instructions for how to sign the application • Instructions how to implement the dual control for the application-signing process • A statement that all applications must be signed via the instructions provided in the *Implementation Guide.*

Domain 3: P2PE Solution Management

Domain	Overview	P2PE Validation Requirements
Domain 3: **P2PE Solution Management**	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the *P2PE Instruction Manual* (PIM).	**3A** P2PE solution management **3B** Third-party management **3C** Creation and maintenance of *P2PE Instruction Manual* for merchants

Target Audience: *The solution provider (or merchant as a solution provider for merchant-managed solutions), who maintains ultimate responsibility of the P2PE solution.*

Overview

The effective management and integration of the essential elements comprising the P2PE solution ultimately results in the absence of clear-text account data within the merchant's encryption environment—e.g., merchant stores, shops, retail premises, etc. Domain 3 is critical to the P2PE solution due to the fact that P2PE solutions consist of numerous devices/products (POI devices, Applications, HSMs) operating in various environments (encryption, decryption, and key-injection), and all of these devices, products, and environments must be successfully integrated together and managed.

Additionally, requirements in Domain 3 include providing detailed instructions for the merchant in the *P2PE Instruction Manual* (PIM). The PIM Template is provided as a separate document so that the solution provider can easily 1) determine required content for the PIM, and 2) transfer that content to the template to produce the PIM deliverable for merchants. The PIM provides merchants pertinent guidance to effectively and securely manage their encryption environments and devices within their purview: e.g., the secure installation of POI devices, monitoring POI devices for signs of tampering, and appropriate incident response procedures for security incidents.

Note: *For merchant-managed solutions, the merchant as a solution provider must prepare the P2PE Instruction Manual (PIM) for its encryption environments.*

For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 5, and 6 of this document refers to the merchant's encryption environments, and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
***3A-1** The solution provider maintains documentation detailing the P2PE solution architecture and data flows.*	
3A-1.1 Current documentation must be maintained to describe or illustrate the architecture of the overall P2PE solution and include the following: • Identification of all parts of the overall solution managed by the solution provider • Identification of any parts of the overall solution outsourced to third-party service providers • Identification of P2PE controls covered by each third-party service provider.	**3A-1.1.a** Interview relevant personnel and review documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the overall P2PE solution.
	3A-1.1.b Interview relevant personnel and review documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document is current.
	3A-1.1.c Interview relevant personnel and review documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document: • Identifies all components of the overall solution managed by the solution provider. • Identifies all components of the overall solution that have been outsourced to third-party solution providers. • Identifies all P2PE controls covered by each third-party service provider.
3A-1.2 Current documentation (including a data-flow diagram) must include details of the account-data flow from the POI device (the point the card data is captured and encrypted) through to the point the encrypted card data is decrypted and the clear-text data exits the decryption environment.	**3A-1.2** Examine the data-flow diagram and interview personnel to verify the diagram: • Shows all account data flows across systems and networks from the point the card data is captured through to the point the card data exits the decryption environment. • Is kept current and updated as needed upon changes to the environment.

Requirement 3A: P2PE solution management

Domain 3 Requirements	Testing Procedures
3A-1.3 Where there is a legal or regulatory obligation in a region for merchants to print full PAN on merchant receipts, it is allowable for the merchant to have access to full PAN for this purpose but the solution provider must document specifics about the legal or regulatory obligation including at least the following: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies *Note that Domain 1 (at **1B-1.1.1**) and Domain 2 (at **2A-3.1.2**) also include requirements that must be met for any POI device and any P2PE application, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*	**3A-1.3.a** Review solution provider's documentation about the legal/regulatory obligation that requires merchants to have access to full PANs for receipt printing purposes to verify that the documentation includes at least the following details about the legal/regulatory obligation: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies
	3A-1.3.b Perform independent review of, or conduct interviews with responsible solution provider personnel, to verify that the exception to facilitate merchants' access to full PANs is based on a legal/regulatory obligation and not solely for convenience.
***3A-2** The solution provider manages and monitors status reporting from P2PE component providers.*	
3A-2.1 Where P2PE component providers are used, a methodology must be implemented to manage and monitor status reporting from P2PE component providers, including: • Ensuring reports are received from all P2PE component providers as specified in the "*Component providers ONLY: report status to solution providers*" sections of Domains 1, 5, and/or 6 (as applicable to the component provider). • Confirming reports include at least the details specified in the "*Component providers ONLY: report status to solution providers*" sections of Domains 1, 5, and/or 6 (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider. • Following up with the component provider to resolve any questions or changes in expected performance of the component provider.	**3A-2.1** Where component providers are used, interview responsible personnel, review documentation, and observe processes to verify the solution provider has implemented a methodology for managing and monitoring status reporting from P2PE component providers, including processes for: • Ensuring reports are received from all P2PE component providers as specified in the "*Component providers ONLY: report status to solution providers*" sections of Domains 1, 5, and/or 6 (as applicable to the component provider). • Confirming reports include at least the details specified in the "*Component providers ONLY: report status to solution providers*" sections of Domains 1, 5, and/or 6 (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider. • Following up with the component provider to resolve any questions or changes in expected performance of the component provider.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-2.2 Processes must be implemented to ensure P2PE controls are maintained when changes to the P2PE solution occur including, but not limited to: • Changes in third-party service providers • Changes in overall solution architecture	**3A-2.2.a** Interview responsible personnel and review documentation to verify the solution provider has a formal process for ensuring P2PE controls are maintained when changes to the P2PE solution occur, including procedures for addressing the following: • Changes in third-party service providers • Changes in overall solution architecture
	3A-2.2.b For a sample of changes, verify changes were documented and the solution updated accordingly.
3A-3 *Solution provider implements processes to respond to notifications from merchants, component providers, and/or other third parties, and provide notifications about any suspicious activity involving the P2PE solution.*	
3A-3.1 Processes must be implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity, and provide immediate notification to all applicable parties of suspicious activity including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures ***Note:*** *"immediate" means promptly or as soon as possible.*	**3A-3.1** Examine documented procedures and interview personnel to verify processes are implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity and provide immediate notification to all applicable parties, including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures
3A-3.2 Upon detection of any suspicious activity defined at **3B-4.1**, the POI device must be immediately removed, shut down, or taken offline until the integrity of the device is verified and the P2PE encryption mechanism is restored.	**3A-3.2** Review documented procedures and interview responsible personnel to verify that upon detection of any suspicious activity defined at **3A-4.1**, POI devices are immediately removed, shut down, or taken offline.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-3.2.1 The POI device must not be re-enabled until it is confirmed that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has provided written notification (signed by a merchant executive officer) formally requesting stopping of P2PE encryption services, according to the solution provider's procedures (as defined in Requirement **3B-5.1**).	**3A-3.2.1** Examine documented procedures and interview personnel to verify the POI devices must not be re-enabled until it is confirmed that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has provided written notification (signed by a merchant executive officer) requesting stopping of P2PE encryption services, according to the solution provider's procedures (as defined in Requirement **3B-5.1**).
3A-3.3 The solution provider must maintain a record of all suspicious activity, to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that the issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled	**3A-3.3** Examine documented procedures and related records, and interview personnel to verify they maintain records of all suspicious activity, including the following details: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled.
3A-3.4 Procedures must incorporate any applicable incident response procedures defined by the PCI payment brands, including timeframes for reporting incidents.	**3A-3.4.a** Examine documented incident-response plans to verify they incorporate procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.
	3A-3.5.b Interview responsible personnel to verify that any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents, are known and implemented.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-3.5 Processes must be implemented to ensure any P2PE control failures are addressed including, but not limited to: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Updating the solution and/or controls to prevent cause from recurring	**3A-3.5.a** Interview responsible personnel and review documentation to verify the solution provider has a formal process for any P2PE control failures, including procedures for addressing the following: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Implementing controls to prevent cause from recurring
	3A-3.6.b For a sample of P2PE control failures, interview personnel and review supporting document to verify that: • Identification occurred. • Corrective actions were implemented and documented. • The solution and/or control was updated accordingly.
***3A-4** If the solution allows a merchant to stop P2PE encryption of account data, the solution provider manages the related process for merchants.*	
3A-4.1 If the solution provides an option to allow merchants to stop P2PE encryption of account data, the solution provider must document and implement a process for merchants that includes the following:	**3A-4.1** If the solution provides an option to allow merchants to stop P2PE encryption of account data, examine documented procedures to verify the solution provider has a documented process for merchants to follow that includes the requirements specified at **3A-4.1.1** and **3A-4.1.2**.
3A-4.1.1 P2PE encryption of account data for a merchant is stopped only upon receipt by the solution provider of a formal request from the merchant (signed by a merchant executive officer).	**3A-4.1.1** Interview responsible personnel and observe processes to verify that P2PE encryption of account data for a merchant is stopped only upon receipt by the solution provider of a formal notification request from the merchant (signed by a merchant executive officer).
3A-4.1.2 Maintaining records of all such requests received from merchants, including the following: • Identification of merchant submitting request • Date request received • Copy of the formal notification from merchant	**3A-4.1.2** Observe implemented processes and interview responsible personnel to verify a record of all received requests is maintained and includes: • Identification of merchant submitting request • Date initial request received • Copy of the formal notification from merchant

Requirement 3B: Third-party management	
Domain 3 Requirements	**Testing Procedures**
3B-1 *The solution provider facilitates and maintains formal agreements with all third parties contracted to perform P2PE functions on behalf of the solution provider.*	
3B-1.1 Solution provider must have formal agreements in place with all third parties that perform P2PE functions on behalf of the solution provider, including: • All functions each third party is responsible for • Agreement to maintain P2PE controls for which they are responsible • Notification and documentation of any changes affecting the third party governed by P2PE requirements • Notification of any security-related incidents • Defining and maintaining appropriate service level agreements (SLAs) • Maintaining compliance with applicable P2PE and/or PCI DSS requirements as needed • Agreement to provide proof of compliance with P2PE requirements and/or PCI DSS requirements as needed • Agreement to provide reports to solution provider as required in the "*Component providers ONLY: report status to solution providers*" section of the applicable P2PE Domain.	**3B-1.1.a** Examine documented procedures to verify the solution provider has a formalized process in place to establish agreements with all third parties performing services or functions governed by any other domain within this standard. The formalized agreement must include: • All functions each third party is responsible for • Maintaining P2PE controls for which they are responsible • Notification and documentation of any changes affecting the third party governed by P2PE requirements • Notification of any security-related incidents • Defining and maintaining appropriate service level agreements (SLAs) • Maintaining compliance with applicable P2PE and/or PCI DSS requirements as needed • Agreement to provide proof of compliance with P2PE requirements and/or PCI DSS requirements as needed • Agreement to provide reports to solution provider as required in the "*Component providers ONLY: report status to solution providers*" section of the applicable P2PE Domain.
	3B-1.1.b If the solution provider utilizes any third parties, examine the business agreements and verify the elements delineated in **3C-1.1.a** are present and adequately accounted for.

Requirement 3B: Third-party management	
Domain 3 Requirements	**Testing Procedures**
3B-1.2 For all third parties that have been contracted by the solution provider to manage any of the SCD types used in the P2PE solution, the solution provider must establish formal agreements with the third parties to provide them with the following: • Notification of any changes to POI devices, P2PE applications, P2PE non-payment software, and/or HSMs per PCI SSC's process for *P2PE Designated Changes to Solutions* • Details of the change, including reason • Updated list of POI devices, P2PE applications, P2PE non-payment software, and/or HSMs used in the solution • Evidence of adherence to PCI's process for *P2PE Designated Changes to Solutions*	**3B-1.2** Verify formal agreements established for all third parties managing SCDs on behalf of the solution provider require: • Notification of any changes to POI devices, P2PE applications, P2PE non-payment software, and/or HSMs per PCI SSC's process for *P2PE Designated Changes to Solutions* • Details of the change, including reason • Updated list of POI devices, P2PE applications, P2PE non-payment software, and/or HSMs used in the solution • Evidence of adherence to PCI's process for *P2PE Designated Changes to Solutions*

Requirement 3C: Creation and maintenance of the* P2PE Instruction Manual *for merchants.	
Domain 3 Requirements	**Testing Procedures**
3C-1 Solution provider develops, maintains, and disseminates a *P2PE Instruction Manual* (PIM) to merchants.	
3C-1.1 The PIM must be developed, maintained, distributed to merchants, and provided to merchants upon request. Content for the PIM must be in accordance with the mandatory *PIM Template*.	**3C-1.1.a** Examine the *P2PE Instruction Manual* (PIM) to verify it covers all related instructions, guidance and requirements as specified in the *PIM Template*.
	3C-1.1.b Examine documented procedures to verify mechanisms are defined to distribute the PIM to all merchants using the P2PE solution, and to provide the PIM to merchants upon request.
	3C-1.1.c Interview responsible personnel and observe processes to verify PIM is distributed to all merchants using the P2PE solution and that the PIM is provided to merchants upon request.
	3C-1.1.d Examine the PIM to verify that all devices specified in the PIM are PCI-approved POI devices that were assessed as part of this P2PE solution assessment.
	3C-1.1.e Examine the PIM to verify the following: • All P2PE applications specified in the PIM are assessed for this solution (per Domain 1) • All P2PE applications specified in the PIM are *either* PCI-listed P2PE applications or assessed to Domain 2 as part of this P2PE solution assessment
	3C-1.1.f Examine the PIM to verify that all P2PE non-payment software specified in the PIM were assessed as part of this P2PE solution assessment (per Requirement **1C-2**).
	3C-1.1.g Configure each POI device type, settings, etc. in accordance with all instructions in the PIM and confirm the following: • The PIM provides accurate instructions. • The PIM instructions result in a securely installed P2PE solution.

Requirement 3C: Creation and maintenance of the* P2PE Instruction Manual *for merchants.	
Domain 3 Requirements	**Testing Procedures**
3C-1.2 Review *P2PE Instruction Manual* (PIM) at least annually and upon changes to the solution or the P2PE requirements. Update PIM as needed to keep the documentation current with: • Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and • Any changes to the requirements in this document.	**3C-1.2.a** Examine documented procedures to verify they include: • PIM must be reviewed at least annually and upon changes to the solution or changes to the P2PE requirements • PIM must be updated as needed to keep the document current with: ○ Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and ○ Any changes to the P2PE requirements.
	3C-1.2.b Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify: • PIM is reviewed at least annually and upon changes to the solution or changes to the PCI P2PE requirements • PIM is updated as needed to keep the document current with: ○ Any changes to the P2PE solution (including additions or removals of POI device types, P2PE applications, and/or P2PE non-payment software), and ○ Any changes to the P2PE requirements.
3C-1.2.1 Communicate PIM updates to affected merchants, and provide merchants with an updated PIM as needed.	**3C-1.2.1.a** Examine documented procedures to verify they include communicating PIM updates to affected merchants and providing an updated PIM as needed.
	3C-1.2.1.b Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify PIM updates are communicated to affected merchants and an updated PIM is provided to merchants as needed.

Domain 4: Merchant-Managed Solutions: Separation between Merchant Encryption and Decryption Environments

Domain	Overview	P2PE Validation Requirements
Domain 4: **Merchant-managed Solutions** *Note that this domain is not applicable to third-party solution providers.*	Separate duties and functions between merchant encryption and decryption environments.	**4A** Restrict access between the merchant decryption environment and all other networks/systems. **4B** Restrict traffic between the encryption environment and any other CDE. **4C** Restrict personnel access between the encryption environment and the merchant decryption environment.

Target Audience: *This Domain applies only to merchants that manage their own P2PE solutions*

Overview

Some merchants may choose to manage their own P2PE solution on behalf of their own merchant encryption environments rather than fully outsourcing the solution to a third-party solution provider. This type of P2PE solution is defined as a "*merchant-managed solution*" since the merchant is acting as its own P2PE solution provider. Domain 4 specifies the requirements that must be met for a *merchant-managed solution* with the objective of reducing the presence of clear-text account data within their encryption environments.

Applicability

This domain (Domain 4) is ***only*** applicable to *merchants acting as their own P2PE solution providers*, as defined in this document. This domain is ***not*** applicable to third-party solution providers who manage P2PE solutions on behalf of merchants. *Merchants acting as their own P2PE solution providers* are responsible for ensuring all requirements and domains within this P2PE standard are met, either directly or in conjunction with P2PE component providers.

Merchants may use a service provider(s) or P2PE component providers to perform some P2PE functions. For example, a *merchant acting as its own P2PE solution provider* may choose to outsource POI device management and cryptographic key management to another entity. In this scenario, both the merchant and the third party may be responsible for meeting different P2PE requirements. While P2PE requirements may be met by either the merchant directly or by a third party on the merchant's behalf, the *merchant acting as its own P2PE solution provider* is ultimately responsible for ensuring that all P2PE requirements are met.

If the merchant manages any element of the solution—that is, if any requirement from Domains 1, 2, 5, or 6 is under the merchant's control—then the merchant must meet Domains 3 and 4 to ensure all P2PE requirements are being met (either by the merchant as the solution provider itself or by a P2PE component provider).

See the "P2PE Solutions and use of Third Parties, and/or P2PE Component Providers" section for more information about solution providers, component providers, and merchant as a solution provider.

Note: *If a merchant outsources the decryption environment to a PCI-listed P2PE decryption-management component provider, Domain 4 would not apply for the merchant-managed solution, and use of a PCI-listed component provider would be noted in the merchant-as-a-solution-provider's P2PE Report on Validation (P-ROV). If a merchant outsources the decryption environment to a non-listed decryption service provider, Domain 4 would also not apply and Domain 5 (covering the outsourced decryption services) would be assessed as part of the merchant-as-solution-provider's P2PE assessment and included in the merchant's P-ROV.*

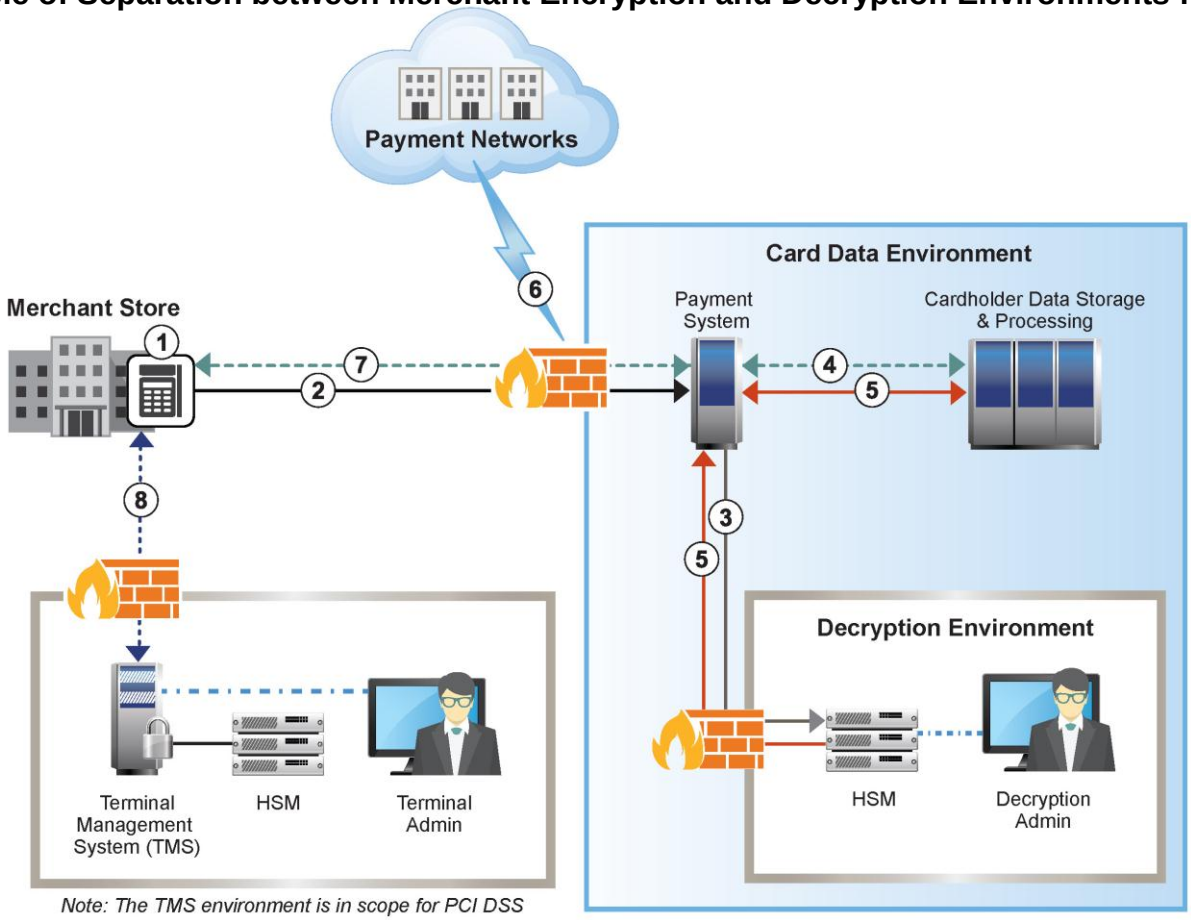
Eligibility Criteria

In a merchant-managed solution, the merchant retains control over the entire solution, from point of capture and encryption at the POI devices in the encryption environment through to the decryption of P2PE transaction data. There is inherently greater risk to the security of the account data when a merchant possesses autonomous control over the P2PE solution without having the separation between the encryption and decryption environments that is naturally included when the solution is delivered by a third-party. Therefore, *merchants acting as their own solution provider* must meet the following additional criteria to be eligible for P2PE solution validation:

- Only use hardware-based decryption as part of the P2PE solution (use of hybrid decryption in a *merchant-managed P2PE solution* is not permitted).
- Satisfy all P2PE domain requirements (Domains 1, 2, 3, 5, and 6) in this standard, including this domain (Domain 4).
- Undergo a full P2PE assessment by a qualified P2PE assessor.

Note: *The PCI SSC does* ***not*** *approve or list merchant-managed solutions on its website.*

At a Glance – Example of Separation between Merchant Encryption and Decryption Environments for Merchant-Managed Solutions



Requirement 4A: Restrict access between the merchant decryption environment and all other networks/systems

Domain 4 Requirements	Testing Procedures
***4A-1** The merchant decryption environment must be dedicated to decryption operations.*	
4A-1.1 Current documentation must be maintained that describes, or illustrates, the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.	**4A-1.1.a** Interview responsible personnel and review documentation to verify that procedures exist for maintaining documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.
	4A-1.1.b Interview responsible personnel and review merchant documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs to verify that the document is kept current.
4A-1.2 Decryption systems must reside on a network that is dedicated to decryption operations. ***Note:** The decryption environment must exist within a cardholder data environment (CDE).*	**4A-1.2.a** Examine network diagram(s) to verify that decryption systems are located on a network that is dedicated to decryption operations.
	4A-1.2.b Inspect network and system configurations to verify that decryption systems are located on a network that is dedicated to decryption operations.
4A-1.3 Systems in the decryption environment must be dedicated to performing and/or supporting decryption and key-management operations: • Services, protocols, daemons, etc. necessary for performing and/or supporting decryption operations must be documented and justified. • Functions not required for performing or supporting decryption operations must be disabled or isolated (e.g., using logical partitions) from decryption operations. ***Note:** Security functions (e.g., logging and monitoring controls) are examples of functions supporting decryption operations. It is not required that supporting functions be present in the merchant decryption environment; these functions may be resident in the CDE. However, any supporting functions that are present in the decryption environment must be wholly dedicated to the decryption environment.*	**4A-1.3.a** Inspect network and system configuration settings to verify that only necessary services, protocols, daemons, etc. are enabled, and any functions not required for performing or supporting decryption operations are disabled or isolated from decryption operations.
	4A-1.3.b Review the documented record of services, protocols, daemons etc. that are required by the decryption systems and verify that each service includes justification.

Requirement 4A: Restrict access between the merchant decryption environment and all other networks/systems

Domain 4 Requirements	Testing Procedures
4A-1.4 Systems providing logical authentication services to system components within the decryption environment must: • Reside within the decryption environment • Be dedicated to supporting the decryption environment. ***Note:*** *Logical authentication services may be internal to the HSM management system.*	**4A-1.4.a** Examine documented policies and procedures, and interview responsible personnel to verify that systems providing logical authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.
	4A-1.4.b Review system configurations and observe processes to verify that systems providing authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.
4A-1.5 Logical administrative/privileged access to systems within the decryption environment must be authorized and must originate from within the merchant decryption environment.	**4A-1.5.a** Examine documented policies and procedures, and interview responsible personnel to verify that logical administrative/privileged access to the systems within the decryption environment must be authorized and originate from within the merchant decryption environment.
	4A-1.5.b Examine firewall/router configurations to verify that logical administrative/privileged access to systems within the decryption environment is authorized and originates from within the merchant decryption environment.
4A-1.6 All remote access features on all systems in the merchant decryption environment must be permanently disabled and/or otherwise prevented from being used	**4A-1.6** Review system configurations and observe processes to verify that all remote access features on all systems within the merchant decryption environment are permanently disabled and/or otherwise prevented from being used.
4A-1.7 Systems in the merchant decryption environment must not store account data.	**4A-1.7.a** Review configurations of all devices and systems in the merchant decryption environment to confirm none of the systems store account data.
	4A-1.7.b Review data flows and interview personnel to verify that account data is not stored in the merchant decryption environment.
4A-2 *Restrict access between the merchant decryption environment and all other networks/systems.*	
4A-2.1 Firewalls must be in place to restrict connections between the merchant decryption environment and all other networks. Firewalls must be configured to restrict traffic as follows:	**4A-2.1** Review documentation and observe network configurations to verify that firewalls are in place between the merchant decryption environment and all other networks.
4A-2.1.1 Inbound and outbound traffic to/from the decryption environment must be restricted to only IP addresses within the CDE.	**4A-2.1.1** Examine firewall and router configurations to verify that inbound and outbound traffic to/from the decryption environment is limited to only IP addresses within the CDE.

Requirement 4A: Restrict access between the merchant decryption environment and all other networks/systems	
Domain 4 Requirements	**Testing Procedures**
4A-2.1.2 Inbound and outbound traffic between the decryption environment and any CDE must be restricted to only that which is necessary for performing and/or supporting decryption operations, with all other traffic specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).	**4A-2.1.2.a** Review firewall configuration standards to verify that inbound and outbound traffic necessary for performing and/or supporting decryption operations is identified and documented.
	4A-2.1.2.b Examine firewall configurations to verify that inbound and outbound traffic between the decryption environment and any CDE is limited to only that which is necessary for performing and/or supporting decryption operations, and all other traffic is specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).
4A-2.2 Inbound and outbound traffic between the merchant CDE and the encryption environment must be restricted to approved POI devices located within the encryption environment.	**4A-2.2** Examine network and system configurations to verify that inbound and outbound traffic between the merchant CDE and the encryption environment is restricted to approved POI devices located within the encryption environment.
4A-2.3 Processes must be implemented to prevent unauthorized physical connections (e.g., wireless access) to the decryption environment as follows: • Wireless connections to the decryption environment are prohibited. • Processes are implemented to detect and immediately (as soon as possible) respond to physical connections (e.g., wireless connections) to the decryption environment.	**4A-2.3.a** Review document policies and procedures to verify that wireless connections to the decryption environment are prohibited**.**
	4A-2.3.b Observe processes and interview personnel to verify a methodology is implemented to immediately (e.g., ASAP) detect, identify, and eliminate any unauthorized physical connections (e.g., wireless access points) that connect to the decryption environment.
	4A-2.3.c Examine firewall/router configurations to confirm that all wireless networks are prevented from connecting to the decryption environment.

Requirement 4B: Restrict traffic between the encryption environment and any other CDE.	
Domain 4 Requirements	**Testing Procedures**
***4B-1** Traffic between the encryption environment and any other CDE is restricted*	
4B-1.1 Traffic between the encryption environment and any other CDE must be limited as follows: • Only those systems (e.g., POI devices) directly related to supporting P2PE transactions, and • Only traffic that is necessary for transaction processing and/or terminal management purposes All other traffic between the encryption environment and any other CDE must be specifically denied.	**4B-1.1.a** Review documentation to verify that inbound and outbound traffic necessary for transaction processing and/or terminal management purposes is identified and documented.
	4B-1.1.b Examine firewall configurations to verify that any traffic between the encryption environment and any other CDE is limited as follows: • Only those systems (e.g., POI devices) directly related to supporting P2PE transactions, and • Only traffic that is necessary for transaction processing and/or terminal management purposes Verify all other traffic between those two networks is specifically denied (e.g., by using an explicit "deny all" or an implicit deny after an allow statement).
	4B-1.1.c Observe traffic between the encryption environment and any other CDE to verify the traffic is limited to systems directly related to supporting P2PE transactions, transaction processing, and/or terminal-management functions.
4B-1.2 Processes must be implemented to prevent clear-text account data from being transmitted from the CDE back to the encryption environment.	**4B-1.2.a** Review documented policies and procedures for the CDE to verify that the transmission of clear-text account data from the CDE back to the encryption environment is prohibited.
	4B-1.2.b Observe processes and interview personnel to verify clear-text account data is prevented from being transmitted from the CDE back to the encryption environment.
	4B-1.2.c Using forensic techniques, observe traffic between the encryption environment and the CDE to verify clear-text account data is not transmitted from the CDE back to the encryption environment.

Requirement 4C: Restrict personnel access between encryption environment and decryption environment.

Domain 4 Requirements	Testing Procedures
4C-1 *Merchant in-store (encryption environment) personnel do not have logical access to the decryption environment, any CDEs, or account-data decryption keys.*	
4C-1.1 Separation of duties must exist such that encryption environment personnel are prohibited from accessing any system components in the decryption environment or any CDE. Access control mechanisms must include both physical and logical controls. *Note: Access restrictions between the encryption and decryption environment are not intended to prohibit employees who work in the decryption environment or CDE from shopping in the stores. This requirement is focused on logical access controls, not physical.*	**4C-1.1.a** Examine documented policies and procedures, and interview responsible personnel to verify that encryption environment personnel are prohibited from accessing any system components in the decryption environment or the CDE.
	4C-1.1.b For a sample of system components in the CDE and the decryption environment, review system configurations and access control lists to verify that encryption environment personnel do not have access to any system components in the decryption environment or the CDE.

Domain 5: Decryption Environment

Domain	Overview	P2PE Validation Requirements
Domain 5: **Decryption Environment**	The secure management of the environment that receives encrypted account data and decrypts it.	**5A** Use approved decryption devices. **5B** Secure the decryption environment. **5C** Monitor the decryption environment and respond to incidents. **5D** Implement secure, hybrid decryption processes. **5E** Component providers *ONLY*: report status to solution providers

Target Audience: *P2PE solution providers, or those who, on behalf of P2PE solution providers, manage the P2PE decryption environment.*

Overview

Within a P2PE solution, the decryption environment is where incoming encrypted account data is decrypted back to its original clear-text. This environment therefore consists of the secure cryptographic devices (and a Host System for hybrid environments) and cryptographic keys involved in the account-data decryption process. Requirements in Domain 5 entail securing all decryption systems and associated cryptographic keys, along with implementing monitoring and response procedures.

See the "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" section for more information about validating this Domain as a solution provider, a decryption-environment component provider, or as a merchant as a solution provider.

Note for hybrid decryption environments:

Hybrid decryption environments require HSMs for cryptographic key-management functions but allow for non-SCD Host Systems to be used for account data decryption. Unlike a P2PE solution with a hardware decryption environment (in which cryptographic key management and account-data decryption are performed entirely within a hardware security module, or HSM), a hybrid decryption environment (which requires HSMs for cryptographic key-management functions) allows for the decryption of account data outside of an HSM in non-SCDs on a Host System. These environments must meet all requirements specified in Domains 5 and 6, including the additional requirements specified in Section **5D** (as well as those specified in Domain 6 in section **6H**).

Note: *References to "devices" within this section are always to be interpreted as referencing decryption devices, such as HSMs, unless specifically noted. For hybrid decryption environments, references to "**decryption devices and systems"** within this section are always to be interpreted as referencing HSMs and the Host System, unless specifically noted. This section is not intended to include requirements to be assessed against encrypting devices, such as POI devices.*

Note: *All decryption devices, including HSMs and related key-management SCDs, must additionally meet all requirements specified in Domain 6.*

Note: *For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 5, and 6 of this document refers to merchant personnel in the encryption environments, and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.*

A Host System is defined as a combination of software and hardware components used for the purpose of decrypting account data, may also be used for transaction processing, and is not considered an SCD.

Requirement 5A: Use approved decryption devices

Domain 5 Requirements	Testing Procedures
***5A-1** Use approved decryption devices*	
5A-1.1 All hardware security modules (HSMs) must be either: • FIPS140-2 Level 3 (overall) or higher certified, or • PCI PTS HSM approved.	**5A-1.1.a** For all HSMs used in the decryption environment, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs used in the solution are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3 (overall), or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid PCI SSC listing number, as Approved PCI PTS Devices under the approval class "HSM."
	5A-1.1.b Examine documented procedures and interview personnel to verify that all account-data decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified in **5A-1.1.a.**
5A-1.1.1 The approval listing must match the deployed devices in the following characteristics: • Vendor name • Model name and number • Hardware version number • Device firmware version number • For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment *(continued on next page)*	**5A-1.1.1.a** For all PCI-approved HSMs used in the solution, examine HSM devices and review the *PCI SSC list of Approved PTS Devices* to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Device firmware version number • Any applications, including application version number, resident within the device which were included in the PTS assessment

Requirement 5A: Use approved decryption devices

Domain 5 Requirements	Testing Procedures
5A-1.1.1 (continued) ***Note:*** *If the solution provider has applied a vendor security patch resulting in an updated HSM firmware version, and the PCI SSC or NIST validation of that updated firmware version has not yet been completed (resulting in a mismatch between the HSM firmware version in use and the listed, validated one), the solution provider must obtain documentation from the vendor regarding the update that includes confirmation the update has been submitted for evaluation per the process specified by either PCI SSC or NIST (as applicable to the HSM).*	**5A-1.1.1.b** For all FIPS-approved HSMs used in the solution, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number
	5A-1.1.1.c If the solution provider has applied a vendor security patch that resulted in an updated HSM firmware version, and the PCI SSC or NIST validation of that updated firmware version has not yet been completed, obtain the vendor documentation and verify it includes confirmation that the update has been submitted for evaluation per the process specified by PCI SSC or NIST (as applicable to the HSM).
5A-1.1.2 If FIPS-approved HSMs are used, the HSM must use the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account data decryption and related processes.	**5A-1.1.2.a** Examine FIPS approval documentation (security policy) and HSM operational procedures to verify that the FIPS approval covers the cryptographic primitives, data-protection mechanisms, and key-management used for account data decryption and related processes.
Note: *Solution providers operating HSMs in non-FIPS mode or adding non-FIPS validated software must complete a written confirmation that includes the following:* • *Description of why the HSM is operated in non-FIPS mode* • *Purpose and description of any non-FIPS validated software added to the HSM* • *A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements* *Note that adding any software may invalidate the FIPS approval.*	**5A-1.1.2.b** If the HSM is operated in non-FIPS mode or non-FIPS validated software has been added to the HSM, review the solution provider's written confirmation and confirm that it includes the following: • Description of why the HSM is operated in non-FIPS mode • Purpose and description of any non-FIPs validated software added to the HSM • A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements.

Requirement 5A: Use approved decryption devices

Domain 5 Requirements	Testing Procedures
5A-1.1.3 If PCI PTS-approved HSMs are used, the HSM must be configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all P2PE operations (including algorithms, data protection, key management, etc.). ***Note:*** *PCI HSMs require that the decryption-device manufacturer make available a security policy document to end users, providing information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.*	**5A-1.1.3** Examine HSM configurations for all P2PE solution functions to verify that HSMs are configured to operate according to the security policy that was included as part of the PTS approval.

Requirement 5B: Secure the decryption environment.	
Domain 5 Requirements	**Testing Procedures**
***5B-1** Maintain processes for securely managing the decryption environment.*	
5B-1.1 Current documentation must be maintained that describes or illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.	**5B-1.1.a** Interview responsible personnel and review documentation to verify that a procedure exists to maintain a document that describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.
	5B-1.1.b Interview responsible personnel and review solution-provider documentation that describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.
	5B-1.1.c Review the solution-provider documentation that describes/illustrates the configuration of the of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.
5B-1.2 Procedures must be implemented to provide secure administration of decryption devices by authorized personnel, including but not limited to: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of user interface • Password/smart card management • Console and non-console administration • Access to physical keys • Use of HSM commands	**5B-1.2.a** Examine documented procedures to verify secure administration by authorized personnel is defined for decryption devices including: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands
	5B-1.2.b Observe authorized personnel performing device-administration operations to verify secure administration procedures are implemented for the following: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands

Requirement 5B: Secure the decryption environment.	
Domain 5 Requirements	**Testing Procedures**
	5B-1.2.c Observe personnel performing decryption-device administration and examine files/records that assign administrative roles and responsibilities to verify that only authorized and assigned personnel perform decryption-device administration operations.
5B-1.3 Only authorized users/processes have the ability to make function calls to the HSM—e.g., via the HSM's application program interfaces (APIs). *For example, require authentication for use of the HSMs APIs and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate use of the API, limit the exposure of the HSM to a trusted host via a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (e.g., high-speed serial or dedicated Ethernet).*	**5B-1.3.a** Examine documented procedures and processes to verify that only authorized users/processes have the ability to make functions calls to the HSM—e.g., via the HSM's application program interfaces (APIs).
	5B-1.3.b Interview responsible personnel and observe HSM system configurations and processes to verify that only authorized users/processes have the ability to make function calls to the HSM (e.g., via the HSM's application program interfaces (APIs)).
5B-1.4 POI devices must be authenticated upon connection to the decryption environment and upon request by the solution provider. ***Note:*** *This authentication can occur via use of cryptographic keys or certificates, uniquely associated with each POI device and decryption system.*	**5B-1.4.a** Examine documented policies and procedures to verify they require POI devices be authenticated upon connection to the decryption environment and upon request by the solution provider.
	5B-1.4.b Verify documented procedures are defined for the following: • Procedures and/or mechanisms for authenticating POI devices upon connection to the decryption environment • Procedures and/or mechanisms for authenticating POI devices upon request by the solution provider
	5B-1.4.c Interview responsible personnel and observe a sample of device authentications to verify the following: • POI devices are authenticated upon connection to the decryption environment. • POI devices are authenticated upon request by the solution provider.

Requirement 5B: Secure the decryption environment.

Domain 5 Requirements	Testing Procedures
5B-1.5 Physical inspections of decryption devices by authorized personnel must be performed at least quarterly to detect tampering or modification of devices. Inspections to include: • The device itself • Cabling/connection points • Physically connected devices	**5B-1.5.a** Examine documented procedure to verify that physical inspection of devices is required at least quarterly to detect signs of tampering or modification, and that inspection procedures include: • The device itself • Cabling/connection points • Physically connected devices
	5B-1.5.b Interview personnel performing physical inspections and observe inspection processes to verify that inspections include: • The device itself • Cabling/connection points • Physically connected devices
	5B-1.5.c Interview personnel performing inspections and review supporting documentation to verify that physical inspections are performed at least quarterly.
5B-1.6 Decryption environment must be secured according to PCI DSS. ***Note:*** *For merchant-managed solutions, PCI DSS validation of the decryption environment is managed by the merchant in accordance with their acquirer and/or payment brand. This requirement is therefore not applicable to P2PE assessments where merchants are the P2PE solution provider.* ***Note:*** *The QSA (P2PE) should NOT challenge or re-evaluate the PCI DSS environment (or its compliance) where a completed and current ROC exists.*	**5B-1.6.a** Review the "Description of Scope of Work and Approach Taken" section of the solution provider's current PCI DSS Report on Compliance (ROC) to verify the PCI DSS assessment scope fully covers the P2PE decryption environment.
	5B-1.6.b Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that all applicable PCI DSS requirements are "in place" for the P2PE decryption environment.
	5B-1.6.c Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that the PCI DSS assessment of the P2PE decryption environment was: • Performed by a QSA • Performed within the previous 12 months
5B-1.7 Processes are implemented to ensure that clear-text account data is never sent back to the encryption environment. ***Note:*** *Output of clear-text data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process when it occurs from the decryption environment is assessed at Requirement* ***5B-1.9***	**5B-1.7.a** Review documented processes and interview personnel to confirm that clear-text account data is never sent back to the encryption environment.
	5B-1.7.b Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends clear-text account data back into the encryption environment.

Requirement 5B: Secure the decryption environment.

Domain 5 Requirements	Testing Procedures
5B-1.8 Any truncated PANs sent back to the encryption environment must adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs that specify allowable digits.	**5B-1.8.a** Review documented processes and interview personnel to confirm that any truncated PANs sent back to the encryption environment adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs
	5B-1.8.b Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends more digits of truncated PANs back to the encryption environment than is specified in PCI DSS and/or related FAQs.

5B-1.9 Any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must ensure that the *ONLY* allowed output of clear-text account data is for non-PCI payment brand account/card data, and includes the following:
• Cryptographic signing (or similar) prior to installation by authorized personnel using dual control.
• Cryptographic authentication by the HSM
• Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.
• Approval of functionality by authorized personnel prior to implementation
• Documentation for all new installations or updates to whitelist functionality that includes the following:
  ○ Description and justification for the functionality
  ○ Who approved the new installation or updated functionality prior to release
  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data
	5B-1.9 Review documented policies and procedures to verify that that any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* ensures the that the *ONLY* allowed output of clear-text account data is for non-PCI payment brand account/card data, and includes the following:
	• Cryptographic signing (or similar) prior to installation by authorized personnel using dual control.
	• Cryptographic authentication by the HSM
	• Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.
	• Approval of functionality by authorized personnel prior to implementation
	• Documentation for all new installations or updates to whitelist functionality that includes the following:
	  ○ Description and justification for the functionality
	  ○ Who approved the new installation or updated functionality prior to release
	  ○ Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data

Requirement 5B: Secure the decryption environment.

Domain 5 Requirements	Testing Procedures
5B-1.9.1 Any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must allow *ONLY* the output of clear-text account data for non-PCI payment brand account/card data.	**5B-1.9.1.a** Observe application and system configurations and interview personnel to verify that whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* only allows the output of clear-text account data for non-PCI payment brand account/card data.
	5B-1.9.1.b Perform test transactions to verify that any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* only allows output clear-text account for non-PCI payment brand account/card data.
5B-1.9.2 Any new installations of, or updates to, whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must be: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM	**5B-1.9.2** Observe the process for new installations or updates to whitelisting functionality and interview personnel to verify that additions or updates to whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* are performed as follows: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM
5B-1.9.3 Any new installations of, or updates to, whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must follow change-control procedures that include: • Coverage for both new installations and updates to such functionality • Description and justification for the functionality • Who approved the new installation or update prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.	**5B-1.9.3** Review records of both new and updated whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment*, and confirm the following: • Both new installations and updates to whitelisting functionality are documented. • The documentation includes description and justification. • The documentation includes who approved it prior to implementation. • The documentation includes confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.

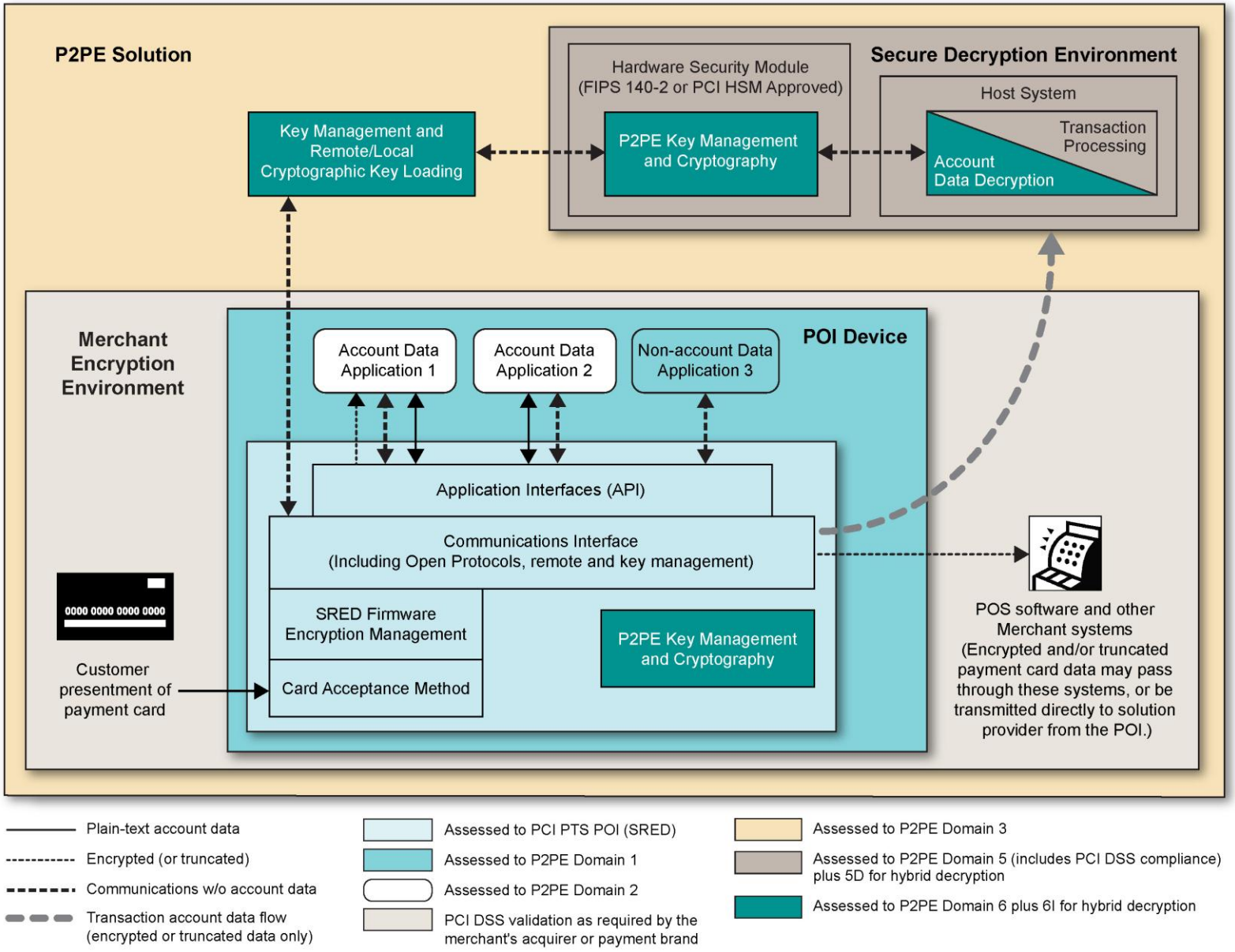
Requirement 5C: Monitor the decryption environment and respond to incidents.	
Domain 5 Requirements	**Testing Procedures**
5C-1 *Perform logging and monitor the decryption environment for suspicious activity, and implement notification processes.*	
5C-1.1 Changes to the critical functions of the decryption devices must be logged. ***Note:*** *Critical functions include but are not limited to application and firmware updates, key-injection, as well as changes to security-sensitive configurations.*	**5C-1.1** Examine system configurations and correlating log files to verify that any changes to the critical functions of decryption devices are logged, including: • Changes to the applications • Changes to the firmware • Changes to any security-sensitive configurations
5C-1.2 Mechanisms must be implemented to detect and respond to suspicious activity, including but not limited to: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API	**5C-1.2.a** Examine documented procedures to verify mechanisms are defined to detect and respond to potential security incidents, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API
	5C-1.2.b Interview personnel and observe implemented mechanisms to verify mechanisms are implemented to detect and respond to suspicious activity, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (configuration, access controls) • Unauthorized use of sensitive functions (e.g., key management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API

Requirement 5C: Monitor the decryption environment and respond to incidents.	
Domain 5 Requirements	**Testing Procedures**
5C-1.3 Mechanisms must be implemented to detect encryption failures, including at least the following: ***Note:*** *Although Domain 5 is concerned with the decryption environment, not the encryption environment, all traffic received into the decryption environment must be actively monitored to confirm that the POI devices in the merchant's encryption environment is not outputting clear-text account data through some error or misconfiguration.*	**5C-1.3** Examine documented procedures to verify controls are defined for the following: • Procedures are defined to detect encryption failures, and include **5C-1.3.1** through **5C-1.3.4** below. • Procedures include immediate notification upon detection of a cryptographic failure, for each **5C-1.3.1** through **5C-1.3.4** below.
5C-1.3.1 Checking for incoming clear-text account data.	**5C-1.3.1.a** Observe implemented processes to verify controls are in place to check for incoming clear-text account data.
	5C-1.3.1.b Observe implemented controls and notification mechanisms to verify mechanisms detect and provide immediate notification upon detection of incoming clear-text account data.
	5C-1.3.1.c Interview personnel to verify that designated personnel are immediately notified upon detection of incoming clear-text account data.
5C-1.3.2 Detecting and reviewing any cryptographic errors reported by the HSM	**5C-1.3.2.a** Observe implemented processes to verify controls are in place to detect and review any cryptographic errors reported by the HSM.
	5C-1.3.2.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification of cryptographic errors reported by the HSM.
	5C-1.3.2.c Interview personnel to verify that designated personnel are immediately notified upon detection of cryptographic errors reported by the HSM.
5C-1.3.3 Detecting and reviewing any unexpected transaction data received. *For example, transaction data received without an expected authentication data block (such as a MAC or signature, or a malformed message).*	**5C-1.3.3.a** Observe implemented processes to verify controls are in place to detect and review any unexpected transaction data received.
	5C-1.3.3.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification for any unexpected transaction data received.
	5C-1.3.3.c Interview personnel to verify that designated personnel are immediately notified upon detection of any unexpected transaction data received.

Requirement 5C: Monitor the decryption environment and respond to incidents.	
Domain 5 Requirements	**Testing Procedures**
5C-1.3.4 Reviewing data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.	**5C-1.3.4.a** Observe implemented processes to verify controls are in place to review data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.
	5C-1.3.4.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification upon detection of POI devices that are causing an unusually high rate of transaction authorization rejections.
	5C-1.3.4.c Interview personnel to verify that designated personnel are immediately notified upon detection of POI devices that are causing an unusually high rate of transaction authorization rejections.
5C-1.4 All suspicious activity must be identified and a record maintained, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during any identified time that encryption was malfunctioning or disabled	**5C-1.4.a** Examine documented procedures to verify they include procedures for identifying the source and maintaining a record, of all suspicious activity, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled
	5C-1.4.b Observe implemented controls and interview responsible personnel to verify that the source of any suspicious activity is identified, and records are maintained to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled

Requirement 5C: Monitor the decryption environment and respond to incidents.	
Domain 5 Requirements	**Testing Procedures**
5C-1.5 Implement mechanisms to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).	**5C-1.5.a** Examine documented procedures to verify mechanisms are defined to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).
	5C-1.5.b Interview personnel and observe implemented mechanisms to verify that immediate notification of suspicious activity is provided to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).

At a Glance – Example P2PE Hybrid Decryption Implementation



Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
***5D-1** Configure the Host System securely.*	
5D-1.1 The solution provider must maintain current documentation that describes, or illustrates, the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.	**5D-1.1.a** Interview responsible personnel and review documentation to verify that a procedure exists to maintain a document that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.
	5D-1.1.b Interview responsible personnel and review solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems within that environment, to verify that the document is current.
	5D-1.1.c Review the solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems, to verify that it accurately represents the decryption environment.
5D-1.2 The Host System must be isolated, or dedicated, to transaction processing, with only necessary services, protocols, daemons etc. enabled: • The necessary services, protocols, daemons etc. must be documented and justified, including description of the enabled security features for these services etc. • Functions not related to transaction processing must be disabled, or isolated (e.g., using logical partitions), from transaction processing. ***Note:** "Isolated" means that the Host System must not be accessed, modified or intercepted by other processes.*	**5D-1.2.a** Inspect network and system configuration settings to verify the host processing system is isolated, or dedicated, to transaction processing, with only necessary services, protocols, daemons etc. enabled.
	5D-1.2.b Review the documented record of services, protocols, daemons etc. that are required by the Host System and verify that each service includes justification and a description of the enabled security feature.
5D-1.3 The Host System and HSM must reside on a network that is dedicated to decryption operations and transaction processing and must be segmented from any other network, or system, that is not performing or supporting decryption operations or transaction processing.	**5D-1.3.a** Examine network diagram(s) to verify the Host System(s) and HSM(s) are located on a network that is segmented from other networks that are not required for decryption operations or transaction processing.
	5D-1.3.b Inspect network and system configurations to verify the Host System(s) and HSM(s) are located on a network that is segmented from other networks not required for decryption operations or transaction processing.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-1.4 All application software installed on the Host System must be authorized and have a business justification.	**5D-1.4.a** Examine documented policies and procedures to verify that all application software installed on the Host System must have a business justification and be duly authorized.
	5D-1.4.b Examine change control and system configuration records to verify that all application software installed on the Host System is authorized.
	5D-1.4.c Inspect Host System and compare with system configuration standards to verify that all software installed on the Host System has a defined business justification.
5D-1.5 A process, either automated or manual, must be in place to prevent and/or detect and alert, any unauthorized changes to applications/software on the Host System.	**5D-1.5.a** Examine documented policies and procedures to verify that a process is defined to prevent and/or detect and alert, any unauthorized changes to applications/software.
	5D-1.5.b Interview personnel and observe system configurations to verify that controls are implemented to prevent and/or detect and alert personnel, upon any unauthorized changes to applications/software.
	5D-1.5.c Examine output from the implemented process to verify that any unauthorized changes to applications/software are either prevented or detected with an alert generated that is immediately investigated.
5D-1.6 The Host System must perform a self-test when it is powered up to ensure its integrity before use. The self-test must include: • Testing integrity of cryptographic functions. • Testing integrity of firmware. • Testing integrity of any security functions critical to the secure operation of the Host System.	**5D-1.6.a** Inspect Host System configuration settings, and examine vendor/solution provider documentation to verify that the Host System performs a self-test when it is powered up to ensure its integrity before use. Verify the self-test includes the following: • Testing integrity of cryptographic functions. • Testing integrity of software/firmware. • Testing integrity of any security functions critical to the secure operation of the Host System.
	5D-1.6.b Review logs/audit trails from when the Host System has previously been powered-up and interview personnel, to verify that the Host System performs a self-test to ensure its integrity before use. Verify the self-tests included the tests described in **5D-1.6.a**.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-1.7 The Host System must perform a self-test when a security-impacting function or operation is modified (e.g., an integrity check of the software/firmware must be performed upon loading of a software/firmware update).	**5D-1.7.a** Inspect Host System configuration settings and examine vendor/solution provider documentation to verify that the Host system performs a self-test when a security-impacting function or operation is modified.
	5D-1.7.b Interview personnel and examine logs/records for when a security-impacting function, or operation, has been modified to verify that the Host System performs a self-test.
5D-1.8 The Host System must enter an error state and generate an alert upon any of the following events: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **5D-1.6** and **5D-1.7** • Failure of a security function or mechanism ***Note:*** *An "error state" identifies the Host System has encountered an issue that requires a response action. To prevent potential damage or compromise, the system must cease cryptographic operations until the issue is resolved and the host is returned to a normal processing state.*	**5D-1.8.a** Inspect Host System configuration settings and examine vendor/solution provider documentation to verify that the host enters an error state and generates an alert in the event of the following: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **5D-1.6** and **5D-1.7** • Failure of a security function or mechanism
	5D-1.8.b Interview personnel and examine logs/records of actual or test alerts to verify that alerts are generated and received when the Host System enters an error state under one of the following conditions: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **5D-1.6** and **5D-1.7** • Failure of a security function or mechanism
5D-1.9 Alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.	**5D-1.9.a** Review documented procedures to verify alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.
	5D-1.9.b Examine system configurations and records of documented alert events to verify alerts generated from the Host System are documented.
	5D-1.9.c Examine a sample of documented alert events and interview personnel assigned with security-response duties to verify alerts initiate a response procedure.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-1.10 The Host System must not perform any cryptographic operations under any of the following conditions: • While in an error state, as described in Requirement **5D-1.8** • During self-tests, as described in Requirements **5D-1.6** and **5D-1.7** • During diagnostics of cryptographic operations.	**5D-1.10.a** Examine documented procedures to verify that controls/processes are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement **5D-1.8** • During self-tests, as described in Requirements **5D-1.6** and **5D-1.7**. • During diagnostics of cryptographic operations.
	5D-1.10.b Inspect Host System configuration settings and interview personnel to verify that controls and/or procedures are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement **5D-1.8** • During self-tests, as described in Requirements **5D-1.6** and **5D-1.7**. • During diagnostics of cryptographic operations.
5D-1.11 All source code and executable code for cryptographic software and firmware on the Host System must be protected from unauthorized disclosure and unauthorized modification.	**5D-1.11.a** Inspect configuration documentation to verify that access controls are defined to ensure all source code and executable code for cryptographic software and firmware is protected from unauthorized disclosure and unauthorized modification.
	5D-1.11.b Observe access controls for cryptographic software and firmware to verify that all source code and executable code is protected from unauthorized disclosure and unauthorized modification.
5D-1.12 The clear-text data-decryption keys must not be accessible to any processes or functions not directly required for decryption operations.	**5D-1.12.a** Review solution provider documentation, including data flow diagrams, to verify that clear-text decryption keys are not accessible to any processes or functions not directly required for decryption operations.
	5D-1.12.b Inspect Host System configurations and access controls and to verify that clear-text decryption keys are not accessible to any processes or functions not directly required for decryption operations.
5D-1.13 The clear-text data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys	**5D-1.13.a** Examine documented key-management policies and procedures to verify clear-text data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys.
	5D-1.13.b Inspect Host System configuration settings and verify that clear-text data-decryption keys are only accessible to authorized personnel with a defined job-related need to access the keys.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-1.14 The Host System must not write clear-text cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory 'swap/page' file purposes. • 'Core dumps' of memory required for troubleshooting. In the above circumstances, the following conditions apply:	**5D-1.14.a** Examine documented configuration procedures to verify that the Host System must not write clear-text cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory 'swap/page' file purposes. • Core dumps' of memory required for trouble-shooting.
	5D-1.14.b Examine Host System configuration settings and interview personnel to verify that clear-text cryptographic keys are not written to persistent storage except in the following circumstances: • Memory 'swap/page' file purposes. • 'Core dumps' of memory required for trouble-shooting.
	5D-1.14.c Verify documented procedures include Requirements **5D-1.14.1** through **5D-1.14.5** below.
5D-1.14.1 The locations must be predefined and documented.	**5D-1.14.1.a** Review Host System configuration standards to verify that storage locations of any 'swap/page' files and 'core dumps' are defined.
	5D-1.14.1.b Examine Host System configuration settings to verify that the Host System only outputs 'swap/page' files and 'core dumps' to the documented storage locations.
5D-1.14.2 Storage can only be made to a dedicated hard drive (on its own bus) within the host.	**5D-1.14.2** Examine Host System configuration settings and storage locations to verify that 'swap/page' files and 'core dumps' are written to a dedicated hard drive on its own bus on the Host System.
5D-1.14.3 The swap/page files and/or core dumps must never be backed up or copied.	**5D-1.14.3.a** Examine backup configuration settings for the Host System and storage locations to verify that 'swap/page' files and 'core dumps' are not backed up.
	5D-1.14.3.b Examine configurations of storage locations to verify that 'swap/page' files and 'core dumps' cannot be copied off the storage locations.
5D-1.14.4 Access to, and the use of, any tools used for trouble-shooting or forensics must be strictly controlled.	**5D-1.14.4.a** Examine documented procedures to verify that controls are defined to ensure that the access to, and use of, any tools used for trouble-shooting or forensics, are strictly controlled.
	5D-1.14.4.b Observe the process for accessing the tools used for trouble-shooting or forensics, and verify that they are strictly controlled in accordance with the documented procedure.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
	5D-1.14.4.c Observe the process for using the tools used for trouble-shooting or forensics, and verify that they are strictly controlled in accordance with the documented procedure.
5D-1.14.5 All files must be securely deleted in accordance with industry-accepted standards for secure deletion of data: • Core dumps must be securely deleted immediately after analysis. • Memory 'swap/page' files must be securely deleted upon system shut down or reset.	**5D-1.14.5.a** Review documented procedures to verify that it defines a process for securely deleting 'swap/page' files and 'core dumps' at the required times: • Core dumps must be securely deleted immediately after analysis. • Memory 'swap/page' files must be securely deleted upon system shut down or reset.
	5D-1.14.5.b Verify, through the use of forensic tools and/or methods, that the secure procedure removes 'swap/page' files and 'core dumps', in accordance with industry-accepted standards for secure deletion of data.
***5D-2** Access controls for the Host System are configured securely.*	
5D-2.1 Host user passwords must be changed at least every 30 days. ***Note:** This requirement applies to all user roles associated to persons with access to the Host System.*	**5D-2.1.a** Examine documented policies and procedures to verify that the Host System (s) user passwords must be changed at least every 30 days.
	5D-2.1.b Inspect Host System configuration settings to verify that user password parameters are set to require users to change passwords at least every 30 days.
5D-2.2 User passwords must meet the following: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.	**5D-2.2.a** Examine documented policies and procedures to verify that user passwords must: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.
	5D-2.2.b Inspect Host System (s) configuration settings to verify that user passwords: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-2.3 Where log-on security tokens (e.g., smart cards) are used to access the Host System, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage. The PIN or password/passphrase must be at least ten alphanumeric characters in length, or equivalent.	**5D-2.3.a** If log-on security tokens are used, observe the security tokens in use to verify that they have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage.
	5D-2.3.b Examine token-configuration settings to verify parameters are set to require that PINs or password/passphrases be at least ten alphanumeric characters in length, or equivalent.
5D-2.4 User accounts must be locked out of the Host System after not more than five failed attempts.	**5D-2.4.a** Examine documented policies and procedures to verify that authentication parameters on the Host System must be set to require that a user's account be locked out after not more than five invalid logon attempts.
	5D-2.4.b Inspect Host System configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon attempts.
5D-2.5 The Host System must enforce role-based access control to include, at a minimum, the following roles: • Host System operator role – for day-to-day non-sensitive operations of the Host System. • Host System administrator role – configuration of host OS, security controls, software and user accounts. • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions	**5D-2.5.a** Examine documented access-control procedures to verify they define, as a minimum, the following roles: • Host System operator role – for day-to-day non-sensitive operations of the Host System. • Host System administrator role – configuration of host OS, security controls, software and user accounts. • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions
	5D-2.5.b Inspect the Host System configuration settings to verify that role-based access control is enforced and, at a minimum, the following roles are defined: • Host System operator role – for day-to-day non-sensitive operations of the Host System. • Host System administrator role – configuration of host OS, security controls, software and user accounts. • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
	5D-2.5.c Interview a sample of users for each role to verify the assigned role is appropriate for their job function.
5D-2.6 The segregation of duties must be enforced between roles, through automated or manual processes, to ensure that no one person is able to control end-to-end processes; or be in a position to compromise the security of the Host System. The following conditions must be applied:	
5D-2.6.1 A Host System user must not be permitted to audit their own activity on the Host System.	**5D-2.6.1.a** Examine documented procedures to verify that a Host System user is not permitted to audit their own activity on the Host System.
	5D-2.6.1.b Interview audit personnel to verify that a Host System user is not permitted to audit their own activity on the Host System.
5D-2.6.2 A Host System administrator must use their operator-level account when performing non-administrative functions.	**5D-2.6.2.a** Review documented policies and procedures to verify a Host System administrator is not permitted to use their administrative-level account when performing non-administrative functions.
	5D-2.6.2.b Interview and observe a Host System administrator to verify they use their operator-level account when performing non-administrative functions.
5D-2.7 Changes to a Host System user's account access privileges must be managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.	**5D-2.7.a** Examine documented policies and procedures to verify that changes to a user's access privileges are managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.
	5D-2.7.b Observe the process required to change a user's access privileges and verify that it is managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
	5D-2.7.c Inspect the Host System configuration settings and, for a sample of user accounts, verify that any changes to their access privileges have been formally documented in the audit log.
5D-2.8 All physical and logical access privileges must be reviewed at least quarterly to ensure that personnel with access to the decryption environment, the Host System and Host System software require that access for their position and job function.	**5D-2.8.a** Examine documented policies and procedures to verify that access privileges are reviewed, as a minimum, on a quarterly basis to ensure that the access privileges for personnel authorized to access the decryption environment, the Host System and Host System software required by their position and job function, are correctly assigned.
	5D-2.8.b Examine records and interview personnel to verify that access privileges are reviewed, as a minimum, on a quarterly basis.
5D-2.9 Tamper detection mechanisms must be implemented on the host, to include an alert generation upon opening of the Host System case, covers and/or doors.	**5D-2.9.a** Review Host System documentation to verify that tamper detection mechanisms are defined for the Host System, including the generation of an alert upon opening of the Host System case, covers and/or doors.
	5D-2.9.b Observe tamper-detection mechanisms on the Host System to verify that a tamper detection mechanism is implemented and includes the generation of an alert upon opening of the Host System case, covers and/or doors.
	5D-2.9.c Review records of alerts and interview personnel to verify an alert is generated upon opening of the Host System, covers and/or doors.
***5D-3** Non-console access to the Host System is configured securely.*	
***Note:** The term "non-console access" refers to any authorized access to the Host System that is performed by a person who is not physically present at the host processing system located within the secure room.*	
5D-3.1 All non-console access to the Host System must use strong cryptography and security protocols	**5D-3.1.a** For a sample of systems that are authorized to connect to the Host System via a non-console connection, inspect configuration settings to verify that access to the Host System is provided through the use of strong cryptography and security protocols
	5D-3.1.b Inspect the configuration settings of system components to verify that all traffic transmitted over the secure channel uses strong cryptography.
5D-3.2 Non-console access to the Host System must not provide access to any other service, or channel, outside of that used to connect to the Host, e.g., "split tunneling."	**5D-3.2.a** Inspect the configuration settings of the secure channel, to verify that 'split tunneling' is prohibited.
	5D-3.2.b Observe a Host System administrator log on to the device which provides non-console access to the Host System to verify that "split tunneling" is prohibited.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-3.3 All non-console access to the Host System must use two-factor authentication.	**5D-3.3.a** Inspect the configuration settings of the Host System and/or the device permitted to connect to the Host System, to verify that two-factor authentication is required for non-console access to the Host System.
	5D-3.3.b Observe a Host System administrator log on to the device that provides non-console access to the Host System to verify that two-factor authentication is required.
5D-3.4 Non-console connections to the Host System must only be permitted from authorized systems.	**5D-3.4.a** Examine documented policies and procedures to verify that a process is defined to authorize systems for non-console access, and not permit access until such times that authorization has been granted.
	5D-3.4.b For a sample of systems, examine device configurations to verify that non-console access is permitted only from the authorized systems.
5D-3.5 Non-console access to the Host System must only be permitted from a PCI DSS compliant environment.	**5D-3.5** Verify that non-console access to the Host System is only permitted from a PCI DSS compliant environment, including **5D-3.5.1** through **5D-3.5.2** Review solution provider documentation, including data flow diagrams, and perform the following:
5D-3.5.1 The authorized system (e.g., workstation) from which non-console access originates must meet all applicable PCI DSS requirements. For example, system hardening, patching, anti-virus protection, a local firewall etc.	**5D-3.5.1** Review solution provider documentation, including PCI DSS ROC and/or Attestation of Compliance (AOC), data flow diagrams, policies and, system configuration standards, to verify that the system authorized for non-console access meets all applicable PCI DSS requirements.
5D-3.5.2 The network/system that facilitates non-console access to the Host System must: • Originate from and be managed by the solution provider. • Meet all applicable PCI DSS requirements.	**5D-3.5.2.** Review solution provider documentation, including PCI DSS ROC and/or Attestation of Compliance (AOC), data flow diagrams, policies and, system configuration standards, to verify that the network/system that facilitates non-console access to the Host System must: • Originate from and be managed by the solution provider. • Meet all applicable PCI DSS requirements.
5D-3.6 Users with access to non-console connections to the Host System must be authorized to use non-console connections.	**5D-3.6.a** Examine documented policies and procedures to verify that non-console access to the Host System must only be provided to authorized users.
	5D-3.6.b Examine a sample of access control records and compare them to Host System settings to verify that non-console access to the Host System is only provided to authorized users.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-3.7 Non-console sessions to the Host System must be terminated after 15 minutes of inactivity.	**5D-3.7.a** Review documented policies and procedures to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.
	5D-3.7.b Inspect the system configuration settings to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.
***5D-4** The physical environment of the Host System is secured.*	
***Note:** When Host Systems are located within a secure rack in a shared data center, where "secure room" is referred to in this section, these controls can be met at room level, rack level, or a combination of both. Whichever way the requirements are applied, they should ensure that access the Host System is appropriately secured, whether in a secure room or a secure rack. For example, access to systems in a rack should be limited to those with a direct need to access that rack.*	
5D-4.1 The Host System must be located within a physically secure room that is dedicated to decryption operations and transaction processing.	**5D-4.1** Observe the physically secure room where the Host System is located and interview personnel to verify that all systems therein are designated to decryption operations and transaction processing.
5D-4.2 All individuals must be identified and authenticated before being granted access to the secure room—e.g., badge-control system, biometrics.	**5D-4.2.a** Examine documented policies and procedures to verify that all individuals must be identified and authenticated before being granted access to the secure room.
	5D-4.2.b Examine physical access controls to verify that all individuals are identified and authenticated before being granted access to the secure room.
	5D-4.2.c Observe authorized personnel entering the secure room to verify that all individuals are identified and authenticated before being granted access.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**

5D-4.3 All physical access to the secure room must be monitored and logs must be maintained as follows:
• Logs must be retained for a minimum of three years.
• Logs must be regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein.
• Log reviews must be documented.
• Logs must include but not be limited to:
  ○ Logs of access to the room from a badge access system
  ○ Logs of access to the room from a manual sign-in sheet
	5D-4.3.a Examine documented policies and procedures to verify all physical access to the secure room must be monitored and logs must be maintained. Policies and procedures must require the following:
	• Logs are retained for a minimum of three years.
	• Logs are regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein.
	• Log reviews are documented.
	• Logs include at a minimum:
	  ○ Access to the room from a badge access system
	  ○ Access to the room from a manual sign-in sheet

	5D-4.3.b Examine a sample of logs used to record physical access to the secure room to verify the following:
	• Logs are being retained for a minimum of three years.
	• Logs include at a minimum:
	  ○ Access to the room from a badge access system
	  ○ Access to the room from a manual sign-in sheet

	5D-4.3.c Interview personnel responsible for reviewing logs used to record physical access to the secure room, to verify the following: • Logs are regularly reviewed. • Log reviews are documented. • The person performing the review does not have access to the secure room or to the systems therein.
5D-4.4 Dual access must be required for the secure room housing the Host System.	**5D-4.4.a** Inspect physical access controls to verify that dual access is enforced.
	5D-4.4.b Observe authorized personnel entering the secure room to verify that dual access is enforced.
5D-4.5 Physical access must be only permitted to designated personnel with defined business needs and duties.	**5D-4.5.a** Examine documented policies and procedures to verify that physical access to the secure room is only permitted to designated personnel with defined business needs and duties.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
	5D-4.5.b Examine the list of designated personnel and interview responsible personnel to verify that only personnel with defined business needs and duties are permitted access to the secure room.
	5D-4.5.c Examine physical access controls to verify that physical access to the secure room is only permitted to pre-designated personnel with defined business needs and duties.
5D-4.6 The secure room must be monitored via CCTV on a 24 hour basis. This must include, as a minimum, the following areas: • All entrances and exists • Access to the Host System and HSM(s) ***Note:*** *Motion-activated systems that are separate from the intrusion-detection system may be used.*	**5D-4.6.a** Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a 24 hour basis, and covers, as a minimum, the following areas: • All entrances and exists • Access to the Host System and HSM(s)
	5D-4.6.b If CCTV is motion-activated, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.
5D-4.7 Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, or other systems which may expose sensitive data.	**5D-4.7** Observe CCTV camera positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any computer screens, PIN pads, keyboards, or other systems which may expose sensitive data.
5D-4.8 CCTV recorded images must be securely archived for at least 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**5D-4.8.a** Examine a sample of recordings to verify that at least the most recent 45 days of images are securely archived.
	5D-4.8.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.
5D-4.9 Personnel with access to the secure room must not have access to the media (e.g., VCR tapes, digital recording systems, etc.) with the recorded surveillance data.	**5D-4.9.a** Examine documented access policies and procedures to verify that personnel with access to the secure room are not permitted to have access to the media containing recorded surveillance data for that environment.
	5D-4.9.b Examine access lists for the secure room as well as access controls to the media containing surveillance data, to verify that personnel with access to the secure room do not have access to the media containing recorded surveillance data

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-4.10 Continuous or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (e.g., when infrared cameras are used).*	**5D-4.10.a** Observe the secure room to verify that continuous or motion-activated lighting is provided for the cameras monitoring the secure room.
	5D-4.10.b Examine a sample of recorded CCTV images to verify that appropriate lighting is provided when persons are present in the secure room.
5D-4.11 A 24/7 physical intrusion-detection system must be in place for the secure room (e.g., motion detectors when unoccupied). This must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.	**5D-4.11.a** Examine security policies and procedures to verify they require: • Continuous (24/7) physical intrusion-detection monitoring of the secure room. • The physical intrusion-detection must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.
	5D-4.11.b Observe the physical intrusion-detection system to verify that it: • Provides continuous (24/7) monitoring of the secure room. • It is connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.
5D-4.12 Any windows in the secure room must be locked, protected by alarmed sensors, or otherwise similarly secured.	**5D-4.12.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	5D-4.12.b Examine configuration of window sensors to verify that the alarm mechanism is active.
5D-4.13 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**5D-4.13** Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
5D-4.14 Access-control and monitoring systems must be connected to an uninterruptible power source (UPS) to prevent outages.	**5D-4.14** Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems are powered through the UPS.
5D-4.15 All alarm events must be logged.	**5D-4.15.a** Examine security policies and procedures to verify they require that all alarm events are logged.
	5D-4.15.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-4.16 Documented alarm events must be signed off by an authorized person who was not involved in the event.	**5D-4.16.a** Examine security policies and procedures to verify alarm events must be signed off by an authorized person other than the individual who was involved in the event.
	5D-4.16.b For a sample of documented alarm events, interview personnel who signed off on the event to verify that person was not involved in the event.
5D-4.17 Use of an emergency entry or exit mechanism must cause an alarm event.	**5D-4.17** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
5D-4.18 Authorized personnel must respond to all physical intrusion alarms within 30 minutes.	**5D-4.18.a** Examine documented policies and procedures to verify they define that all alarm events are responded to by authorized personnel within 30 minutes.
	5D-4.18.b Examine documented alarm events and interview personnel to verify alarm events were responded by authorized personnel within 30 minutes.
5D-4.19 A process for synchronizing the time and date stamps of the access-control, intrusion-detection and monitoring (camera) systems must be implemented. ***Note:*** *This may be done by either automated or manual mechanisms.*	**5D-4.19.a** Examine documented procedures to verify that mechanisms are defined for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems.
	5D-4.19.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	5D-4.19.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
5D-4.19.1 If a manual synchronization process is used, synchronization must occur at least quarterly, and documentation of the synchronization must be retained for at least a one-year period.	**5D-4.19.1.a** If a manual synchronization process is implemented, interview responsible personnel and examine records of synchronization to verify the mechanism is performed at least quarterly.
	5D-4.19.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.
5D-4.20 The entrance to the secure room must include a mechanism to ensure the door is not left open. *For example:* • *A door that is contact monitored and fitted with automatic closing or locking devices.* • *An airlock entrance system.*	**5D-4.20** Observe authorized personnel entering the secure room to verify that a mechanism is in place to ensure the door is not left open. *Examples include:* • *A door that is contact monitored and fitted with automatic closing or locking devices.* • *An airlock entrance system.*

Requirement 5D: Implement secure hybrid decryption process – Not applicable for merchant-managed solutions.	
Domain 5 Requirements	**Testing Procedures**
5D-4.21 An audible alarm must sound if the entrance to the secure room remains open for more than 30 seconds.	**5D-4.21.a** Examine secure room entry mechanisms to verify that an audible alarm is configured to sound if the entrance remains open for more than 30 seconds.
	5D-4.23.b Observe authorized personnel entering the secure room and request the door is held open. Verify that an audible alarm sounds if the entrance remains open for more than 30 seconds.

Requirement 5E: Component providers ONLY: report status to solution providers

Domain 5 Requirements	Testing Procedures
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain for subsequent PCI listing of the component provider's decryption-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 decryption-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).*	
5E-1 For component providers of decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	
5E-1.1 Track status of the decryption-management service and provide reports to solution provider annually and upon significant changes, including at least the following: • Types/models of HSMs • Number of HSMs deployed and any change in numbers since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per **5C-1.2**	**5E-1.1.a** Review component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel, and to confirm that the following processes are documented and implemented: • Providing reports annually and upon significant changes • Types/models of HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per **5C-1.2**
	5E-1.1.b Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per **5C-1.2**

Requirement 5E: Component providers ONLY: report status to solution providers

Domain 5 Requirements	Testing Procedures
5E-1.2 Manage and monitor changes to decryption-management services and notify the solution provider upon occurrence of any of the following: • Addition and/or removal of HSM types. • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status *Note that adding or removing HSM types may require adherence to PCI SSC's process for P2PE Designated Changes to Solutions. Please refer to the P2PE Program Guide for details about obligations when adding, changing, or removing elements of a P2PE solution.*	**5E-1.2.a** Review component provider's documented procedures and interview responsible component-provider personnel, and confirm that processes include notifying the solution provider upon occurrence of the following: • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types
	5E-1.2.b Observe reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types.

Domain 6: P2PE Cryptographic Key Operations and Device Management

Domain	Overview	P2PE Validation Requirements
Domain 6: **P2PE Cryptographic Key Operations and Device Management**	Establish and administer key-management operations for account-data encryption POI devices and decryption HSMs.	**6A** Account data is processed using algorithms and methodologies that ensure they are kept secure. **6B** Account-data keys and key-management methodologies 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. **6C** Keys are conveyed or transmitted in a secure manner. **6D** Key loading is handled in a secure manner. **6E** Keys are used in a manner that prevents or detects their unauthorized usage. **6F** Keys are administered in a secure manner. **6G** Equipment used to process account data and keys is managed in a secure manner. **6H** For hybrid decryption solutions: Implement secure hybrid-key management. **6I** Component providers *ONLY*: report status to solution providers.

Target Audience: *P2PE solution providers or those who, on behalf of P2PE solution providers, manage cryptographic key operations for POI devices, HSMs, and SCDs.*

Overview

Domain 6 covers the requirements for the use of strong cryptographic keys and secure key-management functions for all account-data encryption POI devices and decryption HSMs, including related key-management SCDs. Examples include POI devices, HSMs, key-injection/loading devices (KLDs) and signing devices. Implementation of these procedures is fundamental to the security of a P2PE solution. Domain 6 includes detailed key-management procedures including encryption methodologies, key generation, key distribution, key loading, key usage, key administration, equipment management, and hybrid decryption-key management (for hybrid decryption solutions only).

These requirements apply to all methods of key management that are utilized by the P2PE solution, including both asymmetric and symmetric methods (examples of symmetric key-management methods include fixed key, DUKPT, and master key/session key). Whenever encryption is being utilized, some form of key management must be performed, and it is this key management that must be compliant to the requirements of this domain.

Domain 6 requirements address secure cryptographic key-management operations for the encryption environment (Domain 1) and the decryption environment (Domain 5), as well as environments performing symmetric-key distribution using asymmetric keys (remote key distribution), certification authority/registration authority (Domain 6 Parts A1 and A2 respectively) and key-injection (Domain 6 Annex B).

The requirements in this domain apply to all key types, including keys used to secure account data, any key-encrypting keys used to encrypt these keys, and any keys that have a direct bearing on the security of the P2PE solution (e.g., keys used to protect the integrity of a whitelist). If the solution uses a multi-tier "key hierarchy," all keys up to and including the top-level "master key" must be assessed to meet these requirements.

Note for hybrid decryption environments:

Hybrid decryption environments require HSMs for cryptographic key-management functions but allow for non-SCD Host Systems to be used for account data decryption. Unlike a P2PE solution with a hardware decryption environment (in which cryptographic key management and account-data decryption are performed entirely within a hardware security module, or HSM), a hybrid decryption environment (which requires HSMs for cryptographic key-management functions) allows for the decryption of account data outside of an HSM in non-SCDs on a Host System. These environments must meet all requirements in Domains 5 and 6, including the additional requirements specified in section **6I** (as well as those specified in Domain 5 in section **5D**). See the "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" section for more information about validating this Domain as a solution provider, key-management component provider, or merchant as a solution provider.

Within this domain, the term "Solution Provider" refers to whichever entity is undergoing the P2PE assessment. This may be the solution provider, a component provider, or the merchant as a solution provider.

For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 5, and 6 of this document refers to merchant personnel in the encryption environments, and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.

Applicability of Domain 6 and Annexes to P2PE Solution Providers and Component Providers

Entity	Domain 6	Annex A Part A1	Annex A Part A2	Annex B
Solution provider (1)	X	X (2)	X (3)	
Device-management CP (1)	X	X (2)	X (3)	
Decryption-management CP (1)	X	X (2)	X (3)	
CA/RA		X (2	X(4)	
KIF		X (2)	X (3)	X

(1) Domain 6 with Domain 1 and/or Domain 5 as applicable to the functions performed
(2) As applicable – For any entity doing remote key distribution using asymmetric techniques
(3) As applicable – For any entity performing CA/RA functions
(4) Domain 6 and/or Annex B may also be applicable for CA/RA entities, depending on the functions performed.

Definitions and Annexes

For the purposes of this document:

- Secret Key = symmetric key (also known as a shared secret key)
- Private Key = asymmetric key used only for decryption operations or for creating digital signatures. No one private key should be used for both purposes (except for transaction-originating SCDs).
- Public Key = asymmetric key used only for encryption operations or for verifying digital signatures. No one public key should be used for both purposes (except for transaction-originating SCDs).

Domain 6 Normative Annex A – Symmetric-Key Distribution using Asymmetric Techniques

For specific requirements pertaining to entities involved in the implementation of symmetric-key distribution using asymmetric keys (remote key distribution) or those entities involved in the operation of Certification Authorities for such purposes, see Domain 6 Normative Annex A. Entities involved in remote key distribution are subject to both the requirements stipulated in the main body of the Domain 6 section of this document and the additional criteria stipulated in Annex A.

Domain 6 Normative Annex B – Key-Injection Facilities

For specific requirements pertaining to entities that operate key-injection facilities for the injection of keys (KEKs, PEKs, etc.) used for account data, see Domain 6 Normative Annex B. Note that, for P2PE, entities that solely operate a key-injection facility are only required to meet the requirements stipulated in Annex B (and may be required to meet Annex A as applicable to their services). Solution providers and other entities that perform key injection in addition to other P2PE solution functions are required to meet all requirements stipulated in the main body of Domain 6 that include key-injection requirements; therefore, these entities are not required to additionally meet the requirements stipulated in Annex B.

Domain 6 Normative Annex C – This annex provides the minimum and equivalent key sizes and strengths for the encryption of data and other cryptographic keys.

Requirement 6A: Account data is processed using algorithms and methodologies that ensure they are kept secure.	
Domain 6 Requirements	**Testing Procedures**
***6A-1** Account data is protected with appropriate cryptographic algorithms, key sizes and strengths, and key-management processes.*	
***Note:** An essential part of maintaining the security of POI devices and HSMs and the cryptographic keys used on those devices is for the solution provider to know where those devices and keys are—e.g., during key creation and loading onto devices, while being used at a merchant, when devices are undergoing repair, etc. Therefore, it is the responsibility of the entity managing devices and cryptographic keys to keep track of POI devices and HSMs from the point where the device is first added into the P2PE solution and has cryptographic keys loaded onto the device, until the disposal of that device or its removal from the solution.* *However, it is not the intent of these requirements that solution providers actively manage these devices when deployed at merchant encryption environments; the intent is that the solution provider maintains knowledge of the location and status of devices once deployed to merchants. Knowledge sharing and cross-cooperation may be necessary regarding the location and status of devices when different entities are responsible for managing devices and keys for different functions.*	
6A.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*.	**6A-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*.
	6A-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*.
6A-1.2 Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (e.g., after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (e.g., *NIST Special Publication 800-57*). *See Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.*	**6A-1.2.a** Examine documented key-management procedures to verify: • Crypto-periods are defined for every type of key in use. • Crypto-periods are based on industry best practices and guidelines (e.g., *NIST Special Publication 800-57*). • A process/methodology is in place to determine when the crypto-period is reached for each cryptographic key. • Cryptographic key changes are implemented whenever a key reaches the end of its defined crypto-period.
	6A-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.

Requirement 6A: Account data is processed using algorithms and methodologies that ensure they are kept secure.	
Domain 6 Requirements	**Testing Procedures**
6A-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.	**6A-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.
	6A-1.3.b Observe architecture and key-management operations to verify that the documentation reviewed in **6A-1.1.4.a** is demonstrably in use for all key-management processes.
6A-1.3.1 Maintain documentation of all cryptographic keys managed as part of the P2PE solution, including: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method	**6A-1.3.1.a** Examine key management policies and procedures and verify documentation of all cryptographic keys managed as part of the P2PE solution is required, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method
	6A-1.3.1.b Observe documentation and interview personnel and confirm that documentation of all cryptographic keys managed as part of the P2PE solution exists, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method

Requirement 6A: Account data is processed using algorithms and methodologies that ensure they are kept secure.	
Domain 6 Requirements	**Testing Procedures**
6A-1.3.2 Maintain a list of all devices used to generate keys or key components managed as part of the P2PE solution, including: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **6A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)	**6A-1.3.2.a** Examine key management policies and procedures and verify a list of all devices used to generate keys managed as part of the P2PE solution is required, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **6A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)
	6A-1.3.2.b Observe documentation and interview personnel and confirm that a list of all devices used to generate keys managed as part of the P2PE solution exists, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **6A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)

Requirement 6B:	***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.***

Domain 6 Requirements	Testing Procedures
***6B-1** All keys and key components are generated using an approved random or pseudo-random process .*	
6B-1.1 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. Cryptographic keys or key components must be generated by one of the following: • An approved key-generation function of a PCI–approved HSM or POI device; • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or • An approved random number generator that has been certified by an independent laboratory to comply with *NIST SP800-22* *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.*	**6B-1.1.a** Examine key-management policy document and verify that it requires that all devices used to generate cryptographic keys meet one of the following: • An approved key-generation function of a PCI–approved HSM or POI device; • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*.
	6B-1.1.b Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: • An approved key-generation function of a PCI–approved HSM or POI device; • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*
	6B-1.1.c Observe devices performing key-generation functions, including validation of firmware used.
***6B-2** Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*	
6B-2.1 Implement security controls, including dual control and tamper protection to prevent the unauthorized disclosure of keys/key components.	**6B-2.1** Perform the following:
6B-2.1.1 Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.	**6B-2.1.1.a** Examine documented procedures to verify the following. • 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. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.

Requirement 6B:	***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.***

Domain 6 Requirements	Testing Procedures
	6B-2.1.1.b Observe key-generation processes and interview responsible personnel to verify: • 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.. • There is no mechanism (including connectivity) that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.
6B-2.1.2 There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key. ***Note:*** *Full-length key components or key shares derived using a recognized key-splitting algorithm are not considered key parts and do not provide any information regarding the actual cryptographic key.*	**6B-2.1.2.a** Observe the 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.
	6B-2.1.2.b Examine key-generation logs to verify that at least two individuals performed the key-generation processes.
6B-2.1.3 Devices used for the generation of clear-text key components that are output in the clear must be powered off when not in use. 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.	**6B-2.1.3** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate clear-text key components are powered off when not in use; or • If logically partitioned for concurrent use in other processes, the key-generation capabilities are disabled when not in use and other activities are continuing.
6B-2.1.4 Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (e.g., unnecessary cables).	**6B-2.1.4.a** Review documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering, prior to use.
	6B-2.1.4.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.

Requirement 6B:	***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.***
Domain 6 Requirements	**Testing Procedures**
6B-2.1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area It must not be feasible to observe the key-component/key-generation process whereby clear-text keying material is observable either directly or via camera monitoring	**6B-2.1.5.a** Examine documentation to verify that physical security controls are defined to ensure the key component/key-generation process cannot be observed or accessed by unauthorized personnel.
	6B-2.1.5.b Observe the physical security controls to verify that key-component/key-generation process cannot be observed or accessed by unauthorized personnel.
6B-2.2 Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret key or private key, or key component thereof, appears in unprotected memory. *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 **6B-1** and the controls defined in Requirements at **6D-2** of Annex B.* *Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.* *Single-purpose computers with an installed SCD where clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) meet this requirement. Where the components pass through unprotected memory of the PC, it must meet Requirement **6D-2** of Annex B.*	**6B-2.2.a** Examine documented procedures 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 unprotected memory.
	6B-2.2.b Observe the generation process and review vendor 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 unprotected memory.

Requirement 6B:	***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.***

Domain 6 Requirements	Testing Procedures
6B-2.3 Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that: • Only approved key custodians can observe their own key component. • Tampering can be visually detected. Printers used for this purpose must not be used for other purposes.	**6B-2.3.a** Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed immediately after printing such that: • Only approved key custodians can observe their own key component. • Tampering can be visually detected.
	6B-2.3.b Observe processes for printing key components to verify 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.
	6B-2.3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be visually detected.
6B-2.4 Any residue that may contain clear-text keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual. *Examples of where such key residue may exist include (but are not limited to):* • *Printing material, including ribbons and paper waste* • *Memory storage of a key-loading device, after loading the key to a different device or system* • *Other types of displaying or recording*	**6B-2.4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures are implemented to ensure the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • 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 that will use the key.
	6B-2.4.b Observe the destruction process of the identified key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • 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 that will use the key.

Requirement 6B:	***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.***
Domain 6 Requirements	**Testing Procedures**
6B-2.5 Asymmetric-key pairs must either be: • Generated by the device that will use the key pair; or • If generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair	**6B-2.5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (zeroized) immediately after the transfer to the device that will use the key pair.
	6B-2.5.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (e.g., zeroized) immediately after the transfer to the device that will use the key pair.
6B-2.6 Policy and procedures must exist to ensure that clear-text private or secret keys or their components are prohibited from being transmitted across insecure channels. These include but are not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text private or secret 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	**6B-2.6.a** Examine documented policy and procedures to verify that clear-text private or secret keys or their components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text private or secret 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

Requirement 6B:	***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.***

Domain 6 Requirements	Testing Procedures
instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manuals	**6B-2.6.b** From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text private or secret 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
***6B-3** Documented procedures must exist and must be demonstrably in use for all key-generation processing.*	
6B-3.1 Written key-generation 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.	**6B-3.1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations.
	6B-3.1.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.
	6B-3.1.c Observe key-generation ceremonies, whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.
6B-3.2 Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs.	**6B-3.2.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.
	6B-3.2.b Observe demonstrations for the generation of higher-level keys to verify that all key-generation events are logged.
	6B-3.2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures
6C-1 *Secret or private keys shall be transferred by:* *a) Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or* *b) Transmitting the key in ciphertext form.* *Public keys must be conveyed in a manner that protects their integrity and authenticity.*	
6C-1.1 Keys must be transferred either encrypted or within an SCD. If clear-text outside of an SCD as two or more components using different communication channels. Clear-text key components may be transferred 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. ○ Ensure that details of the serial number of the package are conveyed separately from the package itself. ○ Ensure that that documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material. *(continued on next page)*	**6C-1.1.a** Determine whether keys are transmitted encrypted as clear-text components, or within an SCD. **6C-1.1.b** If key components are ever transmitted in clear-text using pre-numbered, tamper-evident, authenticable mailers, perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. • Examine documented procedures to verify that cryptographic-key components are transferred using different communications channels. • Examine records of key conveyances and interview responsible personnel to verify that cryptographic key components are transferred using different communications channels. • Examine documented procedures to verify that serial numbers are verified prior to the usage of the keying material.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures
6C-1.1 *(continued)* • Where an SCD is used for components, the mechanisms or data (e.g., PIN) to obtain the key component 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 (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. Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.	**6C-1.1.b** Where an SCD is used, perform the following: • Examine documented procedures to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels. • Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering. • Examine records of key transfers and interview responsible personnel to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels.
6C-1.2 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. *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.*	**6C-1.2.a** Examine documented procedures to verify they include controls to ensure that no single person can ever have 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: • 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. • Any person with access to the media conveying a 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 of this key that is sufficient to form the necessary threshold to derive the key.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
	6C-1.2.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can ever have 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: • An individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a key component or key share 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.
	6C-1.2.c Examine documented procedures and interview responsible personnel to verify that the method used does not allow for any personnel to have access to all components.
	6C-1.2.d Observe the method used to transport key components to verify that the method does not allow for any personnel to have access to all components.
6C-1.3 E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) 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 unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear-text of any encrypted text or files conveyed through those systems. Other similar mechanisms, such as SMS, fax, or telephone shall not be used to convey clear-text key values.	**6C-1.3** Validate through interviews, observation, and logs that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures
6C-1.4 Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of public-key certificates as defined in Annex A that are created by a trusted CA that meets the requirements of Annex A • A hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 • Within an SCD ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.*	**6C-1.4.a** For all methods used to convey public keys, perform the following:
	6C-1.4.b Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity, such as: • Use of public-key certificates created by a trusted CA that meets the requirements of Annex A • A hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 • Within an SCD
	6C-1.4.c Observe the process for conveying public keys and interview responsible personnel to verify that self-signed certificates are not be used as the sole method of authentication.
	6C-1.4.d Observe the process for conveying public keys and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures
***6C-2** During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.*	
Sending and receiving entities are equally responsible for the physical protection of the materials involved.	
6C-2.1 Any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • 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. ***Note:** No single person shall be able to access or use all components or a quorum of shares of a single secret or private cryptographic key.*	**6C-2.1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component • 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.
	6C-2.1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text secret or private key component/share is at all times either: • Under the continuous supervision of a person with authorized access to this component • Locked in a security container (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or • Contained within a physically secure SCD.
6C-2.2 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 must result in the destruction and replacement of: • The set of components • Any keys encrypted under this (combined) key	**6C-2.2.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.
	6C-2.2.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.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures
	6C-2.2.c Verify documented procedures require that any sign of package tampering results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
	6C-2.2.d Interview responsible personnel and observe processes to verify that if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
6C-2.3 Only the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.	**6C-2.3.a** Verify that a list(s) of key custodians (and designated backup(s)) authorized to have physical access to key components prior to transmittal or upon receipt of a component is defined and documented.
	6C-2.3.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 transmittal or upon receipt.
	6C-2.3.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.
6C-2.4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal. • Check tamper-evident packaging upon receipt for signs of tamper prior to opening tamper-evident authenticable packaging containing key components. • Check the serial number of the tamper-evident packaging upon receipt of a component package.	**6C-2.4.a** Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
	6C-2.4.b Observe implemented mechanisms and processes to verify that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.
6C-2.5 Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers. ***Note:*** *Numbered courier bags are not sufficient for this purpose*	**6C-2.5** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.
***6C-3** All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*	
6C-3.1 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. *(continued on next page)*	**6C-3.1.a** Examine documented procedures to verify 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.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Requirements	Testing Procedures

6C-3.1 *(continued)*
• DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
• A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength.
• TDEA keys shall not be used to protect AES keys.
• TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.
• RSA keys encrypting keys greater in strength than 80 bits shall have bit strength of at least 112 bits.
	6C-3.1.b Observe key-generation processes to verify 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.
	• Interview appropriate personnel and examine documented procedures for the creation of these keys.
	• Using the table in Annex C, validate the respective key sizes for DEA, RSA, Elliptic Curve, DSA, and Diffie Hellman algorithms where used for key encryption.
	• Verify that:
	  ○ DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
	  ○ A double- or triple-length DEA key must not be encrypted with a DEA 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 bit strength at least 112 bits.

	6C-1.c Examine system documentation and configuration files to validate the above, including HSM settings.
6C-4 *Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.*	
6C-4.1 Written procedures must exist and be known to all affected parties.	**6C-4.1.a** Verify documented procedures exist for all key transmission and conveyance processing.
	6C-4.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.
6C-4.2 Methods used for the conveyance or receipt of keys must be documented.	**6C-4.2** Verify documented procedures include all methods used for the conveyance or receipt of keys.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6D-1** Secret and private keys must be input into hardware (host) security modules (HSMs) and Point of Interaction (POI) devices in a secure manner.* *a) Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.* b) *Key-establishment techniques using public-key cryptography must be implemented securely.*	
6D-1.1 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.*	**6D-1.1.a** Review documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.
	6D-1.1.b Interview appropriate personnel to determine the number of key components for each manually loaded key, the length of the key components, and the methodology used to form the key.
	6D-1.1.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 to information provided through verbal discussion and written documentation.
	6D-1.1.d Verify that the process includes the entry of individual key components by the designated key custodians.
	6D-1.1.e Ensure key-loading devices can only be accessed and used under dual control.
6D-1.2 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.	**6D-1.2**. Examine logs of access to security containers for key components to verify that only the authorized custodian(s) have accessed. Compare the number on the current tamper-evident, authenticable bag for each component to the last log entry for that component.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.

Domain 6 Requirements	Testing Procedures
6D-1.3 The loading of clear-text cryptographic keys using a key-loading device requires dual control to authorize any key-loading session. It shall not be possible for a single person to use the key-loading device to load clear keys alone. Dual control must be implemented using one or more of, but not limited to, the following techniques: • Two or more passwords of five characters or more (vendor default values must be changed) • Multiple cryptographic tokens (such as smartcards), or physical keys • Physical access controls *Note that for devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian*.	**6D-1.3.a** Examine documented procedures for loading of clear-text cryptographic keys to verify they require dual control to authorize any key-loading session.
	6D-1.3.b For all types of production SCDs, observe processes for loading clear-text cryptographic keys to verify that dual control is required to authorize any key-loading session. Verify that any passwords used are a minimum of five characters.
	6D-1.3.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.
	6D-1.3.d Ensure that any default dual-control mechanisms (e.g., default passwords—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.
6D-1.4 Key components for symmetric keys must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components (e.g., via XOR'ing of full-length components). The resulting key must only exist within the SCD. *Note that 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.*	**6D-1.4.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.
	6D-1.4.b Examine key-component lengths or device configuration settings to verify that key components used to create a key are the same length as the resultant key.
6D-1.5 Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.	**6D-1.5** Examine vendor documentation describing options for how the HSM MFK is created. Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6D-1.6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.	**6D-1.6** Through 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.
6D-1.7 The initial terminal master key (TMK) 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 may use techniques described in this documents such as: • Asymmetric techniques • Manual techniques • The existing TMK to encrypt the replacement TMK for download Keys shall not be reloaded by any methodology in the event of a compromised device, and must be withdrawn from use.	**6D-1.7.a** Examine documented procedures for the loading of TMKs to verify that they require asymmetric key-loading techniques or manual techniques for initial loading. **6D-1.7.b** Examine documented procedures to verify that keys are prohibited from reloading or reuse wherever suspected of being compromised and are withdrawn from use.
6D-1.8 If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, these must meet the requirements detailed in Annex A of this document. For example: A public-key technique for the distribution of symmetric secret keys must: • Use public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Provide for mutual device authentication for both the host and the POI device or host-to-host if applicable, including assurance to the host that the POI device actually has (or actually can) compute the session key, and that no entity other than the POI device specifically identified can possibly compute the session key.	**6D-1.8.a** For techniques involving public-key cryptography, examine documentation and develop a schematic 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. **6D 1.8.b** If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, verify that the requirements detailed in Annex A of this document are met, including: • Use of public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.

Domain 6 Requirements	Testing Procedures
6D-2 *The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	
6D-2.1 Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that: • Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of clear-text key components. • There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys. • The SCD must be inspected prior to use to ensure that it has not been subject to any prior tampering 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.	**6D-2.1** Observe key-loading environments, processes, and mechanisms (e.g., terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Ensure cameras are positioned to ensure they cannot monitor the entering of clear-text key components. • Review documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that: ○ SCDs are inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. ○ An SCD transfers a plaintext secret or private key only when at least two authorized individuals are identified by the device. ○ There is not any mechanism at the interface (including cabling) between the conveyance medium and the SCD that might disclose the transferred keys. ○ The SCD is inspected to ensure it has not been subject to any prior tampering, which could lead to the disclosure of clear-text keying material.
6D-2.2 Only SCDs shall 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 this requirement. For example, computer keyboards shall never be used for the loading of clear-text secret or private keys or their components.	**6D-2.2** 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 shall never be used for the loading of clear-text secret or private keys or their components.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6D-2.3 The loading of secret or private key components from electronic medium—e.g., smart card, thumb drive, fob or other devices used for data transport—to a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following • The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium in accordance with Requirement **6F-4**.	**6D-2.3.a** Examine documented procedures for the loading of secret or private key components from electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key injection, including: • Instructions for the medium to be placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.
	6D-2.3.b Observe key-loading processes to verify that the injection process results in one of the following: • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.
6D-2.4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:	**6D-2.4** Review documented procedures and observe processes for the use of key-loading devices. Perform the following:
6D-2.4.1 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.	**6D-2.4.1** 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.
6D-2.4.2 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.	**6D-2.4.2** 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.
6D-2.4.3 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.	**6D-2.4.3.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.
	6D-2.4.3.b Verify 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.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6D-2.4.4 The key-loading device must not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred.	**6D-2.4.4** 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.
6D-2.5 Any media (electronic or otherwise) containing secret or private key components 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 a non-custodian for that component.	**6D-2.5.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.
	6D-2.5.b Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices be in the physical possession of only the designated component holder(s). • The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.
	6D-2.5.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).
	6D-2.5.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.
6D-2.6 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.	**6D-2.6** 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.
6D-2.7 Written or printed key component documents must not be opened until immediately prior to use.	**6D-2.7.a** Review documented procedures and confirm that printed/written key component documents are not opened until immediately prior to use.
	6D-2.7.b Observe key-loading processes and verify that printed/written key component documents are not opened until immediately prior to use.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.

Domain 6 Requirements	Testing Procedures
6D-2.8 A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. *E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.*	**6D-2.8.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.
	6D-2.9.b Examine key-component access controls and access logs to verify that any single authorized custodian can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.
***6D-3** All hardware and access/authentication mechanisms (e.g., passwords) used for key loading or the signing of authenticated applications (e.g., for "whitelists") must be managed under dual control.*	
6D-3.1 Any hardware and passwords 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 and associated hardware) must be managed such that no single individual has the capability to enable key loading of clear-text keys or their components. This is not to imply that individual access authentication mechanisms must be managed under dual control. ***Note:** Where key-loading is performed for POI devices, the secure environment as defined in Annex B Requirement **6G-4.10** must additionally be met.*	**6D-3.1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords 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.
	6D-3.1.b Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function or for the signing of authenticated applications is controlled and maintained in a secure environment under dual control. • All resources (e.g., passwords 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.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6D-3.2 All cable attachments where clear-text keying material traverses must be examined before each key-loading or application signing operation to ensure they have not been tampered with or compromised.	**6D-3.2.a** Review documented procedures to ensure they require that cable attachments be examined prior to key-loading functions or application signing operations.
	6D-3.2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to key-loading functions or application-signing operations.
6D-3.3 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.	**6D-3.3.a** Observe key-loading and application-signing activities to verify that key-loading equipment usage is monitored.
	6D-3.3.b Verify logs of all key-loading and application-signing activities are maintained and contain all required information.
6D-3.4 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 the use of access-control logs for when removed or placed into secure storage.	**6D-3.4.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.
	6D-3.4.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.
	6D-3.4.c Review storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.
	6D-3.4.d Verify that access-control logs exist and are in use.
	6D-3.4.e Reconcile storage contents to access-control logs.
6D-3.5 Default passwords or PINs 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.	**6D-3.5.a** Verify that documented procedures require default passwords or PINs used to enforce dual-control mechanisms are changed.
	6D-3.5.b Verify that documented procedures exist to require that these passwords/PINs be changed when assigned personnel change.

Requirement 6D: Key loading to HSMs and POI devices is handled in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6D-4** The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	
6D-4.1 A cryptographic-based validation mechanism must be in place to ensure the authenticity and integrity of keys and/or their components (e.g., testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See ISO 11568. Where check values are used, recorded or displayed key-component check values and key check values shall not exceed six hexadecimal characters in length.	**6D-4.1.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.
	6D-4.1.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.
	6D-4.1.c Verify that the methods used for key validation are consistent with ISO 11568—e.g., when check values are used, they should return a value of no more than six hexadecimal characters.
6D-4.2 The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted in accordance with Annex C, or if in plaintext form, must: • Be within a certificate as defined in Annex A, or • Be within a PKCS#10, or • Be within an SCD, or • Have a MAC (message authentication code) created using the algorithm defined in ISO 16609	**6D-4.2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.
	6D-4.2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.
***6D-5** Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*	
6D-5.1 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.	**6D-5.1.a** Verify documented procedures exist for all key-loading operations.
	6D-5.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.
	6D-5.1.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.
6D-5.2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.	**6D-5.2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.

Domain 6 Requirements	Testing Procedures
6E-1 *Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems of two organizations or logically separate systems within the same organization.*	
6E-1.1 Where two organizations or logically separate systems share a key to encrypt account data (including a key-encipherment key used to encrypt a data-encryption key) communicated between them, that key must: • Be unique to those two entities or logically separate systems and • Not be given to any other entity or logically separate systems.	**6E-1.1.a** Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations or logically separate systems. 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:
	6E-1.1.b 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.
	6E-1.1.c 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.
	6E-1.1.d Compare key check values against those for known or default keys to verify that known or default key values are not used.
6E-2 *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	
6E-2.1 Synchronization errors must be monitored to help reduce the risk of an adversary's substituting a key known only to them. Procedures must exist and be followed for investigating repeated synchronization errors for online processes such as online key exchanges or transmission or processing of transactions. ***Note:*** *Multiple synchronization errors may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted.*	**6E-2.1.a** Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.
	6E-2.1.b Verify that implemented procedures include: • Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) • Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Requirements	**Testing Procedures**
6E-2.2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.	**6E-2.2.a** Verify documented procedures require that key-component packaging/containers showing signs of tampering must result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
	6E-2.2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
***6E-3** Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	
6E-3.1 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.). 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.	**6E-3.1.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.
	6E-3.1.b Using a sample of device types, validate via review of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.
6E-3.2 Private keys must only be used as follows: • 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). • Private keys must never be used to encrypt other keys.	**6E-3.2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are only used as follows: • To create digital signatures or to perform decryption operations. • For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both. • Private keys are never used to encrypt other keys.
6E-3.3 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).	**6E-3.3** Examine key-management documentation and interview key custodian and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for POI devices).

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Requirements	**Testing Procedures**
6E-3.4 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. *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 must be managed and controlled as production.*	**6E-3.4.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.
	6E-3.4.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.
	6E-3.4.c Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.
	6E-3.4.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.
6E-3.5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements. At all times, the HSMs and servers/computers must be physically and logically secured in accordance with these requirements. *Note this does not apply to HSMs that are never intended to be used for production*	**6E-3.5** Interview personnel to determine whether production platforms are ever temporarily used for test purposes. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.

Domain 6 Requirements	Testing Procedures
6E-4 *All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or account data-encipherment) by a POI device that processes account data must be unique (except by chance) to that device.*	
6E-4.1 POI devices must each implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device. *This means not only the account-data-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.* *POI device private keys must not exist anywhere but the specific POI device they belong to, except where generated external to the POI device and prior to the injection into the POI device.*	**6E-4.1.a** Examine documented procedures for the loading and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations.
	6E-4.1.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.
	6E-4.1.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.
6E-4.2 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.	**6E-4.2.a** Determine whether any POI device interfaces with multiple entities for decryption. If so: • Examine documented procedures for generating all types of keys and verify the procedures ensure that unique keys or sets of keys are used for each acquiring organization and totally independent and are not variants of one another.
	6E-4.2.b Interview personnel and observe key-generation processes to verify that unique keys or sets of keys are generated for each acquiring organization.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Requirements	**Testing Procedures**
6E-4.3 Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device. This requirement refers to the use of a single "base" key to derive master 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.	**6E-4.3.a** Examine documented procedures and observe processes for generating master keys. Verify the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI device. **6E-4.3.b** Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.
6E-4.4 Entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring organizations must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques: • Different BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model • Different BDKs by geographic region, market segment, platform, or sales unit Injection vendors 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.	**6E-4.4** Determine whether the entity processing or injecting DUKPT or other key-derivation methodologies does so on behalf of multiple acquiring organizations. If so: • Interview personnel and review documented procedures to determine that unique Base Derivation Keys are used for each acquiring organization. • Observe key-injection processes for devices associated with different acquiring organizations to verify that Base Derivation Key(s) unique to each organization are used.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Requirements	Testing Procedures
6F-1 *Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	
Note for hybrid decryption solutions: *Requirements specific to hybrid decryption solutions are shown in italics throughout 6F.*	
6F-1.1 Secret or private keys must only exist in one or more of the following forms: • At least two separate key shares or full-length components • Encrypted with a key of equal or greater strength as delineated in Annex C • Contained within a secure cryptographic device ***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.*	**6F-1.1.a** Examine documented procedures for key storage and usage and observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored *(with the exception of DDKs used on the Host System for hybrid decryption solutions)*.
	6F-1.1.b Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored *(with the exception of DDKs used on the Host System for hybrid decryption solutions)*.
6F-1.2 Wherever key components are used, they have the following properties:	**6F-1.2** Examine documented procedures and interview responsible personnel to determine all instances where key components are used. Perform the following wherever key components are used:
6F-1.2.1 Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.	**6F-1.2.1** Review processes for creating key components and examine key components to verify that knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key.
6F-1.2.2 Construction of the cryptographic key requires the use of at least two key components/shares.	**6F-1.2.2** Observe processes for constructing cryptographic keys to verify that at least two key components/shares are required for each key construction.
6F-1.2.3 Each key component/share has one or more specified authorized custodians.	**6F-1.2.3.a** Examine documented procedures for the use of key components and interview key custodians and key-management supervisory personnel to verify that each key component is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component.
	6F-1.2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components are designated as key custodians for those particular components.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Requirements	Testing Procedures
6F-1.2.4 Procedures exist to ensure any custodian never has access to sufficient key components or shares to reconstruct a secret or private key cryptographic key. *For example, in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian must not then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.* *In an m-of-n scheme where n=5, where three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (e.g., component A and component B), as a second custodian (with, in this example, component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*	**6F-1.2.4.a** Examine documented procedures for the use of key components to verify that procedures ensure that any custodian never has access to sufficient key components or shares to reconstruct a secret or private cryptographic key. **6F-1.2.4.b** Examine key-component 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.
6F-1.3 Key components must be stored as follows:	**6F-1.3** Examine documented procedures, interview responsible personnel and inspect key-component storage locations to verify that key components are stored as outlined in Requirements **6F-1.3.1** through **6F-1.3.3** below:
6F-1.3.1 Key components that exist in clear-text outside of an SCD must be sealed in opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging. *(continued on next page)*	**6F-1.3.1.a** Examine key components and storage locations to verify that components are stored in opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging. **6F-1.3.1.b** Inspect any tamper-evident packaging used to secure key components and ensure that it prevents the determination of the key component without visible damage to the packaging.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Requirements	Testing Procedures
6F-1.3.1 *(continued)* ***Note:*** *Tamper-evident authenticable packaging—opacity may be envelopes within tamper-evident packaging— used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless 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.*	**6F-1.3.1.c** Ensure clear-text key components do not exist in any other locations, including in non-secure containers, in databases, on floppy disks, or in software programs.
	6F-1.3.1.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).
6F-1.3.2 Key components for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.* *Components 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.*	**6F-1.3.2** Inspect each key component storage container and verify the following: • 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).
6F-1.3.3 If a key 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.	**6F-1.3.3** 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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6F-2** Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.*	
6F-2.1 Procedures for known or suspected compromised keys must include the following:	**6F-2.1** Verify documented procedures exist for replacing known or suspected compromised keys that includes all of the following (**6F-2.1.1** through **6F-2.1.5** below):
6F-2.1.1 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.	**6F-2.1.1** Interview responsible personnel and observe implemented processes to verify 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.
6F-2.1.2 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.	**6F-2.1.2** 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.
6F-2.1.3. A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s). ***Note:*** *The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.* *Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.*	**6F-2.1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, and all the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6F-2.1.4 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	**6F-2.1.4.a** Interview responsible personnel and observe implemented 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). **6F-2.1.4.b** Verify notifications include the following: • A damage assessment including, where necessary, the engagement of outside consultants • Details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.
6F-2.1.5 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: • Missing secure cryptographic devices • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • *Host System tamper-detection mechanism has been activated, for hybrid decryption solutions*	**6F-2.1.5** Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • *Host System tamper-detection mechanism has been activated, for hybrid decryption solutions*

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6F-2.2 If attempts to load a secret key or key component into an KLD or POI device *(or a Host System, for hybrid decryption solutions)* fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device *(or Host System)*.	**6F-2.2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an KLD or POI device *(or a Host System, for hybrid decryption solutions)* fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device *(or Host System)*.
6F-3 *Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.* *Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.* *Keys generated with a non-reversible process, such as key derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*	
6F-3.1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes, but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from account-data keys. ***Note:*** *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*	**6F-3.1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods. **6F-3.1.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.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Requirements	Testing Procedures
6F-3.2 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 shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration. *A logical configuration is defined as one where all the components form a system used to undertake a particular task and are managed and controlled under a single operational and security policy.*	**6F-3.2.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.* **6F-3.2.b** Review vendor documentation to determine support for key variants. **6F-3.2.c** Via review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used, determine that variants of the MFK are not used external to the logical configuration that houses the MFK.
6F-3.3 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys (e.g., PEKs) from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or working keys with different purposes from another working key. ***Note:*** *Using transforms of keys across different levels of a key hierarchy—e.g., generating a PEK from a key-encrypting key—increases the risk of exposure of each of those keys.* *It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.*	**6F-3.3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys • Variants of working keys must only be calculated from other working keys.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6F-4** Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*	
6F-4.1 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.	**6F-4.1.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.
	6F-4.1.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.
	6F-4.1.c Review storage locations for the sample of destroyed keys to verify they are no longer kept.
6F-4.2 The procedures for destroying keys or key components that are no longer used or that 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. This must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient. ***Note:** Key destruction for keys installed in HSMs and POI devices is addressed in Requirement **6G-3**.*	**6F-4.2.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.
	6F-4.2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.
6F-4.2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic database backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568. *For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.*	**6F-4.2.1.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.
	6F-4.2.1.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.
6F-4.2.2 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.	**6F-4.2.2.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.
	6F-4.2.2.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**.**

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6F-4.3 Key components for keys other than the HSM MFK 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.	**6F-4.3.a** Verify documented procedures exist for destroying key components of keys once the keys are successfully loaded and validated as operational.
	6F-4.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.
***6F-5** Access to secret and private cryptographic keys and key material must be:* a) *Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and* b) *Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*	
6F-5.1 To reduce the opportunity for key compromise, limit the number of key custodians to a minimum required for operational efficiency. For example:	**6F-5.1** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:
6F-5.1.1 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.	**6F-5.1.1** Review key-custodian assignments for each component to verify that: • A primary and a backup key custodian are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel.
6F-5.1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.	**6F-5.1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form.
	6F-5.1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6F-5.1.3 Each key-custodian form provides the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access	**6F-5.1.3** Examine all key-custodian forms to verify that they include the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access.
6F-5.1.4 In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual except as noted below for organizations of insufficient size. *For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual.* *(continued on next page)*	**6F-5.1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisor possess the necessary threshold of key components sufficient to form any given key.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Requirements	Testing Procedures
6F-5.1.4 *(continued)* The components collectively held by an individual and his or her direct reports shall not constitute a quorum (or shall not provide any information about the value of the key that is not derivable from a single component). When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented. Organizations that are of such insufficient size that they cannot support the reporting-structure requirement must ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian), receive explicit training to instruct them from sharing key components with their direct manager, and must sign key-custodian agreements that includes an attestation to the requirement.	**6F-5.1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, ensure that documented procedures exist and are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes whistleblower procedures to report any violations.
***6F-6** Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.*	
6F-6.1 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. At a minimum, logs must include the following: • Date and time in/out • Key-component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)	**6F-6.1.a** Review log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD **6F-6.1.b** Review log files and audit log settings to verify that logs include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6F-7** Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.* ***Note:** It is not a requirement to have backup copies of key components or keys.*	
***Note for hybrid decryption solutions:** Clear-text cryptographic keys used on the Host System must not be included in any system back-up (refer to Requirement 5D-1.13)*	
6F-7.1 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.	**6F-7.1** 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:
	6F-7.1.a 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.
	6F-7.1.b Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: • Securely stored with proper access controls • Under at least dual control • Subject to at least the same level of security control as operational keys as specified in this document
6F-7.2 If backup copies are created, the following must be in place: • Creation (including cloning) of top-level keys—e.g., MFKs—must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.	**6F-7.2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process • All requirements applicable for the original keys also apply to any backup copies of keys and their components.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6F-8** Documented procedures must exist and must be demonstrably in use for all key-administration operations.*	
6F-8.1 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: • Security-awareness 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	**6F-8.1.a** Examine documented procedures for key-administration operations to verify they cover all activities related to key administration, and include: • Security-awareness 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
	6F-8.1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.
	6F-8.1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.
	6F-8.1.d Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
***6G-1**. Equipment used to protect account data (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*	
***Note:** Where POI is mentioned in Requirement **6G-1**, the requirements apply to the solution provider managing POI devices prior to deployment to distribution channels or to the merchants that will process payments with the POI device. Merchant protection and use of POI devices once deployed are not the subjects of these P2PE requirements and are instead covered by guidance provided to merchants by the solution provider in the P2PE Instruction Manual (PIM). See PIM Template for more information about guidance required to be included in the PIM.* *Likewise, distribution channels used by a solution provider to distribute POI devices to the end merchant are also not the subjects of these P2PE requirements. However, regardless of the distribution channel used, the merchant that will process payments with the device must be able to confirm that the device and packaging has not been tampered with via instructions provided in the PIM. For example, this could be done via secure inner packaging that easily shows evidence that it has been tampered with or opened previously via instructions provided to the merchant in the PIM. The merchant in such scenarios must also be able to establish secure, confirmed communications with the solution provider via the POI device keys, also with instructions provided in the PIM.*	
6G-1.1 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.	**6G-1.1.a** Review documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.
	6G-1.1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6G-1.1.1 Controls must be implemented to protect POI devices and other SCDs from unauthorized access up to point of deployment. Controls must include the following:	**6G-1.1.1.a** Review documented procedures to verify controls are defined to protect POIs, and other SCDs from unauthorized access up to point of deployment.
	6G-1.1.1.b Verify that documented procedures include **6G-1.1.1.1** through **6G-1.1.1.3** below.
6G-1.1.1.1 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.	**6G-1.1.1.1.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.
	6G-1.1.1.1.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.
	6G-1.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD.
6G-1.1.1.2 POI devices and other SCDs must not use default keys (such as keys that are pre-installed for testing purposes), passwords, or data.	**6G-1.1.1.2** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys, passwords, or data are not used.
6G-1.1.1.3 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 sending POI devices to either a distribution channel or the end merchant who will use the POI device to process transactions.*	**6G-1.1.1.3.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POI devices and other SCDs are documented in a formal list. • All personnel with access to POI devices and other SCDs are authorized by management. • The authorizations are reviewed annually.
	6G-1.1.1.3.b For a sample of POI device types and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in the formal list have access to devices.
6G-1.2 Not used in Domain 6, but is used in Annex B	

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Requirements	Testing Procedures
6G-1.3 Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the following. Transportation using a trusted courier service (e.g., via bonded carrier). The devices are then securely stored until key-insertion occurs. Use of physically secure and trackable packaging (e.g., pre-serialized, counterfeit-resistant, tamper-evident packaging). 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. 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. *(**Note:** Unauthorized access includes that by customs officials.)* Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised. *(**Note**: this control must be used in conjunction with one of the other methods.)* Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.	**6G-1.3.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. **6G-1.3.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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6G-1.4 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.	**6G-1.4.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.
	6G-1.4.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.
6G-1.4.1 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 validations must be maintained. ***Note:*** *Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.*	**6G-1.4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.
	6G-1.4.1.b For a sample of received devices, review 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 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.
6G-1.4.2 Not used in Domain 6, but is used in Annex B)	
6G-1.4.3 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.*	**6G-1.4.3** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6G-1.4.4 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 :	**6G-1.4.4.a** Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify integrity of device and include requirements specified at **6G-1.4.4.1** through **6G-1.4.4.4** below.
6G-1.4.4.1 Running self-tests to ensure the correct operation of the device.	**6G-1.4.4.1** 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.
6G-1.4.4.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.	**6G-1.4.4.2** 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.
6G-1.4.4.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed	**6G-1.4.4.3** 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.
6G-1.4.4.4 Maintaining records of the tests and inspections, and retaining records for at least one year.	**6G-1.4.4.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	6G-1.4.4.4.b Examine records of inspections to verify records are retained for at least one year.
6G-1.4.5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	**6G-1.4.5.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.
	6G-1.4.5.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.
6G-2 Not used in Domain 6 but is used in Annex B	

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Requirements	Testing Procedures
***6G-3** Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*	
***Note:** The requirements in 6G-3 apply to the solution provider managing POI devices when removed from service, retired at the end of the deployment lifecycle, or returned for repair. Merchant protection and use of POI devices once deployed are not the subjects of these P2PE requirements and are instead covered by guidance provided to merchants by the solution provider in the P2PE Instruction Manual (PIM). See PIM Template for more information about guidance required to be included in the PIM.*	
6G-3.1 Procedures are 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 that all keys, key material, and account data stored within the device must be rendered irrecoverable. Processes must include the following: ***Note:** Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*	**6G-3.1** Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all keys and 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 **6G-3.1.1** through **6G-3.1.6** below.
6G-3.1.1 HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes.	**6G-3.1.1.a** Review documented procedures for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.
	6G-3.1.1.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.
6G-3.1.2 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.	**6G-3.1.2** 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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6G-3.1.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	**6G-3.1.3** 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.
6G-3.1.4 Affected entities are notified before devices are returned.	**6G-3.1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
6G-3.1.5 Devices are tracked during the return process.	**6G-3.1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
6G-3.1.6 Records of the tests and inspections are maintained for at least one year.	**6G-3.1.6** Interview personnel and observe records to verify that records of the tests and inspections are maintained for at least one year.
***6G-4** Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key, or signing applications to be loaded onto a POI device, must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:* *a) Dual access controls required to enable the key-encryption function* *b) Physical protection of the equipment (e.g., locked access to it) under dual control* c) *Restriction of logical access to the equipment*	
6G-4.1 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:	**6G-4.1.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.
	6G-4.1.b Verify that documented procedures cover requirements **6G-4.1.1** through **6G-4.1.5** below.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Requirements	Testing Procedures
6G-4.1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. ***Note:*** *Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords, or for physical access via a physical lock that requires two individuals each with a different high-security key.* *For devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.* *Physical keys, authorization codes, passwords, 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.*	**6G-4.1.1** 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.
6G-4.1.1.1 Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.	**6G-4.1.1.1** Observe password policies and configuration settings to confirm that passwords used for dual control must be at least five numeric and/or alphabetic characters.
6G-4.1.2 Dual control must be implemented for the following: • To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of clear-text key components; • For all access to key-loading devices (KLDs) and authenticated application-signing devices.	**6G-4.1.2** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of clear-text key components; • For all access to KLDs and authenticated application-signing devices.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Requirements	**Testing Procedures**
6G-4.1.3 Devices must not use default passwords.	**6G-4.1.3.a** Examine password policies and documented procedures to confirm default passwords must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists.
	6G-4.1.3.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.
6G-4.1.4 To detect any unauthorized use, devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected.	**6G-4.1.4.a** Examine documented procedures to confirm that they require devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
	6G-4.1.4.b Interview responsible personnel and observe devices and processes to confirm that devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
6G-5 *Documented procedures must exist and be demonstrably in use to ensure the security and integrity of account-data processing equipment (e.g., POI devices and HSMs) placed into service, initialized, deployed, used, and decommissioned.*	
6G-5.1 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.	**6G-5.1.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
	6G-5.1.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.

Requirement 6H: For hybrid decryption solutions: Implement secure hybrid key management	
Domain 6 Requirements	**Testing Procedures**
6H-1 *Hybrid decryption solutions securely manage the Data Decryption Keys (DDKs) that decrypt account data in software on a Host System.*	

Requirement 6H: For hybrid decryption solutions: Implement secure hybrid key management

Domain 6 Requirements	Testing Procedures
Note that DDKs used to decrypt account data in a Host System are the ONLY keys that can ever be managed in software per these 6H Requirements; all other cryptographic keys used in hybrid decryption solutions are managed in HSMs and are never present or managed in software.	
6H-1.1 The Data Decryption Keys (DDKs) used in software to decrypt account data must have defined usage limits. This can be achieved through the use of either one of the following approaches: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in NIST SP800-57, ISO TR 14742 and NIST SP800-131. The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the Host System. ***OR*** • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.	**6H-1.1.a** Examine documented key-management policies and procedures to verify that DDKs managed on the Host System meet one or both of the following: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in NIST SP800-57, ISO TR 14742 and NIST SP800-131. The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the host processing system. ***OR*** • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.
	6H-1.1.b Observe the key-management methods used to manage DDKs on the Host System to verify they meet one, or both of the above options.
6H-1.2 DDKs must be erased from the Host System volatile memory via a mechanism that ensures the key cannot be recovered or reconstructed.	**6H-1.2.a** Examine documented key-management policies and procedures to verify that the mechanism used to erase a DDK from the Host System volatile memory is sufficient to ensure the key cannot be recovered or reconstructed.
	6H-1.2.b Verify, through the use of forensic tools and/or methods, that the mechanism used to erase the DDK from the host volatile memory, is sufficient to ensure the key cannot be recovered or reconstructed.

Requirement 6H: For hybrid decryption solutions: Implement secure hybrid key management

Domain 6 Requirements	Testing Procedures
6H-1.3 If the DDK is generated from a master key, the following conditions apply: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generate the DDK must be dedicated to generating DDKs.	**6H-1.3.a** Examine key-management policies and procedures to verify that the following is required for any DDKs generated from a master key: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generated the DDK must be dedicated to generating DDKs.
	6H-1.3.b Observe key-generation processes for generating DDKs from a master key to verify: • A one-way derivation process is used. • The DDK is never generated as a variant of the HSM master file key. • The master key used to generate the DDK is dedicated to generating DDKs.
6H-1.4 The DDK must be encrypted between the HSM and the Host System, e.g., using a fixed transport key or a cryptographic protocol. The method of encryption used must maintain the security policy to which the HSM was approved (either FIPS140-2, Level 3 or higher, or approved to the PCI HSM standard).	**6H-1.4.a** Examine key-management policies and procedures to verify that DDKs must be encrypted between the HSM and the Host System.
	6H-1.4.b Examine HSM and Host System configurations to verify that DDKs are encrypted between the HSM and the Host System.
	6H-1.4.c Examine the HSM security policies and observe HSM implementations to verify that the method of encryption used maintains the security policy to which the HSM was approved.
6H-1.5 The encryption mechanism used to protect the DDK between the HSM and the Host System:	**6H-1.5** Verify the encryption mechanism used to protect the DDK between the HSM and the Host System, includes **6H-1.5.1** through **6H-1.5.2** Perform the following:
6H-1.5.1 The encryption key must be equal or greater in strength than the key it protects.	**6H-1.5.1.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is equal or greater in strength than the key it protects.
	6H-1.5.1.b Observe key-management processes to verify the encryption mechanism used to protect the DDK between the HSM and the Host System uses an encryption key that is equal or greater in strength than the key it protects.

Requirement 6H: For hybrid decryption solutions: Implement secure hybrid key management

Domain 6 Requirements	Testing Procedures
6H-1.5.2 The encryption key must be unique for each Host System.	**6H-1.5.2.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is unique for each Host System.
	6H-1.5.2.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is unique for each Host System.
6H-1.5.3 The encryption key must only be used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.	**6H-1.5.3.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.
	6H-1.5.3.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.
6H-1.5.4 The encryption key must have a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices	**6H-1.5.4.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices
	6H-1.5.4.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices

Requirement 6I: Component providers ONLY: report status to solution providers

Domain 6 Requirements	Testing Procedures

Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain (in conjunction with Domains 1 or 5 as applicable to the solution provider's services) for subsequent PCI listing of the component provider's device-management or decryption-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 device management or decryption 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).*

6I-1 For component providers performing key management in conjunction with device-management or decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.

6I-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:

- 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 **6F-2.1**

Note that 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.

6I-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:

- 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 6F-2.1

- **6I-1.1.b** Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following:
- Types/models of 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 **6F-2.1**

Domain 6 Normative Annex A: Symmetric-Key Distribution using Asymmetric Techniques

This normative annex contains detailed requirements that apply to remote key-establishment and distribution applications and is in addition to key- and equipment-management criteria stated in the main body of Domain 6. Remote key-distribution schemes shall be used for initial key loading only—i.e., establishment of a TDEA key hierarchy, such as a terminal master key. Standard symmetric-key-exchange mechanisms should be used for subsequent TMK, PEK, or other symmetric-key exchanges, except where a device requires a new key initialization due to unforeseen loss of the existing TMK. Using asymmetric techniques for routine key exchange can result in unnecessary exposure to man-in-the-middle attacks and should not be used.

These requirements pertain to two distinct areas covered separately in the two parts of this Annex.

- **A1 – Remote Key-Distribution Using Asymmetric Techniques Operations:** Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key-distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account data encryption..
- **A2 – Certification and Registration Authority Operations:** Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.
    - Certification Authority requirements apply to all entities (P2PE solution providers, P2PE component providers, and entities performing these functions on behalf of solution providers or component providers) signing public keys to be used for remote distribution of cryptographic keys, whether in X.509 certificate-based schemes or other designs, to allow for the required authentication of these signed public keys. For purposes of these requirements, a certificate is any digitally signed value containing a public key, where the term “digitally signed” refers to any cryptographic method used that enforces the integrity and authenticity of a block of data through the cryptographic processing of that block of data with a private key. The CA requirements apply only to methods that allow for the distribution and use of such signed public keys to multiple systems, and as such do not apply to systems that apply symmetric cryptography to keys for authentication (such as through the use of MACs).
    - The Certification Authority requirements are not intended to be applied to devices that sign their own keys, nor to key-loading systems where the key loading is not performed remotely and authentication is provided by another method—such as properly implemented dual control and key-loading device(s)—even if these systems involve the use of certificates.

The control objectives and security requirements are delineated as found in the preceding “Domain 6” section of this document, and are in addition to requirements for those entities performing transaction processing.

Unless otherwise specified, the term Certification Authority (CA) refers to any CA in the hierarchy, Root or SubCa.

A1 – Remote Key Distribution Using Asymmetric Techniques Operations

Requirement 6A: Account data is processed using equipment and methodologies that ensure they are kept secure.
No additional security requirements added for "Symmetric Key Distribution using Asymmetric Techniques."

Requirement 6B: Account-data keys and key management methodologies 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.
No additional security requirements added for "Symmetric Key Distribution using Asymmetric Techniques."

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 A1 Requirements	Testing Procedures
***6C-3** All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*	
6C-3.2 All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed except as noted in the main body of Domain 6 at Requirement **6C-3.1**.	**6C-3.2** Examine documented procedures to verify that all asymmetric keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed except as noted in the main body of Domain 6 at Requirement **6C-3.1**.
6C-3.3 Key sizes and algorithms must be in accordance with Annex C.	**6C-3.3** Observe key-generation processes to verify that all asymmetric keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 A1 Requirements	**Testing Procedures**
***6D-4** The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	
6D-4.3 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. Mutual authentication of the sending and receiving devices must be performed. ***Note:** Examples of this kind of validation include 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.*	**6D-4.3.a** Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: • 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.
	6D-4.3.b Interview applicable personnel to verify that mutual authentication of the sending and receiving devices is performed, as follows: • 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.
6D-4.4 Key-establishment and distribution procedures must be designed such that: • Within an implementation design, there shall 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.	**6D-4.4** Examine system and process documentation to verify that key-establishment and distribution procedures are designed such that: • There are no means available in the implementation design for “man-in-the-middle” attacks. • System implementations are designed to prevent replay attacks.
6D-4.5 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.	**6D-4.5** If key pairs are generated external to the device that uses the key pair, perform the following: • 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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 A1 Requirements	**Testing Procedures**
***6E-2** Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	
6E-2.4 POIs shall 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.	**6E-2.4.a** Examine documented procedures to verify 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; • POIs only communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.
	6E-2.4.b Interview responsible personnel and observe POI configurations to verify 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; • POIs only communicate with KDHs or key management, normal transaction processing, and certificate (entity) status checking.
6E-2.5 KDHs shall only communicate with POIs for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.	**6E-2.5.a** Examine documented procedures to verify that: • KDHs only communicate with POIs 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.
	6E-2.5.b Interview responsible personnel and observe KDH configurations to verify that: • 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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 A1 Requirements	**Testing Procedures**
***6E-3** Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	
6E-3.6 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.	**6E-3.6.a** Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate
	6E-3.6.b Interview responsible personnel and observe certificate issuing and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Certificates are replaced by generating a new key pair and requesting a new certificate. • Each key pair generated results in only one certificate.
6E-3.7 KDH private keys must not be shared between devices except for load balancing and disaster recovery.	**6E-3.7** Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.
6E-3.8 POI private keys must not be shared between devices.	**6E-3.8.a** Examine documented processes to verify that POI private keys are not permitted to be shared between devices.
	6E-3.8.b Inspect public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A1 Requirements	**Testing Procedures**
***6F-1** Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	
6F-1.4 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: • 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.	**6F-1.4.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.
	6F-1.4.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.

A2 – Certification and Registration Authority Operations

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6C-3 *All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*	
6C-3.2 All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed, except as noted in the main body of Domain 6 at Requirement **6C-3.1.**	**6C-3.2** Examine documented procedures to verify that all asymmetric keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed except as noted in the main body of Domain 6 at Requirement **6C-3.1**.
6C-3.3 Key sizes and algorithms must be in accordance with Annex C.	**6C-3.3** Observe key-generation processes to verify that all asymmetric keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6D-4 *The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	
6D-4.6 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.	**6D-4.6** If key pairs are generated external to the device that uses the key pair, perform the following: • 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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 A2 Requirements	**Testing Procedures**
***6E-3** Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	
6E-3.5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements. At all times, the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.	**6E-3.5** Interview personnel to determine whether production platforms are ever temporarily used for testing. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.
6E-3.6 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.	**6E-3.6.a** Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate
	6E-3.6.b Interview responsible personnel and observe certificate issuing and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Certificates are replaced by generating a new key pair and requesting a new certificate. • Each key pair generated results in only one certificate.
***6E.3.7** and **6E-3.8** not used in this Annex A2.*	
6E-3.9 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 *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.	**6E-3.9.a** Examine key-usage documentation and ensure that the usage is in accordance with the certificate policy.
	6E-3.9.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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 A2 Requirements	**Testing Procedures**
6E-3.9.1 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. ***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.*	**6E-3.9.1.a** Examine certificate policy and documented procedures to verify that: • Certificate signature keys, • Certificate status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs Must not be used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
	6E-3.9.1.b Interview responsible personnel and observe demonstration to verify that: • Certificate signature keys, • Status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs Are not used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
6E-3.9.2 CAs that issue certificates to other CAs must not be used to issue certificates to POIs.	**6E-3.9.2** 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.
6E-3.10 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.	**6E-3.10** 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.
6E-3.11 CA private keys must not be shared between devices except for load balancing and disaster recovery.	**6E-3.11** 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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 A2 Requirements	**Testing Procedures**
6E-3.12 The PKI used for remote key distribution must not be used for any other purpose, e.g., cannot be used for firmware or application authentication.	**6E-3.12.a** Interview responsible personnel to verify that the PKI is operated solely for the purposes of remote key distribution:
	6E-3.12.b Examine the documented certificate policy to verify that the CA is operated solely for the purposes of remote key distribution.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-1 *Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	
6F-1.4 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: • 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.	**6F-1.4.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.
	6F-1.4.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.
6F-2 *Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.*	
6F-2.6 Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.	**6F-2.6** Through the examination of documented procedures, interviews and observation confirm that Root CAs provide for segmentation of risk to address key compromise.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-2.7 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.	**6F-2.7.a** Examine documented procedures to verify that mechanisms are defined to respond to compromise of a CA. Verify the mechanisms include procedures to: • Revoke subordinate certificates, and • Notify affected entities.
	6F-2.7.b Interview responsible personnel to verify that the defined mechanisms to respond to compromise of a CA are in place and include: • Revoke subordinate certificates, and • Notify affected entities.
6F-2.7.1 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.	**6F-2.7.1.a** Examine documented procedures to verify that the following are required in the event a compromise is known or suspected: • 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.
	6F-2.7.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: • 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.
6F-2.7.2 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.	**6F-2.7.2.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.
	6F-2.7.2.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.
6F-2.7.3 Mechanisms (e.g., time stamping) must exist to prevent the usage of fraudulent certificates, once identified.	**6F-2.7.3.a** Examine documented procedures to verify that mechanisms are defined to prevent the usage of fraudulent certificates.
	6F-2.7.3.b Interview responsible personnel and observe implemented mechanisms to verify the prevention of the use of fraudulent certificates

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**

6F-2.7.4 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.	**6F-2.7.4.a** Examine documented procedures to verify that the following procedures are required in the event of a compromise:
	• 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.

	6F-2.7.4.b Interview responsible personnel to verify that the following procedures are performed in the event a compromise:
	• The CA notifies any superior CAs.
	• The CA notifies any subordinate CAs.
	• The CA performs a damage assessment to determine the need to either:
	  ○ Reissues and distributes certificates to affected parties, or
	  ○ Notifies the affected parties to apply for new certificates.

6F-2.8 Minimum cryptographic strength for the CA system shall be: • Root and subordinate CAs have a minimum RSA 2048 bits or equivalent; • EPP/PED devices and KDHs have a minimum RSA 1024 bits or equivalent. *Effective 1 January 2017, KDHs must use a minimum RSA 2048 bits or equivalent.* The key-pair lifecycle shall result in expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.	**6F-2.8.a** Interview appropriate personnel and examine documented procedures for the creation of these keys.
	6F-2.8.b Verify that the following minimum key sizes exist for RSA keys or the equivalent for the algorithm used as defined in Annex C: • 2048 for CAs • 1024 for KDHs and POI devices
	6F-2.8.c Verify that KDH keys expire every five years unless another mechanism exists to prevent the use of a compromised KDH private key.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
***6F-5** Access to secret and private cryptographic keys and key material must be:* a) *Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and* b) *Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*	
6F-5.2 All user access to material that can be used to construct secret and private keys (such as key components) must be directly attributable to an individual user (e.g., through the use of unique IDs).	**6F-5.2.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.
	6F-5.2.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.
6F-5.2.1 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.*	**6F-5.2.1.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.
	6F-5.2.1.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.
6F-5.3 The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include the following:	
6F-5.3.1 CA systems that issue certificates to other CAs and KDHs must be operated offline using a dedicated closed network (not a network segment). • The network must only be used for certificate issuance and/or revocation. • Outside network access shall exist only for the purposes of "pushing" certificate-status information to relying parties (e.g., KDHs).	**6F-5.3.1** Examine network diagrams and observe network and system configurations to verify: • 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).
6F-5.3.2 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).	**6F-5.3.2** Examine software update processes to verify that local console access is used for all CA or RA software updates.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.3.3 Non-console access must use two-factor authentication. This also applies to the use of remote console access.	**6F-5.3.3** Examine remote-access mechanisms and system configurations to verify that all non-console access, including remote access, requires two-factor authentication.
6F-5.3.4 Non-console user access to the CA or RA system environments shall 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.*	**6F-5.3.4.a** Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions.
	6F-5.3.4.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.
6F-5.3.5 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.*	**6F-5.3.5.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.
	6F-5.3.5.b Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.
6F-5.4 The CA shall 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 shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).	**6F-5.4.a** Examine documented procedures to verify they include following: • 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)
	6F-5.4.b Observe CA operations and interview responsible personnel to verify: • 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)

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.5 All CA systems that are not operated strictly offline must be hardened to prevent insecure network access, to include: • 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.	**6F-5.5.a** Examine system documentation to verify the following is required: • 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.
	6F-5.5.b For a sample of systems, examine documentation supporting the enablement of active services and ports, and observe system configurations to verify: • 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.
6F-5.5.1 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 required and otherwise must be disabled from login.	**6F-5.5.1.a** Examine documented procedures to verify that: • 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.
	6F-5.5.1.b Examine system configurations and interview responsible personnel to verify that: • 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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.5.2 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.	**6F-5.5.2.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.
	6F-5.5.2.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.
6F-5.6 Audit trails must include but not be limited to the following: • All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, and 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	**6F-5.6.a** Examine system configurations and audit trails to verify that all key-management operations are logged.
	6F-5.6.b For a sample of key-management operations, examine audit trails to verify they include: • 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
6F-5.6.1 Audit logs must be archived for a minimum of two years.	**6F-5.6.1** Examine audit trail files to verify that they are archived for a minimum of two years.
6F-5.6.2 Records pertaining to certificate issuance and revocation must, at a minimum, be retained for the life of the associated certificate.	**6F-5.6.2.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.
	6F-5.6.2.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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.6.3 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: • 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.	**6F-5.6.3.a** Examine audit trails to verify that logical events are divided into operating-system and CA application events.
	6F-6.3.b Examine a sample of operating-system logs to verify they contain the following information: • 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.
	6F-5.6.3.c Examine a sample of application logs to verify they contain the following information: • 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.
6F-5.7 CA application logs must use a digital signature or a symmetric MAC (based on one of the methods stated in *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration. 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.	**6F-5.7.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 *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration.
	6F-5.7.b Review 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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.7.1 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: • 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.	**6F-5.7.1.a** Examine network and system configurations to verify that certificate-processing system components operated online are protected from unauthorized access by firewall(s). **6F-5.7.1.b** Examine firewall configurations for verify they are configured to: • 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.
6F-5.7.2 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.	**6F-5.7.2.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. **6F-5.7.2.b** Verify that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.8 Implement user-authentication management for all system components as follows:	
6F-5.8.1 Initial, assigned passphrases are pre-expired (user must replace at first logon).	**6F-5.8.1** 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.
6F-5.8.2 Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.	**6F-5.8.2.a** For a sample of system components, examine user ID lists to verify the following: • 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.
	6F-5.8.2.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.
	6F-5.8.2.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.
6F-5.8.3 If passwords are used, system-enforced expiration life must not exceed 30 days and a minimum life at least one day.	**6F-5.8.3** 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 30 days and have a minimum life of at least one day.
6F-5.8.4 Passwords must have a minimum length of eight characters using a mix of alphabetic, numeric, and special characters.	**6F-5.8.4** 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.
6F-5.8.5 Limit repeated access attempts by locking out the user ID after not more than five attempts.	**6F-5.8.5** 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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.8.6 Authentication parameters must require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.	**6F-5.8.6** 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.
6F-5.8.7 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.	**6F-5.8.7** 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.
6F-5.8.8 The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.	**6F-5.8.8.a** Review policies and procedures and interview personnel to determine that the embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.
	6F-5.8.8.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.
6F-5.8.9 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. ***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.*	**6F-5.8.9.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.
	6F-5.8.9.b Examine token-configuration settings to verify parameters are set to require PINs/passwords be at least eight decimal digits in length, or equivalent.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-5.9 Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.	**6F-5.9.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.
	6F-5.9.b For a sample of critical systems, review the time-related system parameters to verify that system clocks and times are synchronized for all systems involved in key-management operations.
	6F-5.9.c If a manual process is defined, verify that the documented procedures require that it occur at least quarterly.
	6F-5.9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.
***6F-8** Documented procedures must exist and must be demonstrably in use for all key-administration operations.*	
6F-8.2 CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.	**6F-8.2.a** Examine documented procedures to verify: • CA operations must be dedicated to certificate issuance and management. • All physical and logical CA system components must be separated from key-distribution systems.
	6F-8.2.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.
	6F-8.2.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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-8.3 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.) • The CPS must be consistent with the requirements described within this document. • The CA shall operate in accordance with its CPS. ***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.* The CPS must be consistent with the requirements described within this document. The CA shall operate in accordance with its CPS.	**6F-8.3.a** Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document. **6F-8.3.b** Examine documented operating procedures to verify they are defined in accordance with the CPS. **6F-8.3.c** Interview personnel and observe CA processes to verify that CA operations are in accordance with its CPS.
6F-8.4 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.)	**6F-8.4** Examine documented certificate policy to verify that the CA has one in place.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6F-8.5 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 with the same secure area. These procedures must include at a minimum, two or more of the following for KDH certificate requests: • 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.	**6F-8.5.a** Examine documented procedures to verify they include validating the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key. **6F-8.5.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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6F-8.5.1 For CA and KDH certificate-signing requests, including certificate or key-validity status changes—e.g., revocation, suspension, replacement—verification must include validation that: • 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.	**6F-8.5.1.a** Examine documented procedures to verify that certificate-signing requests, including certificate or key-validity status changes, require validation that: • 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.
	6F-8.5.1.b Observe certificate-signing requests, including certificate or key-validity status changes, to verify they include validation that: • 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.
6F-8.5.2 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.	**6F-8.5.2** Examine documentation and audit trails to verify that the identification of entities is retained for the life of the associated certificates: • For all certificates issued • For all certificates whose status had changed

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
***6G-3** Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key, or signing applications to be loaded onto a POI device, must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:* *a) Dual access controls required to enable the key-encryption function* *b) Physical protection of the equipment (e.g., locked access to it) under dual control* *c) Restriction of logical access to the equipment*	
6G-3.2.1 The certificate-processing operations center must implement a three-tier physical security boundary, as follows: • 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.	**6G-3.2.1.a** Examine physical security policies to verify three tiers of physical security are defined as follows: • 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
	6G-3.2.1.b Observe the physical facility to verify three tiers of physical security are implemented as follows: • 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
Level 1 Barrier	
6G-3.2.2 The entrance to the CA facility/building must include the following controls:	
6G-4.2.2.1 The facility entrance only allows authorized personnel to enter the facility.	**6G-3.2.2.1.a** Examine physical-security procedures and policies to verify they require that the facility entrance allows only authorized personnel to enter the facility.
	6G-3.2.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed to enter the facility.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6G-3.2.2.2 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.	**6G-3.2.2.2.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.
	6G-3.2.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.
6G-3.2.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.	**6G-3.2.2.3.a** Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.
	6G-3.2.2.3.b Observe the facility entrance and observe personnel entering the facility to verify that visitors are authorized and registered in a logbook.
Level 2 Barrier	
6G-3.2.3 The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.	**6G-3.2.3.a** Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the Level 2 barrier/entrance.
	6G-3.2.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.
6G-3.2.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.	**6G-3.2.3.1.a** Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.
	6G-3.2.3.1.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.
6G-3.2.3.2 Access logs must record all personnel entering the Level 2 environment. ***Note:*** *The logs may be electronic, manual, or both.*	**6G-3.2.3.2.a** Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.
	6G-3.2.3.2.b Observe personnel entering the Level 2 barrier and review corresponding access logs to verify that all entry through the Level 2 barrier is logged.
6G-3.2.4 The Level 2 entrance must be monitored by a video-recording system.	**6G-3.2.4.a** Observe the Level 2 entrance to verify that a video-recording system is in place.
	6G-3.2.4.b Review a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
Level 3 Barrier	
6G-3.2.5 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.*	**6G-3.2.5.a** Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.
	6G-3.2.5.b Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.
	6G-3.2.5.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.
6G-3.2.5.1 Doors to the Level 3 area must have locking mechanisms.	**6G-3.2.5.1** Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.
6G-3.2.5.2 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.*	**6G-3.2.5.2.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
	6G-3.2.5.2.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.
6G-3.2.6 Documented procedures must exist for: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical	**6G-3.2.6.a** Examine documented procedures to verify they include the following: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical
	6G-3.2.6.b Interview responsible personnel to verify that the documented procedures are followed for: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6G-3.2.6.1 All authorized personnel with access through the Level 3 barrier must: • Have successfully completed a background security check. • Be assigned resources (staff, dedicated personnel) of the CA operator with defined business needs and duties. ***Note:*** *This requirement applies to all personnel with pre-designated access to the Level 3 environment.*	**6G-3.2.6.1.a** Examine documented policies and procedures to verify they require personnel authorized as having access through the Level 3 barrier to: • Have successfully completed a background security check. • Be assigned resources of the CA operator with defined business needs and duties.
	6G-4.2.6.1.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.
	6G-3.2.6.1.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.
6G-3.2.6.2 Other personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.	**6G-3.2.6.2.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.
	6G-3.2.6.2.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.
6G-3.2.7 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: 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.*	**6G-3.2.7.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.
	6G-3.2.7.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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6G-3.2.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated.	**6G-3.2.7.1.a** Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.
	6G-3.2.7.1.b Observe enforcement mechanism configuration to verify it is automated.
6G-3.2.7.2 The system must enforce anti-pass-back.	**6G-3.2.7.2.a** Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.
	6G-3.2.7.2.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.
6G-3.2.7.3 Dual occupancy requirements are managed using electronic (e.g., badge and/or biometric) systems.	**6G-3.2.7.3.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.
	6G-3.2.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic systems.
6G-3.2.7.4 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.	**6G-3.2.7.4.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.
	6G-3.2.7.4.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.
	6G-3.2.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.
6G-3.2.8 Access to the Level 3 room must create an audit event, which must be logged.	**6G-3.2.8** 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.
6G-3.2.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel	**6G-3.2.8.1** 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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6G-3.2.9 The Level 3 environment must be monitored as follows:	
6G-3.2.9.1 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.*	**6G-3.2.9.1.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.
	6G-3.2.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.
	6G-3.2.9.1.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.
6G-3.2.9.2 The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.	**6G-3.2.9.2** Examine monitoring system configurations to verify; • The system records to time-lapse VCRs or similar mechanisms. • A minimum of five frames are recorded every three seconds.
6G-3.2.9.3 Continuous or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (e.g., when infrared cameras are used).*	**6G-3.2.9.3.a** Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for each camera monitoring the environment.
	6G-3.2.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.
6G-3.2.9.4 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.	**6G-3.2.9.4.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.
	6G-3.2.9.4.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.
6G-3.2.9.5 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.	**6G-3.2.9.5.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.
	6G-3.2.9.5.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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6G-3.2.9.6 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 to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**6G-3.2.9.6.a** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.
	6G-3.2.9.6.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.
6G-3.2.9.7 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 area) 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.	**6G-3.2.9.7** Examine backup techniques utilized to ensure that: • Backups are securely stored in a separate location from the primary. • Ensure that segregation is maintained between users and administrators of the system.
6G-3.3 The environment must have continuous (24/7) intrusion-detection systems in place, which protects the secure area by motion detectors when unoccupied.	**6G-3.3.a** Examine security policies and procedures to verify they require: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment. • Motion detectors must be active when the environment is unoccupied.
	6G-3.3.b Examine intrusion-detection system configurations to verify: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place. • Motion detectors are active when the environment is unoccupied.
6G-3.3.1 Any windows in the secure area must be locked and protected by alarmed sensors.	**6G-3.3.1.a** Observe all windows in the secure areas to verify they are locked and protected by alarmed sensors.
	6G-3.3.1.b Examine configuration of window sensors to verify that the alarm mechanism is active.
	6G-3.3.1.c Test at least one window (if they can be opened) to verify that the alarms function appropriately.
6G-3.3.2 Any windows or glass walls must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**6G-3.3.2** Observe all windows and glass walls in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 A2 Requirements	Testing Procedures
6G-3.3.3 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 area. The system must be configured to activate within 30 seconds.	**6G-3.3.3.a** Examine security system configurations to verify: • 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.
	6G-3.3.3.b Verify the IDS and alarms function correctly via: • 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.
6G-3.3.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.	**6G-3.3.4** Examine security-system configurations to verify that an alarm event is generated for: • Unauthorized entry attempts • Actions that disable the intrusion-detection system
6G-3.4 All personnel (including CA personnel and visitors) must sign an access logbook when entering the Level 3 environment. ***Note:*** *This log is in addition to those provided by the access-control system.*	**6G-3.4.a** Examine security policies and procedures to verify they require all personnel (including CA personnel and visitors) to sign an access logbook when entering the Level 3 environment.
	6G-3.4.b On the escorted entry into the secure area, observe that all personnel appropriately sign the access logbook and that all escorted visitors are required to sign the access logbook.
6G-3.4.1 The access log must include the following details: • 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	**6G-3.4.1** Examine the access logbook to verify it contains the following information: • 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
6G-3.4.2 The logbook must be maintained within the Level 3 secure environment.	**6G-3.4.2** Observe the location of the access logbook and verify that it is maintained within the Level 3 secure environment.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6G-3.5 All access-control and monitoring systems (including intrusion-detection systems) are powered through an uninterruptible power source (UPS).	**6G-3.5** 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.
6G-3.6 All alarm events must be documented.	**6G-3.6.a** Examine security policies and procedures to verify they require that all alarm events be logged.
	6G-3.6.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
6G-3.6.1 An individual must not sign off on an alarm event in which they were involved.	**6G-3.6.1.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.
	6G-3.6.1.b Determine who is authorized to sign off on alarm events.
	6G-3.6.1.c For a sample of documented alarm events, review the record to verify that personnel authorized to sign off on alarm events were not also the cause of that event.
6G-3.6.2 The use of any emergency entry or exit mechanism must cause an alarm event.	**6G-3.6.2.a** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
	6G-3.6.2.b Conduct a test to verify the mechanisms work appropriately.
6G-3.6.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.	**6G-3.6.3.a** Review documented procedures to verify they require that all alarms for physical intrusion must be responded to within 30 minutes by personnel assigned security duties.
	6G-3.6.3.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.
	6G-3.6.3.c Conduct a test to verify the appropriate response occurs.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 A2 Requirements	**Testing Procedures**
6G-3.7 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. ***Note:*** *This may be done by either automated or manual mechanisms.*	**6G-3.7.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.
	6G-3.7.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	6G-3.7.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
6G-3.7.1 If a manual synchronization process is used, synchronization must occur at least quarterly; and documentation of the synchronization must be retained for at least a one-year period.	**6G-3.7.1.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.
	6G-4.7.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.

Domain 6 Normative Annex B: Key-Injection Facilities

The term key-injection facility (KIF) describes those entities that perform key injection of POI devices used for account data encryption and key injection of HSMs used for decryption. Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer or vendor. *This Annex contains the specific requirements that apply to key-injection facilities, and includes **all** applicable P2PE criteria from the general Domain 6 for entities that provide only key-injection services.* Solution providers and other entities that perform key injection services in addition to other P2PE solution functions are required to meet all requirements stipulated in general Domain 6 which include key injection requirements; therefore, these entities are not required to additionally meet the requirements stipulated in Annex B.

Key-injection systems that allow clear-text secret and/or private keys and/or their components to appear in unprotected memory (e.g., within a computer and outside of the secure boundary of a secure cryptographic device) are inherently less secure. Any such systems are subject to additional controls as delineated in the criteria in this annex. The payment brands may establish dates by which all key-injection facilities providing key-injection services to multiple entities shall have to use secure cryptographic hardware for key-injection.

Key-injection facilities that are engaged in either or both of the following must also meet the criteria delineated in Annex A:

1. Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.
2. Remote distribution of symmetric keys using asymmetric techniques to transaction originating devices. These criteria pertain to the characteristics of the actual key-distribution methodology implemented.

Requirement 6A: Account data is processed using equipment and methodologies that ensure they are kept secure.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6A-1** Account data is processed in equipment that conforms to requirements for secure cryptographic devices (SCDs). Account data never appears in the clear outside of an SCD.*	
6A-1.2 Key-injection facilities must only inject keys into equipment that conforms to the requirements for SCDs. Key-injection platforms and systems shall include hardware devices for managing (e.g., generating and storing) the keys that conform to the requirements for SCDs.	**6A-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.
	6A-1.2.b Examine key-injection platforms and systems used for managing cryptographic keys to verify they conform to the requirements for SCDs.
6A-1.3 Ensure that all hardware security modules (HSMs) are either: • FIPS140-2 Level 3 or higher certified, or • PCI approved.	**6A-1.3.a** For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3, or higher. Refer 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.
	6A-1.3.b Examine documented procedures and interview personnel to verify that all decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified above.

Requirement 6A: Account data is processed using equipment and methodologies that ensure they are kept secure.	
Domain 6 Annex B Requirements	**Testing Procedures**
6A-1.4 The approval listing must match the deployed devices in the following characteristics: • Vendor name • Model name and number • Hardware version number • Firmware version number • The PCI PTS HSM or FIPS 140 version with which the model complies • The PCI PTS 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	**6A-1.4.a** For all PCI-approved HSMs used, examine HSM devices and review the *PCI SSC list of Approved PCI PTS Devices* to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The PCI PTS HSM or FIPS 140 version with which the model complies • The PCI PTS or FIPS 140 Approval Number • Any applications, including application version number, resident within the device which were included in the PTS assessment
	6A-1.4.b For all FIPS-approved HSMs used, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The PCI PTS HSM or FIPS 140 version with which the model complies • The PCI PTS or FIPS 140 Approval Number

Requirement 6A: Account data is processed using equipment and methodologies that ensure they are kept secure.	
Domain 6 Annex B Requirements	**Testing Procedures**
6A-1.5 The KIF platform provider maintains documentation detailing the distributed KIF architecture and key-management flows**.** The platform provider must: • Maintain current documentation that describes or illustrates the architecture of the KIF, including all distributed KIF functionality. • Maintain documentation detailing the flow of keys from the key generation, through the distributed functionality to the destination device. The documentation should indicate how personnel interaction and inventory management is integrated into the flow.	**6A-1.5.a** Interview relevant personnel and review documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the KIF.
	6A-1.5.b Interview relevant personnel and review 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.
	6A-1.5.c Examine the key-management flows and interview personnel to verify: • 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

Requirement 6B:	***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.***

Domain 6 Annex B Requirements	Testing Procedures
6B-1 *All keys and key components are generated using an approved random or pseudo-random process.*	
6B-1.1 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. Cryptographic keys or key components must be generated by one of the following: • An approved key-generation function of a PCI-approved HSM or POI • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM • An approved random number generator that has been certified by an independent laboratory to comply with *NIST SP 800-22* ***Note:*** *Random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key generation relies upon good quality, randomly generated values.*	**6B-1.1.a** Examine key-management policy document and to verify that it requires that all devices used to generate cryptographic keys meet one of the following • An approved key-generation function of a PCI-approved HSM • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM or • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22.*
	6B-1.1.b Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM or • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*
	6B-1.1.c Verify devices used for key generation are those as noted above, including validation of the firmware used.
6B-2 *Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*	
6B-2.1 Implement security controls, including dual control and tamper protection to prevent the unauthorized disclosure of keys/key components.	**6B-2.1** Perform the following:
6B-2.1.1 Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.	**6B-2.1.1.a** Examine documented procedures to verify the following: • 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. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.

Requirement 6B:	***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.***
Domain 6 Annex B Requirements	**Testing Procedures**
	6B-2.1.1.b Observe key-generation processes and interview responsible personnel to verify: • 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. • There is no mechanism including connectivity that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.
6B-2.1.2 There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key. ***Note:*** *Full-length key components or key shares derived using a recognized key-splitting algorithm are not considered key parts and do not provide any information regarding the actual cryptographic key.*	**6B-2.1.2.a** Observe the 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.
	6B-2.1.2.b Examine key-generation logs to verify that at least two individuals performed the key-generation processes.
6B-2.1.3 Devices used for generation of clear-text key components that are output in the clear must be powered off when not in use. 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.	**6B-2.1.3** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate clear-text key components be powered off when not in use; or • If logically partitioned for concurrent use in other processes, the key-generation capabilities are disabled when not in use and other activities are continuing.
6B-2.1.4 Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (e.g., unnecessary cables).	**6B-2.1.4.a** Review documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering, prior to use.
	6B-2.1.4.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.

Requirement 6B:	***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.***
Domain 6 Annex B Requirements	**Testing Procedures**
6B-2.1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area. It must not be feasible to observe the key-component/key-generation process whereby clear-text keying material is observable either directly or via camera monitoring.	**6B-2.1.5.a** Examine documentation to verify that physical security controls are defined to ensure the key component/key-generation process cannot be observed or accessed by unauthorized personnel.
	6B-2.1.5.b Observe the physical security controls to verify that key-component/key-generation process cannot be observed or accessed by unauthorized personnel.
6B-2.2 Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory. *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 loading. Computers that have been specifically purposed and used solely for key loading are permitted for use if all other requirements can be met, including those of **6B-1** and the controls defined in Requirements at **6D-2** of this Annex B.* *Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.* *Single-purpose computers with an installed SCD where clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) meet this requirement. Where the components pass through unprotected memory of the PC, it must meet **6D-2** of this Annex B.* ***Note**: See **6D-2**.*	**6B-2.2.a** Examine documented procedures 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 unprotected memory.
	6B-2.2.b Observe generation process and review vendor 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 unprotected memory.
	6B-2.2.c Where single-purpose computers with an installed SCD are used, verify that either: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) or • Where clear keying material passes through unprotected memory of the PC, the PC requirements of **6D-2** of this Annex B are met.

Requirement 6B:	***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.***

Domain 6 Annex B Requirements	Testing Procedures
6B-2.3 Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that: • Only approved key custodians can observe their own key component. • Tampering can be visually detected. Printers used for this purpose must not be used for other purposes.	**6B-2.3.a** Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed immediately after printing such that: • Only approved key custodians can observe their own key component. • Tampering can be visually detected. Printers used for this purpose are not used for other purposes.
	6B-2.3.b Observe processes for printing key components to verify 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.
	6B-2.3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be visually detected.
6B-2.4 Any residue that may contain clear-text keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key, to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual. *Examples of where such key residue may exist include (but are not limited to):* • *Printing material, including ribbons and paper waste* • *Memory storage of a key-loading device, after loading the key to a different device or system* • *Other types of displaying or recording*	**6B-2.4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures are implemented to ensure the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • 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 that will use the key.
	6B-2.4.b Observe the destruction process of the identified key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed immediately after generation. • 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 that will use the key.

Requirement 6B:	***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.***

Domain 6 Annex B Requirements	Testing Procedures
6B-2.5 Asymmetric-key pairs must either be: • Generated by the device that will use the key pair; or • If generated externally, the private key of 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.	**6B-2.5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.
	6B-2.5.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (e.g., zeroized) immediately after the transfer to the device that will use the key pair.
6B-2.6 Policy and procedures must exist to ensure that clear-text private or secret keys or their components are prohibited from being transmitted across insecure channels. These include but are not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text secret or private 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 manuals	**6B-2.6.a** Examine documented policy and procedures to verify that clear-text private or secret keys or their components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Conveying clear-text private or secret key components without containing them within tamper-evident, authenticable packaging • Writing key or component values into startup instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manual

Requirement 6B:	***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.***
Domain 6 Annex B Requirements	**Testing Procedures**
	6B-2.6.b From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Conveying clear-text private or secret key components without containing them within tamper-evident, authenticable packaging • Writing key or component values into startup instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manual
***6B-3** Documented procedures must exist and must be demonstrably in use for all key-generation processing.*	
6B-3.1 Written key-creation procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of those procedures. All key-creation events performed by a key-injection facility must be documented. Procedures for creating all keys must be documented.	**6B-3.1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations.
	6B-3.1.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.
	6B-3.1.c Observe key-generation ceremonies whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.
6B-3.2 Logs must exist for the generation of higher-level keys such as KEKs exchanged with other organizations and MFKs and BDKs.	**6B-3.2.a** Examine documented key-generation procedures to verify that all 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.
	6B-3.2.b Observe demonstrations for all types of key-generation events to verify that all key-generation events are logged.
	6B-3.2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6C-1 *Secret or private keys shall be transferred by:* *a) Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or* *b) Transmitting the key in ciphertext form.* *Public keys must be conveyed in a manner that protects their integrity and authenticity.*	
*Keys conveyed **to** a key-injection facility must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:* • *Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method;* • *Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf);* • *Terminal master keys (TMKs) used in the master key/session key key-management method;* • *PIN-encryption keys used in the fixed-transaction key method;* • *Public keys used in remote key-establishment and distribution applications;* • *Private asymmetric keys for use in remote key-loading systems.* *Keys conveyed **from** a key-injection facility (including facilities that are device manufacturers) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:* • *Digitally signed HSM-authentication public key(s) signed by a device manufacturer's private key and subsequently loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable);* • *Device manufacturer's authentication key loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable).*	

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures

6C-1.1 Keys must be transferred either encrypted or within an SCD. If clear text outside of an SCD, keys must be transferred as two or more key shares or full-length components using different communication channels, or within an SCD.
 	
Clear-text key components may be transferred 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.
  ○ Ensure that details of the serial number of the package are conveyed transmitted separately from the package itself.
  ○ Ensure that 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 to convey components, the mechanisms or data (e.g., PIN) to obtain the key component from the SCD must be conveyed using a separate communication channel from the SCD, or it must be conveyed in the same manner as a paper component. SCDs must be inspected for signs of tampering.
 	
(continued on next page)
	6C-1.1.a Determine whether keys are transmitted encrypted, or as clear-text components, or within an SCD.
	
	6C-1.1.b If key components are ever transmitted in clear-text using pre-numbered tamper-evident mailers, perform the following:
	• Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself.
	• Observe the method used to transport clear-text key components using tamper-evident mailers and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.
	• Examine documented procedures to verify that cryptographic-key components are transferred using different communications channels.
	• Examine records of key conveyances and interview responsible personnel to verify that cryptographic key components are transferred using different communications channels.
	• Examine documented procedures to verify that serial numbers are verified prior to the usage of the keying material.
	
	6C-1.1.c Where SCDs are used to convey components, perform the following:
	• Examine documented procedures to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels.
	• Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering.
	• Examine records of key transfers and interview responsible personnel to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6C-1.1 *(continued)* • Where an SCD (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. *Where an SCD (HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual-control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering.* ***Note:*** *Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.*	**6C-1.1.d** Where SCDs are conveyed with pre-loaded secret and/or private keys, perform the following: • Examine documented procedures to verify that the SCD requires dual-control mechanisms to become operational. • Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering. • Examine records of key transfers and interview responsible personnel to verify that the mechanisms make the SCD operational are conveyed using separate communication channels.
6C-1.2 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 sufficient to form the necessary threshold to derive the key. *E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.*	**6C-1.2.a** Examine documented procedures to verify they include controls to ensure that no single person can ever have 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: • 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 components or shares sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a 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 of this key that is sufficient to form the necessary threshold to derive the key.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
	6C-1.2.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can ever have 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: • 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.
6C-1.3 E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) 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 unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear-text of any encrypted text or files conveyed through those systems. Other similar mechanisms, such as SMS, fax, or telephone shall not be used to convey clear-text key values.	**6C-1.3** Validate through interviews, observation, and logs that e-mail, SMS, fax, or telephone or similar communication is not used as means to convey secret or private keys or key components.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6C-1.4 Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of public-key certificates as defined in Annex A that are created by a trusted CA that meets the requirements of Annex A. • A hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 • Be within an SCD ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.*	**6C-1.4** For all methods used to convey public keys, perform the following: • Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity such as: ○ Use of public-key certificates created by a trusted CA that meets the requirements of Annex A ○ A hash of the public key sent by a separate channel (e.g., mail) ○ Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 ○ Be within an SCD • Observe the process for conveying public keys and interview responsible personnel to verify that self-signed certificates must not be used as the sole method of authentication. • Observe the process for conveying public keys and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6C-2 *During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.* *Sending and receiving entities are equally responsible for the physical protection of the materials involved.*	
Key components conveyed to and from a key-injection facility must be conveyed in compliance with these requirements. Such key components include but are not limited to those for key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf), or key components for the BDKs themselves, and terminal master keys used in the master key/session key key-management method.	
6C-2.1 Any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • Locked in a security container (including tamper-evident, authenticable packaging) in such a way that unauthorized access to it would be detected, or • Contained within a physically secure SCD. ***Note:*** *No single person shall be able to access or use all components or a quorum of shares of a single secret or private cryptographic key.*	**6C-2.1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, • 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 and unauthorized access to it would be detected, or • Contained within a physically secure SCD.
	6C-2.1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text secret or private key component/share is at all times either: • Under the continuous supervision of a person with authorized access to this component, • Locked in a security container (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it and unauthorized access to it would be detected, or • Contained within a physically secure SCD.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6C-2.2 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 must result in the destruction and replacement of: • The set of components • Any keys encrypted under this (combined) key	**6C-2.2.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.
	6C-2.2.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.
	6C-2.2.c Verify documented procedures require that any sign of package tampering results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
	6C-2.2.d Interview responsible personnel and observe processes to verify that, if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
6C-2.3 Only the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.	**6C-2.3.a** Verify that a list(s) of key custodians (and designated backup(s)) authorized to have physical access to key components prior to transmittal or upon receipt of a component is defined and documented.
	6C-2.3.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 transmittal or upon receipt.
	6C-2.3.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.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6C-2.4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal. • Check tamper-evident packaging upon receipt for signs of tamper prior to opening the tamper-evident, authenticable packaging containing key components. • Check the serial number of the tamper-evident packing upon receipt of a component package.	**6C-2.4.a** Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packing upon receipt of a component package.
	6C-2.4.b Observe implemented mechanisms and processes to verify that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packing upon receipt of a component package.
6C-2.5 Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers. ***Note:*** *Numbered courier bags are not sufficient for this purpose*	**6C-2.5** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
***6C-3** All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.*	
Key-encryption keys used to convey keys to a key-injection facility must be (at least) as strong as any key transmitted or conveyed. Such keys include but are not limited to, key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf).	
6C-3.1 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. • DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. • A double- or triple-length DEA key must not be encrypted with a DEA key of a lesser strength. • TDEA keys shall not be used to protect AES keys. • TDEA keys shall not be used to encrypt keys greater in strength than 112 bits. • RSA keys encrypting keys greater in strength than 80 bits shall have bit strength at least 112 bits.	**6C-3.1.a** Examine documented procedures to verify 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.

	6C-3.1.b Observe key-generation processes to 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 below for RSA keys used for key transport.
	• Interview appropriate personnel and examine documented procedures for the creation of these keys.
	• Using the table in Annex C, validate the respective key sizes for DEA, RSA, Elliptic Curve, DSA, and Diffie Hellman algorithms where used for key encryption.
	• Verify that:
	  ○ DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
	  ○ A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength.
	  ○ TDEA keys are not used to protect AES keys.
	  ○ TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.
	  ○ RSA keys encrypting keys greater in strength than 80 bits have bit strength at least 112 bits.

	6C-3.1.c Examine system documentation and configuration files to validate the above, including HSM settings.

Requirement 6C: Keys are conveyed or transmitted in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6C-4** Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.*	
6C-4.1 Written procedures must exist and be known to all affected parties.	**6C-4.1.a** Verify documented procedures exist for all key transmission and conveyance processing.
	6C-4.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.
6C-4.2 Methods used for the conveyance or receipt of keys must be documented.	**6C-4.2** Verify documented procedures include all methods used for the conveyance or receipt of keys.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
***6D-1** Secret and private keys must be input into hardware (host) security modules (HSMs) and Point of Interaction (POI) devices in a secure manner.* a) *Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.* b) *Key-establishment techniques using public-key cryptography must be implemented securely.*	
Key-injection facilities must load keys using dual control and for clear-text secret and private keys, split knowledge. Such keys include, but are not limited to: • *Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method;* • *Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is injecting keys on their behalf);* • *Terminal master keys (TMKs) used in the master key/session key key-management method;* • *PIN-encryption keys used in the fixed-transaction key method;* • *Master keys for key-injection platforms and systems that include hardware devices (SCDs) for managing (e.g., generating and storing) the keys used to encrypt other keys for storage in the key-injection platform system;* • *Public and private key pairs loaded into the POIs for supporting remote key-establishment and distribution applications;* • *Digitally signed POI public key(s) signed by a device manufacture's private key and subsequently loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable). Dual control is not necessary where other mechanisms exist to validate the authenticity of the key, such as the presence in the device of an authentication key;* • *Device manufacturer's authentication key (e.g., vendor root CA public key) loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable).*	
6D-1.1 The loading of secret or private keys, when loaded from the individual key components, must be managed 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.*	**6D-1.1.a** Review documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.
	6D-1.1.b Interview appropriate personnel to determine the number of key components for each manually loaded key, and the methodology used to form the key.
	6D-1.1.c Witness a structured walk-through/demonstration of various key-loading processes for all key types (MFKs, TMKs, PEKs. etc.). Verify the number and length of the key components to information provided through verbal discussion and written documentation.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
	6D-1.1.d Verify that the process includes the entry of individual key components by the designated key custodians.
	6D-1.1.e Ensure key-loading devices can only be accessed and used under dual control.
6D-1.2 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.	**6D-1.2** Examine logs of access to security containers for key components to verify that only the authorized custodian(s) have accessed. Compare the number on the current tamper-evident authenticable bag for each component to the last log entry for that component.
6D-1.3 The loading of clear-text cryptographic keys using a key-loading device requires dual control to authorize any key-loading session. It shall not be possible for a single person to use the key-loading device to load clear keys alone. Dual control must be implemented using one or more of, but not limited to, the following techniques: • Two or more passwords of five characters or more (vendor default values must be changed), • Multiple cryptographic tokens (such as smartcards), or physical keys, • Physical access controls *Note that for devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.*	**6D-1.3.a** Examine documented procedures for loading of clear-text cryptographic keys, including public keys, to verify they require dual control to authorize any key-loading session.
	6D-1.3.b For all types of production SCDs, observe processes for loading clear-text cryptographic keys, including public keys, to verify that dual control is required to authorize any key-loading session. Verify that any passwords used are a minimum of five characters.
	6D-1.3.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.
	6D-1.3.d Ensure that any default dual-control mechanisms (e.g., default passwords—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.
6D-1.4 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. *Note that 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.* The resulting key must only exist within the SCD.	**6D-1.4.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.
	6D-1.4.b Examine key-component lengths or device configuration settings to verify that key components used to create a key are the same length as the resultant key.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-1.5 Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.	**6D-1.5** Examine vendor documentation describing options for how the HSM MFK is created. Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.
6D-1.6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.	**6D-1.6** Through 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,
6D-1.7 The initial terminal master key (TMK) 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 may use techniques described in this documents such as: • Asymmetric techniques • Manual techniques • The existing TMK to encrypt the replacement TMK for download. Keys shall not be reloaded by any methodology in the event of a compromised device, and must be withdrawn from use.	**6D-1.7.a** Examine documented procedures for the loading of TMKs to verify that they require asymmetric key-loading techniques or manual techniques for initial loading.
	6D-1.7.b Examine documented procedures to verify that keys are prohibited from reloading or reuse wherever suspected of being compromised and are withdrawn from use.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-1.8 If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, these must meet the requirements detailed in Annex A of this document. For example: A public-key technique for the distribution of symmetric secret keys must: • Use public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Provide for mutual device authentication for both the host and the POI device or host-to-host if applicable, including assurance to the host that the POI device actually has (or actually can) compute the session key and that no entity other than the POI device specifically identified can possibly compute the session key.	**6D-1.8.a** For techniques involving public key cryptography, examine documentation and develop a schematic 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. **6D-1.8.b** If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, verify that the remote key distribution requirements detailed in Annex A of this document are met, including: • Use of public and private key lengths that are in accordance with Annex C for the algorithm in question . • Use of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6D-1.9 Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (e.g., POIs and other SCDs). ***Note:*** *Such controls may include but are not limited to:* • *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*	**6D-1.9.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. **6D-1.9.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. **6D-1.9.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.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2 *The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	
Key-injection facilities must ensure key-loading mechanisms are not subject to disclosure of key components or keys. *Some key-injection platforms use personal-computer (PC)-based software applications, whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. These weaknesses include:* • *XOR'ing of key components is performed in software.* • *Clear-text keys and components can reside in software during the key-loading process.* • *Some systems require only a single password.* • *Some systems store the keys (e.g., BDKs, TMKs) on removable media or smart cards. These keys are in the clear with some systems.* • *PCs, by default, are not managed under dual control. Extra steps (e.g., logical user IDs, physical access controls, etc.) must be implemented to prevent single control of a PC.* • *Data can be recorded in the PC's non-volatile storage.* • *Software Trojan horses or keyboard sniffers can be installed on PCs.*	

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.1 Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that: • Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of clear-text key components. • There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys. • The SCD must be inspected prior to use to ensure that it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying materials. • 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.	**6D-2.1** Observe key-loading environments, processes, and mechanisms (e.g., terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Ensure that any cameras that are present are positioned to ensure they cannot monitor the entering of clear-text key components. • Review documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that: ○ SCDs 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.
6D-2.2 Only SCDs shall 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 this Annex. For example, computer keyboards shall never be used for the loading of clear-text secret or private keys or their components.	**6D-2.2** 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 Annex. For example, ATM keyboards shall never be used for the loading of clear-text secret or private keys or their components.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.3 The loading of secret or private key components from an electronic medium to a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following: • The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.	**6D-2.3** Examine documented procedures for the loading of secret or private key components from an electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key loading, including: • Instructions for the medium to be placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.
	6D-2.3 Observe key-loading processes to verify that the loading process results in one of the following: • The medium used for key loading 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.
6D-2.4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:	**6D-2.4** Review documented procedures and observe processes for the use of key-loading devices. Perform the following:
6D-2.4.1 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.	**6D-2.4.1** 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.
6D-2.4.2 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.	**6D-2.4.2** 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.
6D-2.4.3 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.	**6D-2.4.3.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.
	6D-2.4.3.b Verify 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.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.4.4 The key-loading device must not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred.	**6D-2.4.4** Verify the key-loading device does not retain any information that might disclose the key 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.
6D-2.5 Any media (electronic or otherwise) containing secret or private key components used for loading cryptographic keys must be maintained in a secure storage 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/displayed (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 a non-custodian for that component.	**6D-2.5.a** Interview personnel and observe media locations to verify that the media is maintained in a secure storage location accessible only to custodian(s) authorized to access the key components.
	6D-2.5.b Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices are 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.
	6D-2.5.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.
	6D-2.5.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.
6D-2.6 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.	**6D-2.6** Validate through interview and observation that, if components are in human-readable form, they are visible only to the designated key-component custodian and only for the duration of time required for this person to privately enter the key component into an SCD.
6D-2.7 Written or printed key-component documents must not be opened until immediately prior to use.	**6D-2.7.a** Review documented procedures and confirm that printed/written key-component documents are not opened until immediately prior to use.
	6D-2.7.b Observe key-loading processes and verify that printed/written key components are not opened until immediately prior to use.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.8 A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. *E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.*	**6D-2.8.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.
	6D-2.8.b Examine key-component access controls and access logs to verify that any single authorized custodians can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.
6D-2.9 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 unprotected memory outside the secure boundary of an SCD must minimally implement the following additional controls:	**6D-2.9** Interview appropriate personnel and review documentation to determine the procedures for key loading to POIs, key-loading devices, and HSMs that are part of the key-loading platform. Review any logs of key loading.
6D-2.9.1 PCs and similar devices must be: • 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 that is dedicated to key-loading activities.	**6D-2.9.1** For facilities using PC-based key-loading software platforms or similar devices, verify through interviews and observation that the platform is: • Standalone • Dedicated to only key loading • Located in a physically secure room that is dedicated to key loading activities

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.9.2 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.	**6D-2.9.2** Verify through interviews and observation that: • 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.
6D-2.9.3 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: • 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.	**6D-2.9.3.a** Verify through interviews and observation that logs of key-loading activities are maintained and meet the following: • 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.

	6D-2.9.3.b Verify through interviews and observation that logs of key-loading activities are maintained and meet the following:
	• 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:
	  ○ 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,
	  ○ Video surveillance logs with a minimum retention period of 45 days.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.9.4 Additionally:	**6D-2.9.2** Verify through interviews and observation that:
6D-2.9.4.1 Cable attachments and the key-loading device must be examined before each use to ensure the equipment is free from tampering.	**6D-2.9.4.1** Cable attachments and the key-loading device are examined before each use to ensure the equipment is free from tampering.
6D-2.9.4.2 The key-loading device must be started from a powered-off position every time key-loading activities occur.	**6D-2.9.4.2** The key-loading device is started from a powered-off position every time key-loading activities occur.
6D-2.9.4.3 The software application must load keys without recording any clear-text values on portable media or other unsecured devices.	**6D-2.9.4.3** The software application loads keys without recording any clear-text values on portable media or other unsecured devices.
6D-2.9.4.4 Clear-text keys must not be stored except within an SCD.	**6D-2.9.4.4** Clear-text keys are not stored except within an SCD.
6D-2.9.4.5 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 to operate the key-injection application.	**6D-2.9.4.5** 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 to operate the key-injection application.
6D-2.9.4.6 The key-injection personnel must not have system-administration capability at either the O/S or the application level on the PC.	**6D-2.9.4.6** Key-injection personnel do not have system-administration capability at either the O/S or the application level on the PC.
6D-2.9.4.7 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.	**6D-2.9.4.7** The PC is not able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-2.9.4.8 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.	**6D-2.9.4.8** 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.
6D-2.9.4.9 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. ***Note:*** *For DUKPT implementations, the BDK should 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 to be used to initiate decryption of keys on portable electronic media (e.g., smart cards) must ensure the passwords are maintained under dual control and split knowledge.*	**6D-2.9.4.9** 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.
6D-2.9.4.10 Manufacturer's default passwords for PC-based applications must be changed.	**6D-2.9.4.10** Manufacturer's default passwords for PC-based applications are changed.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6D-3** All hardware and access/authentication mechanisms (e.g., passwords) used for key loading or the signing of authenticated applications (e.g., for "whitelists") must be managed under dual control.*	
Key-injection facilities must ensure that the key-injection application passwords and associated user IDs are managed in such a way as to enforce dual control. Also, the hardware used for key-injection must be managed under dual control. Vendor default passwords must be changed.	
6D-3.1 Any hardware and passwords used in the key-loading function must be controlled and maintained in a secure environment under dual control. Resources (e.g., passwords and associated hardware must be managed such that no single individual has the capability to enable key loading. This is not to imply that individual access authentication mechanisms must be managed under dual control.	**6D-3.1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords and associated hardware) used in the key-loading function must be controlled and managed such that no single individual has the capability to enable key loading.
	6D-3.1.b Observe key-loading environments and controls to verify the following: • 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.
6D-3.2 All cable attachments must be examined before each key-loading operation to ensure they have not been tampered with or compromised.	**6D-3.2.a** Review documented procedures to ensure they require that cable attachments be examined prior to key-loading function.
	6D-3.2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to a key-loading function.
6D-3.3 Key-loading equipment usage must be monitored and a log of all key-loading activities maintained for audit purposes containing at a minimum date, time, personnel involved, and number of devices keys are loaded to.	**6D-3.3.a** Observe key-loading activities to verify that key-loading equipment usage is monitored.
	6D-3.3.b Verify logs of all key-loading activities are maintained and contain all required information.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-3.4 Any physical tokens (e.g., brass keys or chip cards) used to enable key-loading must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control. These tokens must be secured in a manner similar to key components including the use of access-control logs for when removed or placed into secure storage.	**6D-3.4.a** Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key loading. 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 under single control.
	6D-3.4.b Inspect locations and controls for physical tokens to verify 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.
	6D-3.4.c Review storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.
	6D-3.4.d Verify that access-control logs exist and are in use.
	6D-3.4.e Reconcile storage contents to access-control logs.
6D-3.5 Default password or PINs used to enforce dual-control must be changed, and documented procedures must exist to require that these password/PINs be changed when assigned personnel change.	**6D-3.5.a** Verify that documented procedures require default passwords or PINs used to enforce dual control are changed.
	6D-3.5.b Verify that documented procedures exist to require that these passwords/PINs be changed when assigned personnel change.
***6D-4** The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	
6D-4.1 A cryptographic-based validation mechanism must be is in place to ensure the authenticity and integrity of keys and/or their components (e.g., testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See ISO 11568. Where check values are used, recorded, or displayed, key-component check values and key check values shall not exceed six hexadecimal characters in length.	**6D-4.1.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.
	6D-4.1.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 are verified by the applicable key custodians.
	6D-4.1.c Verify that the methods used for key validation are consistent with ISO 11568—e.g., when check values are used, they should return a value of no more than six hexadecimal characters.

Requirement 6D: Key loading to HSMs and POIs is handled in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6D-4.2 The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plaintext form, must: • Be within a certificate as defined in Annex A; or • Be within a PKCS#10; or • Be within an SCD; or • Have a MAC (message authentication code) created using the algorithm defined in ISO 16609.	**6D-4.2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.
	6D-4.2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.
***6D-5** Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*	
6D-5.1 Documented key-loading procedures must exist for all devices (e.g., HSMs and POIs), and all parties involved in cryptographic key loading must be aware of those procedures.	**6D-5.1.a** Verify documented procedures exist for all key-loading operations.
	6D-5.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.
	6D-5.1.c Observe 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.
6D-5.2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.	**6D-5.2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6E-2** Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	
6E-2.2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.	**6E-2.2.a** Verify documented procedures require that key-component packaging/containers showing signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
	6E-2.2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
***6E-2.3** not used in this Annex B.*	
6E-2.4 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.*	**6E-2.4.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.
	6E-2.4.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.
6E-2.5 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: • 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.	**6E-2.5.a** Examine documented procedures to verify they include: • Controls to protect against unauthorized substitution of keys, and • Controls to prevent the operation of devices without legitimate keys.
	6E-2.5.b Interview responsible personnel and observe key-loading processes and controls to verify that: • Controls are implemented that protect against unauthorized substitution of keys, and • Controls are implemented that prevent the operation of devices without legitimate keys.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6E-3** Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	
• *Where test keys are used, key-injection facilities must use a separate test system for the injection of test keys.* • *Test keys must not be injected using the production platform, and test keys must not be injected into production equipment.* • *Production keys must not be injected using a test platform, and production keys must not be injected into equipment that is to be used for testing purposes.* • *Keys used for signing of test certificates must be test keys.* • *Keys used for signing of production certificates must be production keys.*	
6E-3.1 Encryption keys must be used only for the purpose they were intended (i.e., key-encryption keys must not to be used as PIN-encryption keys, PIN-encryption keys must not be used for account data, etc.). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.	**6E-3.1.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.
	6E-3.1.b Using a sample of device types, validate via review of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.
6E-3.2 Private keys must only be used as follows: • 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). • Private keys shall never be used to encrypt other keys.	**6E-3.2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are only used: • To create digital signatures or to perform decryption operations. • For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for POI devices). • Private keys are never used to encrypt other keys.
6E-3.3 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).	**6E-3.3** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for POI devices).

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
6E-3.4 Keys must never be shared or substituted between production and test/development systems: • Key used for production keys must never be present or used in a test system, and • Keys used for testing keys must never be present or used in a production system.	**6E-3.4.a** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and development systems.
	6E-3.4.b Observe processes for generating and loading keys into in production systems to ensure that they are in no way associated with test or development keys.
	6E-3.4.c Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.
	6E-3.4.d Compare check, hash, cryptogram, or fingerprint values for production and test/development keys for higher-level keys (e.g., MFKs, KEKs shared with other network nodes, and BDKs) to verify that development and test keys have different key values.
6E-3.5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the key-injection server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements. At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements. *Note this does not apply to HSMs that are never intended to be used for production.*	**6E-3.5** Interview personnel to determine whether production platforms are ever temporarily used for test purposes. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media, • Prior to reuse for production purposes the HSM is returned to factory state, • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
6E-4 *All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or account data-encipherment) by a POI device that processes account data must be unique (except by chance) to that device.*	
6E-4.1 POI devices must implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device. This means that not only the account-data-encryption key(s), but also keys that are used to protect other keys: firmware-authentication keys, payment application authentication, and display prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.	**6E-4.1.a** Examine documented procedures for the generation, loading, and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations.
	6E-4.1.b Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POIs to verify that unique keys are generated and used for each POI device.
	6E-4.1.c Examine check values, hashes, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.
6E-4.2 If a POI device directly interfaces with more than one entity for decryption of account data (e.g., a different acquiring organization), the POI must have a completely different and unique key or set of keys for each acquiring organization. These different keys, or sets of keys, must be totally independent and not variants of one another.	**6E-4.2** Determine whether POI devices are intended to interface with multiple entities for decryption. If so: • Examine documented procedures for generating all types of keys and verify the procedures ensure that unique keys, or sets of keys, are used for each acquiring organization and are totally independent and not variants of one another. • Interview personnel and observe key-generation processes to verify that unique keys or sets of keys are generated for each acquiring organization.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
6E-4.3 Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device. This requirement refers to the use of a single "base" key to derive master keys for many different POIs, 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.	**6E-4.3.a** Examine documented procedures and observe processes for generating master keys. Verify the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POIs receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.
	6E-4.3.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.
6E-4.4 Entities processing or injecting DUKPT or other key-derivation methodologies for more than one acquiring organization must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques: • Different BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model • Different BDKs by geographic region, market segment, platform, or sales unit Injection vendors 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.	**6E-4.4.a** Examine documented key-generation and injection procedures to verify that the following is required when injecting keys into a single POI for more than one acquiring organization: • The POI must have a completely different and unique key, or set of keys, for each acquiring organization. • These different keys, or sets of keys, must be totally independent and not variants of one another.
	6E-4.4.b Observe processes for generation and injection of keys into a single POI for more than one acquiring organization, to verify: • The POI has a completely different and unique key, or set of keys, for each acquiring organization. • These different keys, or sets of keys, are totally independent and not variants of one another.
6E-4.5 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.	**6E-4.5.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.
	6E-4.5.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.

Requirement 6E: Keys are used in a manner that prevents or detects their unauthorized usage.	
Domain 6 Annex B Requirements	**Testing Procedures**
6E-4.6 Remote Key-Establishment and Distribution Applications The following requirements apply to key-injection facilities participating in remote key-establishment and distribution applications: • 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).	**6E-4.6.a** For techniques involving public key cryptography, examine documentation and develop a schematic 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 POIPED.
	6E-4.6.b If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that: • Cryptographic mechanisms exist to uniquely identify the keys. • Key pairs used by POI devices are unique per device.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6F-1** Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	
Key-injection facilities must ensure that KEKs and account-data-encryption keys do not exist outside of SCDs except when encrypted or stored under dual control and split knowledge. *Some key-injection platforms use personal-computer (PC)-based software applications or similar devices whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems do not therefore meet this requirement. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key-injection facilities that use PC-based key-loading software platforms whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD must minimally implement the compensating controls outlined in **6D-2.***	
6F-1.1 Secret or private keys must only exist in one or more of the following forms: • At least two separate key shares or full-length components • Encrypted with a key of equal or greater strength as delineated in Annex C • Contained within a secure cryptographic device	**6F-1.1.a** Examine documented procedures for key storage and usage and observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.
	6F-1.1.b Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.
6F-1.2 Wherever key components are used, they have the following properties:	**6F-1.2** Examine documented procedures and interview responsible personnel to determine all instances where key components are used.
6F-1.2.1 Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.	**6F-1.2.1** Review processes for creating key components to verify that knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key.
6F-1.2.2 Construction of the cryptographic key requires the use of at least two key components/shares.	**6F-1.2.2** Observe processes for constructing cryptographic keys to verify that at least two key components are required for each key construction.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6F-1.2.3 Each key component/share has one or more specified authorized custodians.	**6F-1.2.3.a** Examine documented procedures for the use of key components and interview key custodians and key-management supervisory personnel to verify that each key component is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component.
	6F-1.2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components are designated as key custodians for those particular components.
6F-1.2.4 Procedures exist to ensure any custodian never has access to sufficient key components or shares of a secret or private key to reconstruct a cryptographic key. *For example, in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian must not then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.* *In an m-of-n scheme where n =5 and where all three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (e.g., component A and component B), as a second custodian (with, in this example, component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*	**6F-1.2.4.a** Examine documented procedures for the use of key components to verify that procedures ensure that any custodian never has access to sufficient key components or shares to reconstruct a secret or private cryptographic key.
	6F-1.2.4.b Examine key-component 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.
6F-1.3 Key components must be stored as follows:	**6F-1.3** Examine documented procedures, interview responsible personnel and inspect key-component storage locations to verify that key components are stored as outlined in Requirements **6F-1.3.1** through **6F-1.3.3** below:

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6F-1.3.1 Key components that exist in clear text clear-text outside of an SCD must be sealed in opaque, pre-numbered tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging. ***Note:*** *Tamper-evident, authenticable packaging (opacity may be envelopes within tamper-evident packaging) used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless 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.*	**6F-1.3.1.a** Examine key components and storage locations to verify 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.
	6F-1.3.1.b Inspect any tamper-evident packaging used to secure key components and ensure that it prevents the determination of the key component without visible damage to the packaging.
	6F-1.3.1.c Interview responsible personnel to determine that clear-text key components do not exist in any other locations, including in non-secure containers, in databases, on floppy disks, or in software programs.
	6F-1.3.1.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).
6F-1.3.2 Key components for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.* *Components 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.*	**6F-1.3.2** Inspect each key component storage container and verify the following: • 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).
6F-1.3.3 If a key component 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.	**6F-1.3.3** 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.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6F-2** Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.*	
Key-injection facilities must have written procedures to follow in the event of compromise of any key associated with the key-injection platform and process. Written procedures must exist, and all parties involved in cryptographic key loading must be aware of those procedures. All key-compromise procedures must be documented.	
6F-2.1 Procedures for known or suspected compromised keys must include the following:	**6F-2.1** Verify documented procedures exist for replacing known or suspected compromised keys that include all of the following (**6F-2.1.1** through **6F-2.1.5** below):
6F-2.1.1 Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.	**6F-2.1.1** Interview responsible personnel and observe implemented processes to verify key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.
6F-2.1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.	**6F-2.1.2** Interview responsible personnel and observe implemented processes to verify that if unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.
6F-2.1.3 A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s). ***Note**: The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.* *Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.*	**6F-2.1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, all the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6F-2.1.4 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	**6F-2.1.4.a** Interview responsible personnel and review documented procedures 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). **6F-2.1.4.b** Verify notifications include the following: • A damage assessment including, where necessary, the engagement of outside consultants. • Details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.
6F-2.1.5 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: • Missing secure cryptographic devices • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation	**6F-2.1.5** Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation
6F-2.2 If attempts to load a secret key or key component into a KLD or POI fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI	**6F-2.2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into a KLD or POI fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6F-3 *Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.* *Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.* *Keys generated with a non-reversible process, such as key derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*	
6F-3.1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes, but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from PIN keys. ***Note:*** *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*	**6F-3.1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.
	6F-3.1.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.
6F-3.2 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 shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration.	**6F-3.2.a I**nterview 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.*
	6F-3.2.b Review vendor documentation to determine support for key variants.
	6F-3.2.c Via review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used, determine that variants of the MFK are not used external to the logical configuration that houses the MFK.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6F-3.3 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys (e.g., PEKs) from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or working keys with different purposes from another working key. ***Note:*** *Using transforms of keys across different levels of a key hierarchy—e.g., generating a PEK key from a key-encrypting key—increases the risk of exposure of each of those keys.* *It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as a PIN key, 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.*	**6F-3.3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys. • Variants of working keys must only be calculated from other working keys.
***6F-4** Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*	
6F-4.1 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	**6F-4.1.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.
	6F-4.1.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.
	6F-4.1.c Review storage locations for the sample of destroyed keys to verify they are no longer kept.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6F-4.2 The procedures for destroying keys or key components that are no longer used or that 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. This must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient. ***Note:*** *Key destruction for keys installed in HSMs and POI devices is addressed in Requirement* ***6G-3****.*	**6F-4.2.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.
	6F-4.2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.
6F-4.2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic DB backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568. *For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.*	**6F-4.2.1.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.
	6F-4.2.1.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—are destroyed following the procedures outlined in ISO–9564 or ISO–11568.
6F-4.2.2 The key-destruction process must be observed by a third party other than the custodian. The third-party witness must sign an affidavit of destruction.	**6F-4.2.2.a** Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian.
	6F-4.2.2.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.
6F-4.2.3 Key components for keys other than the HSM MFK 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.	**6F-4.2.3.a** Verify documented procedures exist for destroying key components of keys, once the keys are successfully loaded and validated as operational.
	6F-4.2.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6F-5** Access to secret and private cryptographic keys and key material must be:* a) *Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and* b) *Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*	
6F-5.1 To reduce the opportunity for key compromise, limit the number of key custodians to the minimum required for operational efficiency. For example:	**6F-5.1** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:
6F-5.1.1 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	**6F-5.1.1** Review key-custodian assignments for each component to verify that: • A primary and a backup key custodian are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel
6F-5.1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.	**6F-5.1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form.
	6F-5.1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form.
6F-5.1.3 Each key-custodian form provides the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date for the custodian's access • Signature of management authorizing the access	**6F-5.1.3** Examine all key-custodian forms to verify that they include the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date for the custodian's access • Signature of management authorizing the access

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6F-5.1.4 In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual except as noted below for organizations of insufficient size. *For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual.* The components collectively held by an individual and his or her direct reports shall not constitute a quorum (or shall not provide any information about the value of the key that is not derivable from a single component). When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented. Organizations that are of such insufficient size that they cannot support the reporting-structure requirement must ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian), receive explicit training to instruct them from sharing key components with their direct manager and must sign key-custodian agreements that includes an attestation to the requirement.	**6F-5.1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisor possess the necessary threshold of key components sufficient to form any given key. **6F-5.1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, ensure that documented procedures exist and are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes whistleblower procedures to report any violations.

Requirement 6F: Keys are administered in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
***6F-6** Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.* *Key-injection facilities must maintain logs for the key management of all keys and keying material used in all key-loading sessions. These include keys and materials removed from safes and used in the loading process.*	
6F-6.1 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. At a minimum, logs must include the following: • Date and time in/out • Key-component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)	**6F-6.1.a** Review log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD **6F-6.1.b** Review log files and audit log settings to verify that logs include the following: • Date and time in/out • Key-component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)
***6F-7** Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.*	
***Note:** It is not a requirement to have backup copies of key components or keys.*	

6F-7.1 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.	**6F-7.1** 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:
	• 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.
	• Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows:
	  ○ Securely stored with proper access controls
	  ○ Under at least dual control
	  ○ Subject to at least the same level of security control as operational keys as specified in this document

Requirement 6F: Keys are administered in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6F-7.2 If backup copies are created, the following must be in place: • Creation (including cloning) must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.	**6F-7.2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies requires at least two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.
***6F-8** Documented procedures must exist and must be demonstrably in use for all key-administration operations.*	
6F-8.1 Written procedures must exist, and all affected parties must be aware of those procedures. All activities related to key administration performed by a key-injection facilities must be documented. This includes all aspects of key administration, as well as: • Security awareness 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	**6F-8.1.a** Examine documented procedures for key-administration operations to verify they include: • Security-awareness 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
	6F-8.1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.
	6F-8.1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.
	6F-8.1.d Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6G-1** Equipment used to protect account data (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*	
Key-injection facilities must ensure that only legitimate, unaltered devices are loaded with cryptographic keys. *Secure areas must be established for the inventory of POI devices that have not had keys injected.The area must have extended walls from the real floor to the real ceiling using sheetrock, wire mesh, or equivalent. Equivalence can be steel cages extending floor to real ceiling. The cages can have a steel cage top in lieu of the sides extending to the real ceiling. The cages must have locks (with logs) or badge control with logging for entry.*	
6G-1.1 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 subject to unauthorized modification, substitution, or tampering and has not otherwise been subject to misuse prior to deployment.	**6G-1.1.a** Review documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POIs 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.
	6G-1.1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POIs 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.
6G-1.1.1 Controls must be implemented to protect POIs and other SCDs from unauthorized access up to point of deployment. Controls must include the following:	**6G-1.1.1** Review documented procedures to verify controls are defined to protect POIs and other SCDs from unauthorized access up to point of deployment.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-1.1.1.1 Access to all POIs and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection.	**6G-1.1.1.1.a** Examine access-control documentation and device configurations to verify that access to all POIs and key-injection/loading devices is defined and documented.
	6G-1.1.1.1.b For a sample of POIs and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POIs and other SCDs is logged.
	6G-1.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI or other SCD.
6G-1.1.1.2 POIs and other SCDs must not use default keys or data (such as keys that are pre-installed for testing purposes) or passwords.	**6G-1.1.1.2** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys or passwords are not used.
6G-1.1.1.3 All personnel with access to POIs 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 POIs and other SCDs as authorized by management. The list of authorized personnel is reviewed at least annually.	**6G-1.1.1.3.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POIs and other SCDs are documented in a formal list. • All personnel with access to POIs and other SCDs are authorized by management. • The authorizations are reviewed annually.
	6G-1.1.1.3.b For a sample of POIs and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in the formal list have access to devices.
6G-1.2 Implement a documented "chain of custody" to ensure that all devices are controlled from receipt through to placement into service. The chain of custody must include records to identify responsible personnel for each interaction with the devices.	**6G-1.2.a** Examine documented processes to verify that the chain of custody is required for devices from receipt to placement into service.
	6G-1.2.b For a sample of devices, review documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to placement into service.
	6G-1.2.c Verify that the chain-of-custody records identify responsible personnel for each interaction with the device

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures

6G-1.3 Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the following.
• Transportation using a trusted courier service (e.g., via bonded carrier). The devices are then securely stored until key-insertion and deployment occurs.
• Use of physically secure and trackable packaging (e.g., pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored in such packaging, or in secure storage, until key insertion and deployment occurs.
• A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. Before key-insertion, 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.
• Each cryptographic device is carefully inspected and tested immediately prior to key-insertion and deployment using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized access or modifications. *(**Note:** Unauthorized access includes that by customs officials.)*
  ○ Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised. (Note: This control must be used in conjunction with one of the other methods.)
  ○ Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.
	6G-1.3.a Examine documented procedures to confirm that they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods.
	6G-1.3.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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6G-1.4 Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs but must not supplant the implementation of dual-control mechanisms.	**6G-1.4.a** Examine documented procedures to confirm that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.
	6G-1.4.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..
6G-1.4.1 HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to the manufacturer's invoice or similar document*	**6G-1.4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.
	6G-1.4.1.b For a sample of received devices, review sender documentation sent via a different communication channel than the devices shipment (e.g., the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.
6G-1.4.2 The security policy enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required in account data-processing equipment to support specified functionality must be disabled before the equipment is commissioned.	**6G-1.4.2.a** Obtain and review the defined security policy to be enforced by the HSM
	6G-1.4.2.b Examine documentation of the HSM configuration settings to determine that the functions and command authorized to be enabled are in accordance with the security policy.
	6G-1.4.2.c For a sample of HSMs, review the configuration settings to determine that only authorized functions are enabled.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-1.4.3 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:	**6G-1.4.3** Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify integrity of device and include requirements specified at **6G-1.4.4.1** through **6G-1.4.4.4** below.
6G-1.4.3.1 Running self-tests to ensure the correct operation of the device	**6G-1.4.3.1** 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.
6G-1.4.3.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised	**6G-1.4.3.2** 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.
6G-1.4.3.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed	**6G-1.4.3.3** Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.
6G-1.4.3.4 Maintaining records of the tests and inspections, and retaining records for at least one year	**6G-1.4.3.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	6G-1.4.3.4.b Examine records of inspections to verify records are retained for at least one year.
6G-1.4 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	**6G-1.4.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.
	6G-1.4.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
***6G-2** Physical and logical protections must exist for deployed POI devices.*	
6G-2.3 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: • 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. ***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.*	**6G-2.3.a** Obtain and review documentation of inventory control and monitoring procedures. Determine that the procedures cover: • 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. **6G-2.3.b** Interview applicable personnel to determine that procedures are known and followed.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
***6G-3** Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair*	
Key-injection facilities must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any SCDs (e.g., HSM) used in the key-injection platform, as well as to any devices that have been loaded with keys and securely stored or warehoused on site that are subsequently deemed to be unnecessary and never to be placed into service. *If a key-injection facility receives a used device to reload with keys, procedures shall ensure that old keys that may be in the device are destroyed prior to loading of new keys. (The used device should have had its keys destroyed when it was removed from service, but this is a prudent secondary check that the keys were destroyed.)*	
6G-3.1 Procedures are 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 that all keys, key material, and account data stored within the device must be rendered irrecoverable. Processes must include the following: ***Note:** Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*	**6G-3.**1 Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all keys and key material stored within the device be securely destroyed. • Procedures cover all devices removed from service or for repair. • Procedures cover requirements at **6G-3.1.1** through **6G-3.1.6** below.
6G-3.1.1 HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.	**6G-3.1.1.a** Review documented procedures for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes.
	6G-3.1.1.b Interview personnel and observe demonstration (if HSM is available) of processes for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes
6G-3.1.2 Keys are rendered irrecoverable (e.g., zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.	**6G-3.1.2** Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material is rendered irrecoverable (e.g., zeroized), or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-3.1.3 SCDs being decommissioned are tested and inspected to ensure keys have been rendered irrecoverable.	**6G-3.1.3** Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.
6G-3.1.4 Affected entities are notified before devices are returned.	**6G-3.1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
6G-3.1.5 Devices are tracked during the return process.	**6G-3.1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
6G-3.1.6 Records of the tests and inspections maintained for at least one year.	**6G-3.1.6** Interview personnel and observe records to verify that records of the tests and inspections are maintained for at least one year.
***6G-4** Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key, or signing applications to be loaded onto a POI device, must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:* *a) Dual access controls required to enable the key-encryption function* *b) Physical protection of the equipment (e.g., locked access to it) under dual control* *c) Restriction of logical access to the equipment*	
Key-injection facilities must ensure protection against unauthorized use for SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.	
6G-4.1 For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:	**6G-4.1** 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, and that they cover the requirements at **6G-4.1.1** through **6G-4.1.5** below.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6G-4.1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. ***Note:*** *Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords at least five characters in length, or for physical access via a physical lock that requires two individuals, each with a different high-security key.* *For devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.* *Physical keys, authorization codes, passwords, 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.*	**6G-4.1.1** 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.
6G-4.1.2 Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.	**6G-4.1.2** Observe password policies and configuration settings to confirm that passwords used for dual control must be at least five numeric and/or alphabetic characters.
6G-4.1.3 Dual control must be implemented for the following: • To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; • To 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	**6G-4.1.3** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing; • To place the device into a state that allows for the input or output of clear-text key components; • For all access to KLDs

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-4.1.4 Devices must not use default passwords.	**6G-4.1.4.a** Examine password policies and documented procedures to confirm default passwords must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys.
	6G-4.1.4.b Observe device configurations and interview device administrators to verify that HSMs, KLDs, and other SCDs used to generate or load cryptographic keys do not use default passwords.
6G-4.1.5 To detect any unauthorized use, devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected. ***Note:*** *POI devices may be secured by storage in the dual-control access key injection room.*	**6G-4.1.5.a** Examine documented procedures to confirm that they require devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
	6G-4.1.5.b Interview responsible personnel and observe devices and processes to confirm that devices at all times within a secure room and are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
*Functionality of a key-injection facility may be located at a single physical location or distributed over a number of physical locations. Distributed KIF functionality may include key generation, CA functionality, key distribution and key injection. In order to mitigate the expanded attack surface of a distributed KIF, specific controls apply to a distributed architecture. If any secret or private keys or their components/shares appear in the clear outside of a SCD, Requirement **6G-4.10** for a secure room must be met.*	
6G-4.9 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 **6C**.	
6G-4.9.1 The KIF must ensure that keys are transmitted between KIF components in accordance with **6C**.	**6G-4.9.1.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 **6C**.
	6G-4.9.1.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.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-4.9.2 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.	**6G-4.9.2** Examine documented procedures to confirm they specify the establishment of a channel for mutual authentication of the sending and receiving devices.
6G-4.9.3 The KIF must ensure that injection of enciphered secret or private keys into POI devices meets the requirements of **6D**.	
6G-4.9.4 The channel for mutual authentication is established using the requirements of **6D**.	**6G-4.9.4.a** Examine documented procedures for key loading to hosts and POI devices to verify that they are in accordance with applicable criteria in **6D**.
	6G-4.9.4.a 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.
6G-4.9.5 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.	**6G-4.9.5** 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.
6G-4.9.6 Mutual authentication of the sending and receiving devices must be performed. • KIFs must validate authentication credentials of a POI 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 POIs and a KIF HSM it must not be possible to insert an unauthorized SCD into the flow without detection.	**6G-4.9.6** Interview responsible personnel and observe processes for establishment of enciphered secret or private keys between sending and receiving devices to verify: • 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
6G-4.9.7 Mechanisms must exist to prevent a non-authorized host from injecting keys into POIs or an unauthorized POI from establishing a key with a legitimate KIF component.	**6G-4.9.7** Examine documented procedures to confirm they define mechanisms to prevent an unauthorized host from performing key transport, key exchange, or key establishment with POIs.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.

Domain 6 Annex B Requirements	Testing Procedures
6G-4.10 The KIF must implement a physically secure area (secure room) for key injection where any secret or private keys or their components/shares appear in the clear outside of an SCD. The secure room for key injection must include the following:	
6G-4.10.1 The secure area 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 area must have extended walls from the real floor to the real ceiling using sheetrock or wire mesh.	**6G-4.10.1** Inspect the secure area 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.
6G-4.10.2 Any windows into the secure room must be locked and protected by alarmed sensors.	**6G-4.10.2.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	6G-4.10.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.
6G-4.10.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**6G-4.10.3** Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
6G-4.10.4 A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.	**6G-4.10.4** Inspect the secure area 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.
6G-4.10.5 An electronic access control system (e.g., badge and/or biometrics) must be in place that enforces: • Dual-access requirements for entry into the secure area, and • Anti-pass-back requirements.	**6G-4.10.5** Observe authorized personnel entering the secure area to verify that a badge-control system is in place that enforces the following requirements: • Dual-access for entry to the secure area • Anti-pass-back
6G-4.10.6 The badge-control system must support generation of an alarm when one person remains alone in the secure area 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.*	**6G-4.10.6** 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 area for more than 30 seconds.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
6G-4.10.7 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.	**6G-4.10.7** Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a 24/7 basis.
6G-4.10.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	**6G-4.10.8** 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.
6G-4.10.9 The CCTV server and digital storage must be secured in a separate secure area that is not accessible to personnel who have access to the key-injection area.	**6G-4.10.9.a** Inspect location of the CCTV server and digital-storage to verify they are located in a secure area that is separate from the key-injection area.
	6G-4.10.9.b Inspect access-control configurations for the CCTV server/storage area and the key-injection area to identify all personnel who have access to each area. Compare access lists to verify that personnel with access to the key-injection area do not have access to the CCTV server/storage area.
6G-4.10.10 The CCTV cameras must be 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.	**6G-4.10.10** Inspect CCTV positioning and review a sample of recordings to verify 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.
6G-4.10.11 CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials.	**6G-4.10.11** Inspect CCTV positioning and review a sample of recordings to verify that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials.

Requirement 6G: Equipment used to process account data and keys is managed in a secure manner.	
Domain 6 Annex B Requirements	**Testing Procedures**
***6G-5** Documented procedures must exist and be demonstrably in use to ensure the security and integrity of account-data-processing equipment (e.g., POIs and HSMs) placed into service, initialized, deployed, used, and decommissioned.*	
6G-5.1 Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed by key-injection facilities on PIN-processing devices before they are placed into service, as well as devices being decommissioned.	**6G-5.1.a** Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for devices placed into service, initialized, deployed, used, and decommissioned,
	6G-5.1.b Verify that written records exist for the tests and inspections performed on PIN-processing devices before they are placed into service, as well as devices being decommissioned.

Requirement 6I: KIF component providers ONLY: report status to solution providers

Domain 6 Annex B Requirements	Testing Procedures
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain 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).*	
6I-1 For component providers of key-injection services: maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	

6I-1.1 Track status of key-management services for POIs and HSMs and provide reports to solution provider annually and upon significant changes, including at least the following:
• 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 **6F-2.1**
Note that adding, changing, or removing POI device 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 or removing elements of a P2PE solution.
	6I-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:
	• 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 **6F-2.1**
	
	6I-1.1.b Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following:
	• Types/models of 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 **6F-2.1**

Domain 6 Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange, or establishment and for data protection:

Algorithm	DEA	RSA	Elliptic Curve	DSA	AES
Minimum key size in number of bits [4]	168	2048	224	2048/224	128

The strength of a cryptographic key is a measure of the expected work effort an attacker would have to spend to discover the key. Cryptographic strength is measured in "bits of security" (see, e.g., *NIST SP 800-57* Part 1). While the concept of bits of security originated with symmetric encryption algorithms, it extends to asymmetric algorithms as well. In neither case do the bits of security necessarily equal the length of the key.

The following table, which is consistent with *NIST SP 800-57* Part 1, Table 2, and with *ISO TR-14742,* lists the cryptographic strength of the most common key lengths for the relevant symmetric and asymmetric cryptographic algorithms. DEA (DES) refers to TDEA (TDES) keys with non-parity bits. The RSA key size below refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

Bits of Security	Symmetric encryption algorithms	RSA	Elliptic Curve	DSA/D-H
112	Triple-length TDEA	2048	224	2048/224
128	AES-128	3072	256	3072/256
192	AES-192	7680	384	7680/384
256	AES-256	15360	512	15360/512

In general, the weakest algorithm and key size used to provide cryptographic protection determines the strength of the protection. For example, if a 2048-bit RSA key is used to encipher an AES-128 key, henceforth that AES key will only have 112-bit strength, not 128-bit. Intuitively this is because once you break the key encryption key, you have access to the data encryption key. The strength hence reflects the expected amount of effort an attacker needs to spend in order to discover the key.

[4] The requirement for longer DH, ECDH, ECC and DSA keys reflects an industry transition to longer key lengths (see *NIST SP800-131A*) without any requirement for legacy support.

This applies to any key-encipherment keys used for the protection of secret or private keys that are stored, or for keys used to encrypt any secret or private keys for loading or transport.

For implementations using Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH):

1. **DH implementations** – Entities must securely generate and distribute the system-wide parameters: generator *g,* prime number *p* and parameter *q,* the large prime factor of (*p* - 1). Parameter *p* must be at least 2048 bits long, and parameter *q* must be at least 224 bits long. Each entity generates a private key *x* and a public key *y* using the domain parameters (*p, q, g*,).
2. **ECDH implementations** – Entities must securely generate and distribute the system-wide parameters. Entities may generate the elliptic curve domain parameters or use a recommended curve (See *FIPS186-4*). The elliptic curve specified by the domain parameters must be at least as secure as P-224. Each entity shall generate a private key *d* and a public key *Q* using the specified elliptic curve domain parameters. (See *FIPS186-4* for methods of generating *d* and *Q*).
3. Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
4. Entities must authenticate the DH or ECDH public keys using either DSA, ECDSA, a certificate, or a symmetric MAC (see *ISO 16609 – Banking –Requirements for message authentication using symmetric techniques).* One of the following: MAC algorithm 1 using padding method 3, MAC algorithm 5 using padding method 4 should be used).

Appendix A: P2PE Domain Responsibility Scenarios

Example scenario matrices are being provided to illustrate the applicability of the P2PE domains (and subsequently the associated requirements) relative to various entities that may contribute to the P2PE solution. The scenarios serve only as examples. As a reminder, the Solution Provider assumes ultimate responsibility for their P2PE solution.

Scenario 1: Solution provider uses a third-party POI application, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security		X				
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment	X					
Domain 6: P2PE Cryptographic Key Operations and Device Management	X					
Domain 6 Annex A	X as applicable					
Domain 6 Annex B						

Scenario 2: Solution provider uses a third-party POI application, and outsources all other solution functions

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management			X			
Domain 2: Application Security		X				
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment				X		
Domain 6: P2PE Cryptographic Key Operations and Device Management			X	X		
Domain 6 Annex A			X as applicable	X as applicable		
Domain 6 Annex B						

Scenario 3: Solution provider writes own POI application(s), outsources decryption management, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security	X					
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment			X			
Domain 6: P2PE Cryptographic Key Operations and Device Management	X		X			
Domain 6 Annex A	X as applicable		X as applicable			
Domain 6 Annex B						

Scenario 4: Solution provider uses a third-party POI application(s), outsources device and decryption management, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management			X			
Domain 2: Application Security		X				
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment				X		
Domain 6: P2PE Cryptographic Key Operations and Device Management			X	X		
Domain 6 Annex A			X as applicable	X as applicable		
Domain 6 Annex B						

Scenario 5: Solution provider uses a third-party POI application, outsources to a KIF, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security		X				
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment	X					
Domain 6: P2PE Cryptographic Key Operations and Device Management	X					
Domain 6 Annex A	X as applicable				X as applicable	
Domain 6 Annex B					X	

Scenario 6: Solution provider outsources key-injection facility and CA/RA functions, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security	X					
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions						
Domain 5: Decryption Environment	X					
Domain 6: P2PE Cryptographic Key Operations and Device Management	X					
Domain 6 Annex A	X as applicable				X as applicable	X
Domain 6 Annex B					X	

Scenario 7: Merchant-managed solution (MMS) – Merchant as the solution provider manages all functions of the solution, including writing own POI applications.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security	X					
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions	X					
Domain 5: Decryption Environment	X					
Domain 6: P2PE Cryptographic Key Operations and Device Management	X					
Domain 6 Annex A	X as applicable					
Domain 6 Annex B						

Scenario 8: Merchant-managed solution (MMS) – Merchant as solution provider, uses a third-party POI application, outsources device management and KIF functions, and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management			X			
Domain 2: Application Security		X				
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions	X					
Domain 5: Decryption Environment	X					
Domain 6: P2PE Cryptographic Key Operations and Device Management	X		X			
Domain 6 Annex A	X as applicable		X as applicable		X as applicable	
Domain 6 Annex B					X	

Scenario 9: Merchant-managed solution (MMS) – Merchant as the solution provider, outsources decryption management and manages all other solution functions.

Domain	Solution Provider	P2PE Application Vendor	Encryption-Management Services Entity	Decryption-Management Services Entity	KIF Services Entity	CA/RA Services Entity
Domain 1: Encryption Device and Application Management	X					
Domain 2: Application Security	X					
Domain 3: P2PE Solution Management	X					
Domain 4: Merchant-managed Solutions	Not required for MMS if decryption is outsourced					
Domain 5: Decryption Environment				X		
Domain 6: P2PE Cryptographic Key Operations and Device Management	X			X		
Domain 6 Annex A	X as applicable			X as applicable		
Domain 6 Annex B						