Payment Card Industry (PCI)

Point-to-Point Encryption

Solution Requirements and Testing Procedures:

Encryption and Key Management within Secure Cryptographic Devices, and Decryption of Account Data in Software

(Hardware/Hybrid)

Version 1.1.1

July 2013

Document Changes

Date	Version	Description	Pages
December 2012	1.1	Initial release of *PCI Point-to-Point Encryption: Solution Requirements – Encryption and Key Management within Secure Cryptographic Devices, and Decryption of Account Data in Software (Hardware/Hybrid).*	
July 2013	1.1.1	Updated to address errata revisions including typographical errors, format and numbering issues. Minor updates to align with Hardware/Hardware Standard.	

Table of Contents

Introduction: Solution Requirements for Point-to-Point Encryption

Purpose of this Document

This document, *Point-to-Point Encryption: Solution Requirements – Encryption and Key Management within Secure Cryptographic Devices and Decryption of Account Data in Software,* defines requirements for hardware/hybrid Point-to-Point Encryption (P2PE) solutions, with the goal of reducing the scope of a PCI DSS assessment for merchants using such solutions. Its intended audience is vendors, assessors, and solution providers that may develop products for, implement, and evaluate P2PE solutions, as well as merchants who want to understand more about P2PE solutions and their effect on PCI DSS scope.

Point-to-point encryption technology may assist merchants to reduce the scope of their cardholder data environment and annual PCI DSS assessments. As implementations of these technologies increase, the Council believes it is imperative to build, test, and deploy solutions that provide strong support for PCI DSS compliance. With this aim the Council is launching requirements and testing procedures for point-to-point encryption solutions. The Council reminds stakeholders that requirements for validating point-to-point encryption solutions do not supersede the PCI Data Security Standard or other PCI Standards, nor does the launch of 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.

Note: *In the term "hardware/hybrid," the "forward slash" or "oblique" punctuation mark is used to separate the methods used for account-data encryption and decryption. The word before the slash denotes the encryption methodology, and the word after the slash denotes the decryption and key-management methodology. So in the case of hardware/hybrid, hardware is used for encryption while a combination of hardware and software (hybrid) is used for decryption.*

This document for hardware/hybrid point-to-point encryption solutions provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this version contains validation requirements and testing procedures for hardware/hybrid solutions which utilize secure cryptographic devices at the point of merchant acceptance for encryption and for managing cryptographic keys in the decryption environment while utilizing non-SCDs for the decryption of account data.

Definition of Secure Cryptographic Devices (SCDs) to be used for Point-to-Point Encryption

This document requires the use of secure cryptographic devices, or SCDs, for the encryption of payment-card data, as well as for the storage and management of cryptographic keys. For the purposes of this P2PE standard, SCDs, which are used in hardware/hybrid for both encryption and key-management functions, include but are not limited to key-loading devices, point-of-interaction (POI) devices, and host/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, with SRED (secure reading and exchange of data) listed as a "function provided," and with the SRED capabilities enabled and active. SCDs used for cryptographic-key management functions are

host/hardware security modules (HSMs), and must be either approved and configured to FIPS140-2 (level 3 or higher), or approved to the PCI HSM standard.

Hardware/Hybrid – Solutions with Encryption and Key Management within SCDs and Account Data Decryption in Software

Requirements for a P2PE solution will vary depending on the deployment environment and the technologies used for a specific implementation. This version of the *P2PE Solution Requirements and Testing Procedures* presents requirements covering each domain for hardware/hybrid environments (where SCDs are used for encryption and cryptographic-key management, and software is used for the decryption of account data). Hardware/hybrid P2PE solutions are for merchants who do not store or decrypt encrypted data within their P2PE environment, and who use validated P2PE solutions consisting of hardware-based encryption and third-party hybrid-based decryption.

Unlike a hardware/hardware P2PE solution, the decryption of account data for a hardware/hybrid P2PE solution is performed outside of an HSM on the Host System. In addition to the decryption of account data, the Host System may also be used for transaction processing; however, it should be not used for any purpose unrelated to these functions.

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

The solution provider's decryption environment may consist of multiple Host Systems in one or more locations. The Host System may take a variety of forms—for example, the Host System may be a dedicated PC with single or multiple processors, or a combination of hardware components operating as a single system. Where a Host System is comprised of multiple hardware components (for example, a server chassis containing multiple processors, servers, etc.), the connectivity between this hardware must be made through physical connections rather than using a network connection. Alternatively, the Host System may comprise of a partition on a mainframe computing system.

The Host System is connected to one or more HSMs to securely protect the data-decryption keys (DDKs) when not in use. The HSM(s) is a fundamental component of a hardware/hybrid P2PE solution; however, unlike hardware/hardware solutions, the decryption of account data is performed outside of the HSM on the Host System. When the Host System is required to decrypt encrypted account data received from POI, the DDK is retrieved from a key store protected by the HSM, and then passed to the Host System. The Host System then uses the DDK to decrypt the account data in the software of the Host System. The Host System will temporarily retain DDKs in volatile memory for the purpose of decrypting account data. When the DDK reaches the end of its cryptoperiod, it will be erased from memory

The Host System and HSM(s) must reside on a network that is dedicated to decryption operations and transaction processing, which may also include services required to support these functions. The decryption network must be segmented from any other network or system that is not performing or supporting decryption operations or transaction processing.

This standard differs from the P2PE hardware/hardware requirements and testing procedures, as hardware/hybrid permits the decryption of account data outside of an SCD and the presence of DDKs in software on the Host System. Hardware/hybrid builds on the hardware/hardware requirements and testing procedures as follows:

- Domains 1-4 of this document are unchanged from hardware/hardware.
- Domains 5 and 6 have been modified to permit the management of DDKs on the Host System for the sole purpose of account data decryption.
- Domains 5 and 6 have additional requirements and testing procedures to protect the Host System.

Merchants Using P2PE Solutions

Merchants may choose to implement Council-listed point-to-point encryption solutions to receive reduced scope for their PCI DSS assessment. For the hardware/hybrid scenario, this is achievable by implementing a hardware device (POI) at the point of account-data encryption that is part of a validated P2PE solution. These validated P2PE solutions are provided or specified by a P2PE solution provider (which is typically an acquirer (merchant bank), processor, or payment gateway). For the hardware/hybrid scenario, a validated P2PE solution includes the following:

- A PCI PTS-approved POI device that is part of the P2PE solution. This POI device in essence provides segmentation at the merchant's location between the merchant's cardholder data environment (which is contained within the device) and the rest of the merchant environment.
- Within the P2PE environment, account data is always entered directly into, and encrypted within, this POI before being transmitted.
- All account-data related operations are managed by the validated solution provider.

Characteristics for Merchants Eligible for Reduced Scope for PCI DSS via P2PE Solutions

To use a validated P2PE solution for reduced PCI DSS scope, merchants must meet certain characteristics as cited below. As an example of a reduced PCI DSS validation effort (either via annual self-assessment questionnaire or onsite review, as required by the merchant's acquirer or the payment brands), merchants *may* be asked to attest that they meet the following merchant characteristics, which include but are not limited to:

- Merchant uses a validated P2PE solution.
- Merchant never stores, processes, or transmits clear-text account data within their P2PE environment outside of a PCI-approved POI device.
- Physical environment controls for POI terminals, third-party agreements, and relevant merchant policies and procedures are in place.
- Merchant has followed the *P2PE Instruction Manual (PIM),* provided to the merchant by the P2PE Solution Provider.
- Merchant has adequately segmented (isolated) the P2PE environment from any non-P2PE payment channels or confirmed that no other channels exist.
- Merchant has removed or isolated any legacy cardholder data, or systems that stored, processed, or transmitted cardholder data, from the P2PE environment.

Merchant Responsibilities

Merchants who use a validated P2PE solution for reduced PCI DSS scope are responsible for:

- Coordinating with their acquirer (merchant bank) to determine which POI (as part of a validated P2PE solution) to implement.
- Reviewing the *P2PE Instruction Manual (PIM)* provided by the solution provider, and implementing the POI and in-store processes in accordance with the PIM.
- Coordinating with the acquirer to validate applicable PCI DSS requirements (if required to do so by the acquirer) in accordance with payment brand validation requirements.

Note: *Merchants can use the PCI SSC website list to find validated P2PE solutions, associated POIs, and other P2PE solution information.*

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

P2PE solutions help reduce merchant PCI DSS scope by eliminating clear-text account data from a merchant's environment, or by isolating the P2PE environment from clear-text account data present in other merchant payment channels.

A P2PE validated solution is one that has been validated by a P2PE assessor as compliant with P2PE solution requirements and testing procedures specified in this document, and is listed on PCI SSC's list of Validated P2PE Solutions. The P2PE Solution Requirements and Testing Procedures are set out in six P2PE domains; many of the P2PE requirements are based on elements of other PCI standards as follows:

- POI devices must meet PIN Transaction Security (PTS) requirements validation.
- Cryptographic-key operations for both encryption and decryption environments use key-management practices derived from the PTS PIN Security Standard.
- Applications on POI devices meet requirements derived from the Payment Application Data Security Standard (PA-DSS).
- The decryption environment is PCI DSS compliant.

Please note that the PCI PIN Security Requirements specify an independent set of requirements for PINs, and that this P2PE standard does not supersede or replace any requirements in the PCI PIN Security Requirements.

P2PE Roles and Responsibilities

The following section summarizes the roles and responsibilities of stakeholders with direct responsibility for P2PE solutions. For more detailed descriptions of all P2PE stakeholders with both direct and indirect P2PE responsibilities, please refer to the *P2PE Program Guide.*

Stakeholder Role	Responsibilities
P2PE Solution Provider	The P2PE solution provider is a third-party entity (for example, a processor, acquirer, or payment gateway) that has overall responsibility for the design and implementation of a specific P2PE solution, and (directly or indirectly through outsourcing) manages P2PE solutions for its customers and/or manages corresponding responsibilities. The solution provider has overall responsibility for ensuring that all P2PE requirements are met, including ensuring that P2PE requirements are met by any third-party organizations that perform P2PE functions on behalf of the solution provider, such as Certification Authorities and key-injection facilities.
P2PE Assessors	P2PE assessors are companies and individuals qualified by PCI SSC as either a QSA (P2PE) or PA-QSA (P2PE), which have met additional requirements to assess P2PE solutions and/or applications. P2PE assessors are qualified by PCI SSC to evaluate P2PE solutions (and with respect to PA-QSA (P2PE)s, perform P2PE application assessments) and submit corresponding P2PE reports on behalf of the applicable P2PE Solution Providers (and with respect to PA-QSA (P2PE)s, the applicable P2PE Application Vendors) directly to PCI SSC for review and acceptance. P2PE assessors are responsible for performing assessments in accordance with PCI SSC documentation, including this document, the *P2PE Reporting Instructions,* and the *P2PE Program Guide.* ***Note:*** *Not all QSAs are P2PE assessors—there are additional qualification requirements that must be met for a QSA to become a P2PE assessor*.
PCI PTS Laboratories	PCI PTS security laboratories are responsible for the evaluation of POI devices against the PCI PTS requirements. Evaluation reports on devices found compliant to the requirements are submitted by the PCI PTS laboratories to PCI SSC for approval and listing. Note that this device evaluation per PCI PTS requirements is separate from the P2PE solution validation; the P2PE validation will confirm the device is listed on PCI SSC's PTS listing.
Payment Device (Hardware) Vendors	A POI vendor submits a POI device for evaluation to an independent PCI PTS security laboratory. Vendors must develop a supplemental security guidance document describing the secure operation and administration of their equipment to assist merchants, application vendors, and solution providers.

Stakeholder Role	Responsibilities
Application (Software) Vendors	An application vendor that develops applications with access to account data on the POI device must have that application assessed for secure operation within the POI device, and must provide an *Implementation Guide* that describes secure installation and administration of the application on the POI device.
Certification Authorities	A Certification Authority (CA) is a trusted party that is responsible for the issuance of digital certificates. For purposes of these requirements, a certificate is any digitally signed value containing a public key. Specific requirements for CAs involved in remote key distribution are set out in Domain 6, Annex A. Certification Authority requirements apply to all entities signing public keys, whether in X.509 certificate-based schemes or other designs. These requirements apply equally to third-party CAs or a CA that is hosted by the solution provider. Ultimately, it remains the solution provider's responsibility to ensure that the CA is in compliance with the requirements set out in Annex A.
Key-Injection Facilities	The term "key-injection facility" (KIF) describes the entities performing key injection into POI devices. Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer or vendor. Environmental and key-management requirements are defined in Domains 1, 5 and 6 of this document; and Domain 6 Annex B contains additional requirements for KIFs. Ultimately, it remains the solution provider's responsibility to ensure that the KIF is in compliance with the requirements set out in Annex B.

Scope of Assessment for P2PE Solutions

The first step of a P2PE solution assessment is to accurately determine the scope of the solution. At least annually and prior to each assessment, the solution provider should confirm the accuracy of their solution scope by identifying all devices, P2PE data flows and processes, key-management functions and account-data stores, and ensure they are included in the solution scope. To ensure the accuracy of the solution scope is maintained on an ongoing basis, the solution provider must have processes in place that ensure the following:

- Any changes are implemented in a manner that ensures continued adherence to P2PE requirements for the entire solution.
- Any new rollouts/additions adhere to all P2PE solution requirements.
- Any new rollouts/additions are included in the next P2PE assessment.

For further details, please refer to the *P2PE Program Guide.*

The P2PE solution provider retains documentation that shows how P2PE solution scope was determined and maintained during the period of time until the next P2PE assessment, for assessor review and/or for reference during the next scope-confirmation activity. Annually, in accordance with the *P2PE Program Guide*, the solution provider provides an attestation to PCI SSC to confirm, among other things, the scope of their solution.

The scope of a P2PE solution validation encompasses the following across the six P2PE domains.

1. **Domain 1 –** For all secure cryptographic devices used to provide or support encryption of account data:
   - All PCI-approved POI devices included in the P2PE solution (for the merchant to use for payment acceptance)
   - All HSMs, key-loading devices, etc., used by the solution provider or nominated third party for any cryptographic-key operations on the POIs (for example, for loading of encryption keys onto POIs)
2. **Domain 2** – For all applications on POI devices:

   All applications on POI devices must be evaluated per P2PE Domain 2 (a "P2PE Application Assessment"); the extent of the assessment depends on whether the application has access to clear-text account data as follows:
   - All applications with access to clear-text account data undergo a full P2PE application assessment.
   - All applications with no access to clear-text account data (for example, a loyalty or advertising application) are subject to only one requirement (Requirement 2A-3) within Domain 2 for P2PE applications.

3. **Domain 3 –** The merchant encryption environment
   - The solution provider's management of encryption devices and any applications.
   - The merchant-focused *P2PE Instruction Manual (PIM)* that the solution provider prepares for, and distributes to, merchants.
4. **Domain 4** – *Domain 4, which addresses proper segmentation between the encryption and decryption systems,* ***has no applicable requirements*** *for hardware/hybrid solutions since the account data is encrypted for transmission by the PCI-approved POI device before the data leaves the device, and the merchant has no access to the decryption environment or the cryptographic keys.*
5. **Domain 5 –** The decryption environment
   - Solution-provider management of all system components located within or connected to the decryption environment, including HSMs and the Host System used for account-data decryption
   - Solution-provider management of all system components that may impact the security of account data

   Note that PCI DSS compliance of the decryption environment must be confirmed on an annual basis. This review may be performed as part of the P2PE solution validation or as a separate PCI DSS assessment, at the solution provider's discretion. Where the PCI DSS and P2PE assessments are performed separately, the QSA (P2PE) needs to confirm, via review of the scope in the PCI DSS Report on Compliance, that the PCI DSS scope fully covered the P2PE decryption environment and processes.
6. **Domain 6 –** P2PE Key-Management Operations
   - Secure key management for all cryptographic-key operations performed in both Domains 1 and 5.

Network Segmentation

The solution provider must ensure that network segmentation is in place between any systems owned or managed by the solution provider that are used in the P2PE solution, and any that are not included in their PCI DSS compliant environment. The QSA (P2PE) must validate that the network segmentation is adequate to isolate the P2PE environment from out-of-scope networks and systems.

At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented. *Please refer to PCI DSS for more information about network segmentation.*

Third Parties/Outsourcing

A given P2PE solution may be entirely performed and managed by a single solution provider, or the solution provider may outsource certain functions (for example, loading keys into POIs) to third parties who perform these functions on behalf of the solution provider. All third parties that perform P2PE functions on behalf of the assessed P2PE solution provider, including POI vendors, KIFs, CAs, etc., must be validated per P2PE solution requirements.

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

1. They can undergo a P2PE assessment of relevant P2PE requirements on their own and provide evidence to their customers to demonstrate their compliance; or
2. If they do not undergo their own P2PE assessment, they will need to have their services reviewed during the course of each of their solution provider customers' P2PE assessments.

Third-party providers that have been validated as meeting all relevant P2PE criteria may complete a specific attestation of validation (signed by the third party and the QSA (P2PE), which can be used as evidence for each individual P2PE solution provider (per option 1, above).

Sampling of System Components

After considering the overall scope and complexity of the 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.

Sampling of system components should adhere to the following principles:

- Sample must include all types of system components that exist at each facility.
- System components that may be sampled include:
  - POI devices
  - Application configurations
  - Other systems and network devices, as applicable

- Samples of system components must include every variation of the type of item that is in use. For example, samples of POI devices must include all models and firmware versions used by the solution; samples of applications must include all versions and platforms for each type of application, etc.
- All HSMs must be reviewed to verify secure configuration.
- All Host Systems must be reviewed to verify secure configuration
- Samples of keys/key components must include all key types and/or functions.

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 solution provider. 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 which govern 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
- 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.

P2PE At-a-Glance

At-a-Glance – Domains and Requirements for P2PE Validation

The table below presents the six control domains for validation of P2PE solutions. These domains represent the core areas where security controls need to be applied and validated.

This table provides an overview of each domain, including a description of the scope for the current scenario and the high-level requirements for each domain. Additionally, the table identifies the responsible parties for validation of each domain and for ultimately ensuring protection of account data in a P2PE solution. Each requirement identified here has corresponding sub-requirements and validation procedures, which are presented in detail beginning on page 18.

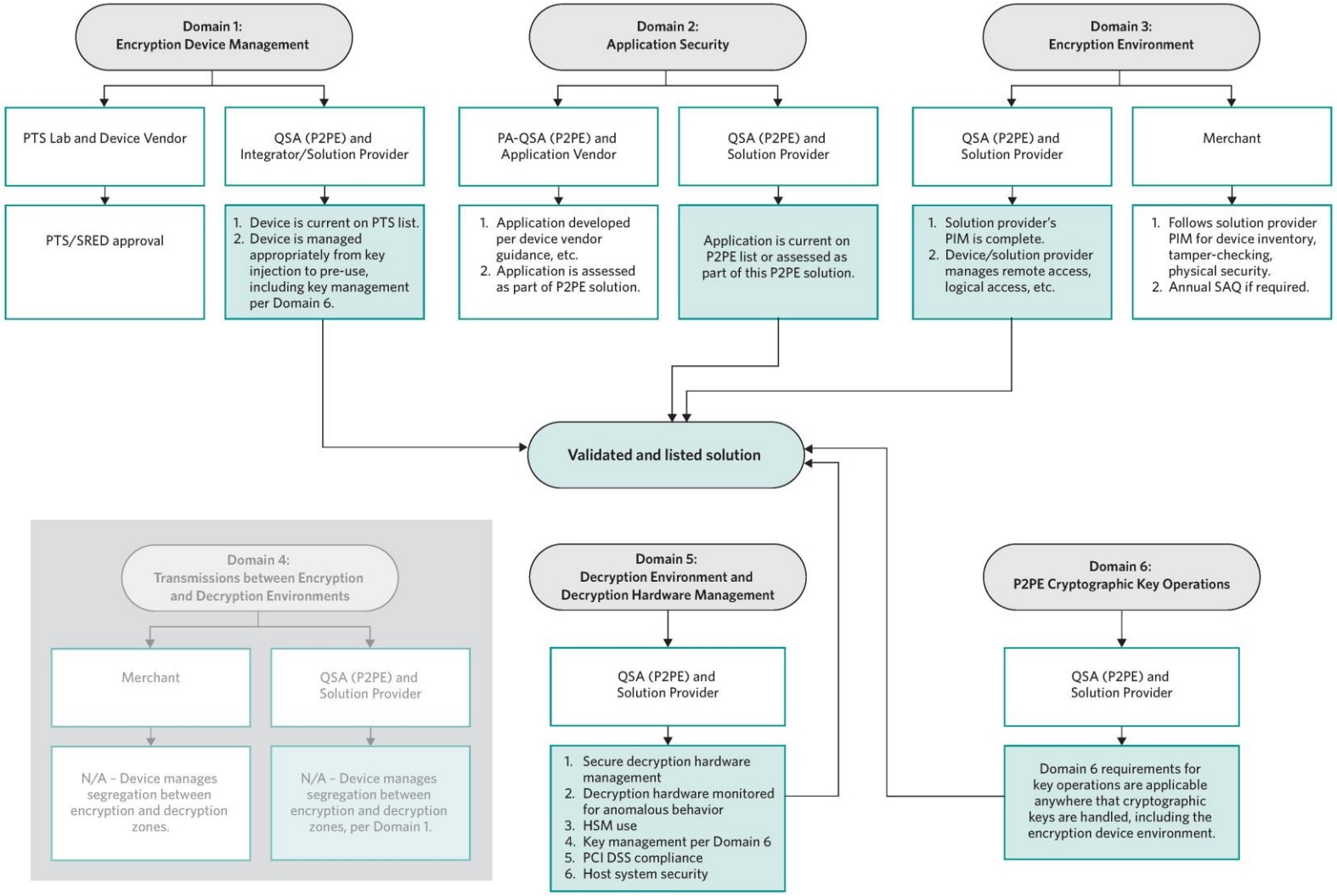
	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 1: Encryption Device Management Use secure encryption devices and protect devices from tampering.	▪ POI is a PCI-approved POI device. ▪ POI device managed by solution provider. ▪ Hardware encryption performed by device.	**1A** Build PCI-approved POI devices. **1B** Securely manage equipment used to encrypt account data.	▪ P2PE Solution Provider
Domain 2: Application Security Secure applications in the P2PE environment.	▪ Application on a PCI-approved POI device. ▪ All applications are assessed as part of the validated P2PE solution.	**2A** Protect PAN and SAD. **2B** Develop and maintain secure applications. **2C** Implement secure application-management processes.	▪ Application Vendor ▪ P2PE Solution Provider

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 3: Encryption Environment Secure environments where POI devices are present.	▪ No storage of CHD after transaction processes are complete. ▪ Within the segmented P2PE environment, no CHD stored, processed, or transmitted through channels or methods external from an approved SCD. ▪ All device-administration and cryptographic operations are managed by solution provider. ▪ The *P2PE Instruction Manual (PIM)* for merchants, with instructions on how to implement and maintain POI devices	**3A** Secure POI devices throughout the device lifecycle. **3B** Implement secure device-management processes. **3C** Maintain *P2PE Instruction Manual* for merchants.	▪ P2PE Solution Provider
Domain 4: Segmentation between Encryption and Decryption Environments Segregate duties and functions between encryption and decryption environments.	▪ All decryption operations managed by solution provider. ▪ Merchant has no access to the encryption environment (within POI device) or decryption environment. ▪ Merchant has no involvement in encryption or decryption operations.	***Domain 4 has no applicable requirements for the hardware/hybrid scenario.***	
Domain 5: Decryption Environment and Device Management Secure decryption environments and decryption devices.	▪ Decryption environment implemented at and managed by solution provider. ▪ Merchant has no access to the decryption environment. ▪ Decryption environment must be PCI DSS compliant.	**5A** Use approved HSMs. **5B** Secure all decryption systems and devices. **5C** Implement secure decryption hardware-management processes. **5D** Maintain secure decryption environment. **5E** Implement secure hybrid decryption process.	▪ P2PE Solution Provider

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 6: P2PE Cryptographic Key Operations Use strong cryptographic keys and secure key-management functions.	▪ All key-management functions implemented and managed by solution provider ▪ Merchant has no involvement in key-management operations.	**6A** Use secure encryption methodologies. **6B** Use secure key-generation methodologies. **6C** Distribute cryptographic keys in a secure manner. **6D** Load cryptographic keys in a secure manner. **6E** Ensure secure usage of cryptographic keys. **6F** Ensure secure administration of cryptographic keys. **6G** Implement secure hybrid key management.	▪ P2PE Solution Provider

At-a-Glance – Steps Required to Create and Validate a P2PE Solution

The process for developing and validating a P2PE solution that uses SCDs for encryption and cryptographic key management and decryption within software, is provided below. This flow chart and the following table illustrate the parties responsible for implementing requirements and validating compliance with each domain, the high-level purpose of controls for each domain, and how validation of each domain can ultimately lead to a P2PE solution validation.



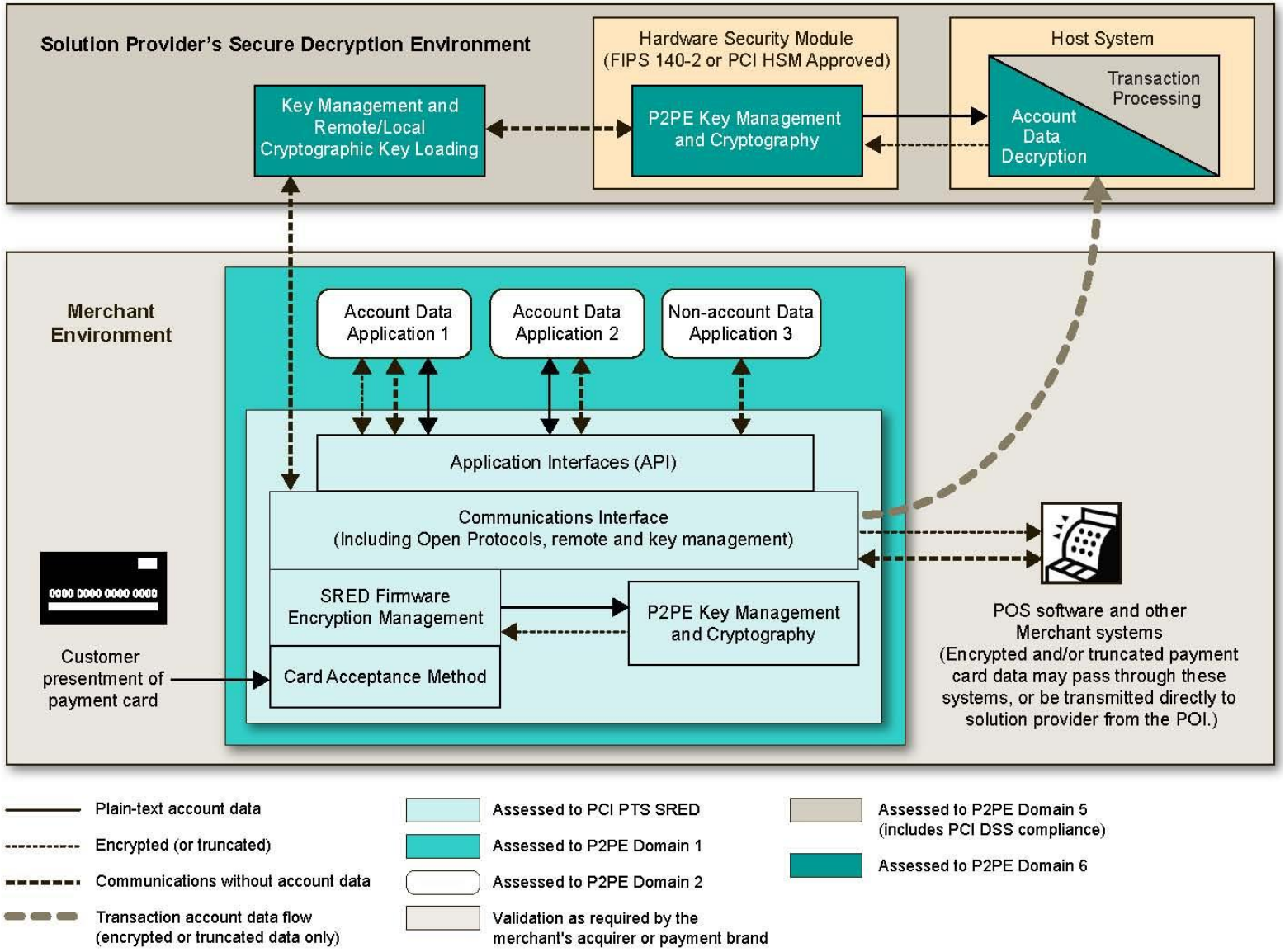
At a Glance – Requirements and Processes for P2PE Solution Validation

Validation Requirements and Process for P2PE Solution Developers and Providers				
Stakeholder	**Step**	**Validation Process**	**Validation Requirements**	**Validation Result**
POI Manufacturer	Design and build a PCI-approved POI device.	PCI PTS lab evaluates all account-data entry methods to ensure that they protect account-data entry, and provide for encryption.	PCI PTS SRED	**PCI PTS listed**
	Securely manufacture and distribute POIs.	Compliance to PCI PTS attested by manufacturer, including the POI device vendor's security guidance. See first step below for solution provider.	PCI PTS	
Application Developer	Produce secure applications for POI.	PA-QSA (P2PE) evaluates all POI applications with access to clear-text account data, and the application developer's *P2PE Implementation Guide(s)*.	PCI P2PE Domain 2	**PCI SSC list of validated P2PE applications**
Solution Provider	Secure environments where encryption devices are present.	QSA (P2PE) ensures solution provider securely manages devices in their possession, and provides merchant instructions via the *P2PE Instruction Manual (PIM)* for security of devices in the merchant's possession.	PCI P2PE Domain 1, Domain 3	**PCI SSC list of validated P2PE solutions**
	Securely install and manage all applications on devices.	PA-QSA (P2PE) ensures solution provider installs and maintains all POI applications securely in accordance with the application developers' *Implementation Guide(s).*	PCI P2PE Domain 2	
	Provide a secure decryption environment for the HSM and the Host System.	QSA (P2PE) evaluates the decryption environment of the solution provider to ensure it secures any decrypted account data.	PCI P2PE Domain 5	
	Provide secure key management for all SCDs (POIs and HSMs) and the Host System.	QSA (P2PE) evaluates the ways in which keys are generated, distributed, loaded, and managed. This includes the loading of any root public keys.	PCI P2PE Domain 6	
	Provide integrated P2PE solution to merchants.	QSA (P2PE) ensures that the overall solution provided to the merchants complies with the above requirements, and provides instructions for secure deployment.	PCI P2PE All Domains	

Validation Requirements and Process for P2PE Solution Developers and Providers				
Stakeholder	**Step**	**Validation Process**	**Validation Requirements**	**Validation Result**
P2PE Merchant	Implement and maintain P2PE systems according to the *P2PE Instruction Manual.*	Merchant's assessor ensures that the P2PE system is implemented per the *P2PE Instruction Manual* provided by the solution provider.	*P2PE Instruction Manual*	**ROC or SAQ and Attestation**
	Validate PCI DSS scope and meet PCI DSS requirements.	Merchant's assessor validates that the merchant's P2PE environment meets the applicable PCI DSS requirements per the reduced validation scope. Any other methods of card acceptance are validated against all applicable PCI DSS requirements.	PCI DSS	

As shown in the above table, a P2PE merchant may be able to reduce PCI DSS scope by implementing a validated P2PE solution, and validating compliance as required by their acquirer or payment brands. However, this scope reduction does not entirely remove or replace all of a merchant's PCI DSS compliance or validation obligations, as defined by the payment brands. Merchants with account-data channels external to the validated P2PE solution will also need to verify that the scope of their PCI DSS assessment is appropriate for their overall validation and, to be eligible for PCI DSS scope reduction due to use of a validated P2PE solution, must ensure that any other payment channels within the merchant environment are adequately segmented (isolated) from the P2PE environment.

At a Glance – Illustration of a Hardware/Hybrid Implementation and Associated Requirements



The above diagram shows an example of a generic P2PE implementation and illustrates which domains apply to each of the areas involved.

It should be noted that this diagram is provided only as an example of one type of scenario that may occur. Many different examples are possible, including where the SRED POI device does not have any applications, and where all functionality is provided by the firmware of the PCI-approved POI device.

Other important requirements of the P2PE requirements illustrated in the diagram include:

1. All key-management and key-loading functions must be implemented within the SRED-approved firmware. Applications must neither bypass these functions, nor provide key-management or key-loading functions themselves.
2. All applications on the device are in scope of the requirements of P2PE Domain 2. This may include traditional payment applications, non-payment applications that may require access to payment data (for example, loyalty applications), as well as applications that are not used for any payment functions and do not access account data. This last group of applications must be evaluated only to verify that they do not access account data in any way, and do not do anything to compromise the security of the device (for example, provide non-approved remote management functions).
3. The POI device only outputs account data that has been encrypted by the approved SRED functions. Applications must not implement their own encryption functions, algorithms, or modes of operation which replace or bypass SRED encryption.
4. Within the P2PE environment, the merchant does not allow for any other method of acceptance of payment card information, except through the PCI-approved POI device.
5. The secure decryption environment is external to the merchant, provided by a P2PE solution provider that also provides the key-management functions for the SCDs. Data sent to the solution provider for decryption may pass through other merchant systems (such as cash registers or internal networks) but there is no possibility that this data may be decrypted within the merchant environment.
6. Although specific message formats can be implemented within an application, all external communications occur through the communications options provided by the combination of PCI-approved POI device hardware and firmware.

The remainder of this document details the P2PE validation requirements for hardware/hybrid solutions on a domain-by-domain basis.

Domain 1: Encryption Device Management

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 1: Encryption Device Management Use secure encryption devices and protect devices from tampering.	▪ POI is a PCI-approved POI device ▪ POI device managed by solution provider. ▪ Hardware encryption performed by PCI-approved POI device.	**1A** Use PCI-approved POI devices **1B** Securely manage equipment used to encrypt account data	▪ P2PE Solution Provider

Domain 1 requirements encompass the use of secure point-of-interaction (POI) devices and the secure management and protection of those POI devices. In a P2PE hardware/hybrid solution, 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 are presented as follows:

- Requirement 1A ensures that the P2PE solution uses only PCI-approved POI devices, and that devices are properly configured for use in the P2PE solution.

- Requirement 1B encompasses solution provider responsibilities for the secure management of POI devices as well as the additional processes and devices involved in preparing, managing, and securing POI devices. These requirements apply to POIs as well as SCDs capable of generating or loading cryptographic keys, encrypting keys, or for signing applications to be loaded onto POI devices. Examples of these SCDs include HSMs, key-injection/loading devices (KLDs) and any other devices used to generate or load keys or sign applications and/or whitelists.

P2PE Domain 1 Requirements	Testing Procedures
Requirement 1A: Use PCI-approved POI devices.	
Account data must be encrypted in equipment that is resistant to physical and logical compromise.	
1A-1 The security characteristics of secure cryptographic devices (SCDs) provide tamper-resistance, detection, and response features to help prevent successful attacks involving penetration, monitoring, manipulation, modification, or substitution of the devices to recover protected data.	
1A-1.1 Encryption operations must be performed using a device approved per the PCI PTS program (for example, a PCI-approved PED or SCR), with SRED (secure reading and exchange of data) listed as a "function provided." The PTS approval listing must match the deployed devices in the following characteristics: • Model name and number • Hardware version number • Firmware version number • Name and application version number of any applications resident within the device that were included in the PTS assessment	**1A-1.1.a** For all types of POI devices used in the solution, examine a sample of devices and device configurations, and review the list of approved PTS devices at www.pcisecuritystandards.org to verify that all POI devices used in this solution are listed, with a valid SSC listing number, on the PCI SSC website as Approved PCI PTS Devices with SRED listed as a "function provided."
	1A-1.1.b Examine POI device configurations and review the PCI SSC list of Approved PCI PTS Devices to verify that all of the following POI device characteristics match the PCI PTS listing for the SRED function of each device: • Model name/number • Hardware version number • Firmware version number • Name and application version number of any applications resident within the device that were included in the PTS assessment
1A-1.1.1 SRED capabilities must be enabled and active.	**1A-1.1.1.a** Examine the solution provider's documented procedures 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 environments.
	1A-1.1.1.b Interview personnel and observe processes to verify that the implemented processes include ensuring that SRED capabilities are enabled and active on all devices prior to devices being deployed to merchant environments.

P2PE Domain 1 Requirements	Testing Procedures
	1A-1.1.1.c For a sample of all POI devices used in the solution, review POI device configurations to verify that all POI devices 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 environments.
1A-1.2 POIs must be configured to use only SRED-validated capture mechanisms for accepting and processing P2PE transactions. *For example, if a PCI-approved secure card reader (SCR) is provided with other POI components, the PCI-approved SCR must be the only capture mechanism used for P2PE transactions.*	**1A-1.2.a** Examine documented deployment procedures to verify that POIs must be configured to use only SRED-validated capture mechanisms for accepting and processing P2PE transactions.
	1A-1.2.b For all types of POI devices used in the solution, examine a sample of device configurations to verify that only SRED-validated capture mechanisms are configured to accept P2PE transactions.
1A-1.2.1 All capture mechanisms provided by the solution provider that are not SRED validated must be disabled or otherwise prevented from being used for P2PE transactions, and 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 environments.
	1A-1.2.1.c For all types of POI devices used in the solution, examine a sample of device configurations to 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 environments. • Disabled capture mechanism 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 Clear-text account data must not be disclosed to any component or device outside of the PCI-approved POI device prior to being transmitted to the solution provider's decryption environment.	**1A-1.3.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 prior to being transmitted to the solution provider's decryption environment.

P2PE Domain 1 Requirements	Testing Procedures
	1A-1.3.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 prior to being transmitted to the solution provider's decryption environment.
1A-1.3.1 Any cryptographic keys that can be used to decrypt account data must not exist on any device outside of the PCI-approved POI device or the solution provider's decryption environment.	**1A-1.3.1.a** Examine documented key-management policies and procedures to verify cryptographic keys that can be used to decrypt account data must not exist on any device outside of the PCI-approved POI or the solution provider's decryption environment.
	1A-1.3.1.b Examine documented data flows and observe a sample of transactions to verify cryptographic keys that can be used to decrypt account data do not exist on any device outside of the PCI-approved POI, other than within the solution provider's decryption environment.

Requirement 1B: Securely manage equipment used to encrypt account data.

Note: *this requirement applies to POIs as well as SCDs used to generate or load keys or sign applications and/or whitelists for POIs. Examples include HSMs, key-injection/loading devices (KLDs) and signing devices.*

Equipment used to protect account data must not be placed into service unless there is assurance that it has not been modified, tampered with, or in any way deviates from the configuration that has been assessed and approved as part of this program.

1B-1 Employ device management at initial key-loading facility and pre-use until placed into service, and for any POI devices returned to the key-management facility, or the vendor or their agent, for repair or other disposition.	
1B-1.1 POIs and other SCDs 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 loading of cryptographic keys.	**1B-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 signing have not been substituted or subjected to unauthorized modifications or tampering.

P2PE Domain 1 Requirements	Testing Procedures
	1B-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 signing have not been substituted or subjected to unauthorized modifications or tampering.
1B-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:	**1B-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.
	1B-1.1.1.b Verify that documented procedures include 1B-1.1.1.1 through 1B-1.1.1.3 below.
1B-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.	**1B-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.
	1B-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.
	1B-1.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI or other SCD.
1B-1.1.1.2 POIs and other SCDs do not use default keys (such as keys that are pre-installed for testing purposes) or passwords.	**1B-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.
1B-1.1.1.3 All personnel with access to POIs and other SCDs are documented in a formal list and authorized by management.	**1B-1.1.1.3.a** Examine documented authorizations to verify: • 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.

P2PE Domain 1 Requirements	Testing Procedures
	1B-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.
1B-1.2 Protect SCDs from unauthorized access, modification, or substitution, from receipt through to installation and use.	
1B-1.2.1 A documented "chain-of-custody" process must be in place to ensure that all POIs and other SCDs are controlled from receipt through to installation and use. The chain of custody must include records to identify personnel responsible for each interaction with the devices.	**1B-1.2.1.a** Examine documented procedures to verify that a chain-of-custody process is required for all POIs and other SCDs from receipt through to installation and use.
	1B-1.2.1.b For a sample of POIs and other SCDs, review documented records and interview responsible personnel to verify that chain of custody is maintained from receipt through to installation and use for: • All POIs • All devices used for key injection/loading or signing
	1B-1.2.1.c Verify the chain-of-custody records identify personnel responsible for each interaction with the devices.
1B-1.2.2 Controls, including the following, must be in place to ensure that all installed devices are from a legitimate source:	**1B-1.2.2.a** Examine documented purchasing, receipt, and deployment procedures to confirm that controls are defined for ensuring that all received devices are from a legitimate source.
	1B-1.2.2.b Confirm that the documented procedures include 1B-1.2.2.1 through 1B-1.2.2.2 below.
1B-1.2.2.1 Device serial numbers must be compared to the serial numbers documented by the sender to ensure device substitution has not occurred. A record of device serial-number validations must be maintained. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document.*	**1B-1.2.2.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender for all POIs and other SCDs.
	1B-1.2.2.1.b For a sample of received POIs and other SCDs, observe records of serial-number validations to verify: • Device serial numbers for the received device were verified to match that documented by the sender. • Records of serial-number verifications are maintained.

P2PE Domain 1 Requirements	Testing Procedures
1B-1.2.2.2 Documentation used for validating device serial numbers must be received via a separate communication channel and must not have arrived with the device shipment.	**1B-1.2.2.2** For a sample of received POIs and other SCDs, review delivery records and interview responsible personnel to verify that documentation used to validate the device serial numbers was received via a separate communication channel than the device and was not received in the same shipment as the device.
1B-1.3 Dual-control mechanisms must exist to help prevent substitution of POIs and other SCDs. This applies to both in-service and spare or backup devices. ***Note:*** *Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted cryptographic devices, but cannot supplant the implementation of dual-control mechanisms.*	**1B-1.3.a** Examine documented procedures to verify that dual-control mechanisms are defined to: • Prevent substitution of POIs, both in-service and spare or backup devices. • Prevent substitution of SCDs, both in-service and spare or backup devices.
	1B-1.3.b Examine dual-control mechanisms in use to verify that the mechanisms: • Prevent substitution of POIs, both in-service and spare or backup devices. • Prevent substitution of key injection/loading devices, both in-service and spare or backup devices.
1B-1.4 Implement physical protection of POIs and other SCDs 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 (for example, via bonded carrier). The devices are then securely stored until key-insertion occurs. • Use of physically secure and trackable packaging (for example, 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 SCD 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.	**1B-1.4.a** Examine documented procedures to verify they require physical protection of POIs and other SCDs, from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the defined methods.
	1B-1.4.b Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for POIs and other SCDs, from the manufacturer's facility up to the point of key-insertion.
	1B-1.4.c For a sample of received POIs and other SCDs, observe processes and physical protections in use (for example, storage locations, packaging, device configurations), to verify that the defined methods are implemented for POIs and other SCDs, up to the point of key-insertion.
1B-1.5 Inspect and test all POIs and other SCDs immediately prior to key-insertion to ensure that devices are legitimate and have not been subject to any unauthorized modifications. Procedures must include the following:	**1B-1.5.a** Examine documented procedures to verify they require inspection and testing of POIs and other SCDs immediately prior to key-insertion, to ensure that devices are legitimate and have not been subject to any unauthorized modifications.

P2PE Domain 1 Requirements	Testing Procedures
	1B-1.5.b Verify documented procedures include 1B-1.5.1 through 1B-1.5.4 below.
1B-1.5.1 Running self-tests to ensure the correct operation of the device.	**1B-1.5.1** Examine records of device inspections and tests, and observe tests in progress to verify that self-tests are run on POIs and other SCDs to ensure the correct operation of the device.
1B-1.5.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.	**1B-1.5.2** 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.
1B-1.5.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed.	**1B-1.5.3** 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.
1B-1.5.4 Maintaining records of the tests and inspections, and retaining records for at least one year.	**1B-1.5.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	1B-1.5.4.b Examine records of inspections to verify records are retained for at least one year.
1B-1.6 Maintain inventory-control and monitoring procedures to accurately track device locations from receipt of the device until ready to ship. The inventory-control and monitoring procedures must provide for the following:	**1B-1.6.a** Examine documented inventory-control and monitoring procedures to confirm they define methods for tracking device locations from receipt until the device is ready to ship.
	1B-1.6.b Verify documented procedures include 1B-1.6.1 through 1B-1.6.3 below.
	1B-1.6.c For a sample of devices, review the documented device inventory and observe device locations to verify that the inventory-control and monitoring procedures accurately track device locations.
1B-1.6.1 As soon as possible upon receipt and no later than key loading, the device serial number is entered into the inventory-control system.	**1B-1.6.1** Review documented device inventories and interview personnel to verify that devices are entered into the inventory-control system as soon as possible after receipt of the device, and no later than key loading.

P2PE Domain 1 Requirements	Testing Procedures
1B-1.6.2 Devices are protected against unauthorized substitution or modification until all applicable keys have been loaded. ***Note**: This includes any cryptographic keys needed for the operation of the device and any keys used to encrypt account data.*	**1B-1.6.2** Review implemented controls and interview personnel to verify that devices are protected against unauthorized substitution or modification until all applicable keys have been loaded.
1B-1.6.3 Control and monitoring procedures must provide for detection of lost or stolen equipment and notification to authorized personnel.	**1B-1.6.3** Review implemented controls and interview personnel to verify that procedures are implemented to detect lost or stolen devices and notify authorized personnel.
1B-1.7 When the POI is shipped from the key-loading facility to the initial point of use (or an intermediary facility), procedures are implemented to ensure that the device is tracked and that it arrives unaltered at its destination.	**1B-1.7** Examine documented procedures, interview responsible personnel, and observe processes for shipping POI devices to verify that the following are in place: • Controls to ensure that device location is known and tracked throughout the entire shipping process • Controls to ensure devices arrive unaltered
1B-1.7.1 If POI devices are stored en route, processes must be in place to account for the location of every device at any point in time.	**1B-1.7.1** Examine device shipping procedures and records, and interview personnel to determine if POI devices are stored en route. If devices are stored en route, examine device shipping records for a sample of POIs and interview personnel to verify processes are in place to account for the location of every device at any point in time.
1B-1.7.2 Documented procedures are in place and implemented to transfer accountability for POI devices from the key-loading facility.	**1B-1.7.2** For a sample of POI devices, examine device shipping records and interview personnel to verify accountability for the device is formally transferred from the key-loading facility to the destination.
1B-2 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.	
1B-2.1 Procedures are in place to ensure that any SCDs to be removed from service, retired, or returned for repair are not intercepted or used in an unauthorized manner, as follows:	**1B-2.1.a** Examine documented procedures to verify that procedures are defined for any SCDs to be removed from service, retired, or returned for repair.
	1B-2.1.b Verify documented procedures include 1B-2.1.1 through1B-2.1.5 below.

P2PE Domain 1 Requirements	Testing Procedures
1B-2.1.1 Affected entities are notified before devices are returned.	**1B-2.1.1** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
1B-2.1.2 Devices are transported via trusted carrier service—for example, bonded carrier.	**1B-2.1.2** Interview responsible personnel and examine device-return records to verify that devices are transported via trusted carrier service—for example, bonded carrier.
1B-2.1.3 Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	**1B-2.1.3** Interview responsible personnel and observe device-return processes and packaging to verify that devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.
1B-2.1.4 Devices are tracked during the return process.	**1B-2.1.4** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process
1B-2.1.5 Once received, devices remain in their packaging (as defined in 1B-2.1.3) until ready for repair or destruction.	**1B-2.1.5** Interview responsible personnel and observe device-return processes to verify that once received, devices remain in their packaging (defined in 1B-2.1.3) until ready for destruction.
1B-2.2 When SCDs are removed from service, permanently or for repair, all keys and key material, and all 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.*	**1B-2.2** 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 include 1B-2.2.1 through 1B-2.2.4 below.
1B-2.2.1 Dual control is implemented for all critical decommissioning processes.	**1B-2.2.1** Interview personnel and observe processes for removing SCDs from service to verify that dual control is implemented for all critical decommissioning processes.
1B-2.2.2 Key and data storage (including account data) are rendered irrecoverable (for example, zeroized). If data cannot be rendered irrecoverable, devices must be physically destroyed to prevent the disclosure of any sensitive data or keys.	**1B-2.2.2** Interview personnel and observe processes for removing SCDs from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed to prevent the disclosure of any sensitive data or keys.

P2PE Domain 1 Requirements	Testing Procedures
1B-2.2.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	**1B-2.2.3** 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.
1B-2.2.4 Records of the tests and inspections (as required in 1B-2.2.3) are maintained for at least one year.	**1B-2.2.4** Interview personnel and observe records to verify that records of the tests and inspections (as required in 1B-2.2.3) are maintained for at least one year.
1B-3 Any SCD capable of generating or loading cryptographic keys, encrypting keys, or signing applications to be loaded onto a POI device, is protected against unauthorized use. *This requirement applies to HSMs, key-injection/loading devices (KLDs) and any other devices used to generate or load keys or to sign applications or whitelists for loading onto POIs.*	
1B-3.1 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 a POI device, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:	**1B-3.1.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 a POI device.
	1B-3.1.b Verify that documented procedures include 1B-3.1.1 through 1B-3.1.4 below.
1B-3.1.1 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.*	**1B-3.1.1** 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.
1B-3.1.1.1 Passwords used for dual control must each be of at least five decimal digits (or an equivalent size).	**1B-3.1.1.1** Observe password policies and configuration settings to confirm that passwords used for dual control must be at least five decimal digits (or an equivalent size).

P2PE Domain 1 Requirements	Testing Procedures
1B-3.1.2 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.	**1B-3.1.2** 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.
1B-3.1.3 Devices must not use default passwords.	**1B-3.1.3.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.
	1B-3.1.3.b Observe device configurations and interview device administrators to verify HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords.
1B-3.1.4 To detect any unauthorized use, devices are at all times either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people.	**1B-3.1.4.a** Examine documented procedures to confirm that they require devices 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.
	1B-3.1.4.b Interview responsible personnel and observe devices and processes to confirm that devices 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.

P2PE Domain 1 Requirements	Testing Procedures
1B-4 Documented procedures exist and are demonstrably in use to ensure the security and integrity of SCDs placed into service, initialized, deployed, used, and decommissioned.	
1B-4.1 All affected parties are aware of required processes and provided suitable guidance on the secure procedures for devices placed into service, initialized, deployed, used, and decommissioned.	**1B-4.1** 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
1B-4.2 Procedures that govern access to SCDs, including HSMs, key-injection/loading devices (KLDs), and any other devices used to generate or load keys or sign applications for loading onto POIs, must be documented, implemented, and known to data-center personnel and any others involved with the physical security of such devices. HSM protections must include at least the following:	**1B-4.2.a** Examine documented procedures to verify that procedures are defined that govern access to all SCDs.
	1B-4.2.b Verify that procedures governing access to HSMs include at least those defined in Requirements 1B-4.2.1 – 1B-4.2.4 below.
	1B-4.2.c Interview data-center personnel and others responsible for the physical security of the devices to verify that the documented procedures are known.
1B-4.2.1 Any physical keys needed to activate the HSM are stored securely.	**1B-4.2.1** Interview responsible personnel and observe key-storage locations and security controls to verify that any physical keys needed to activate the HSM are stored securely.
1B-4.2.2 If multiple physical keys are needed to activate the HSM: • They are assigned to separate designated custodians, and • Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.	**1B-4.2.2** If multiple physical keys are needed to activate the HSM, interview responsible personnel and observe key operations to verify that: • Keys are assigned to separate designated custodians, and • Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys
1B-4.2.3 Anti-tamper sensors are enabled as required by the security policy of the HSM.	**1B-4.2.3** Examine HSM security policy and HSM anti-tamper controls to verify that anti-tamper sensors are enabled as required by the security policy of the HSM.

P2PE Domain 1 Requirements	Testing Procedures
1B-4.2.4 When HSMs are connected to online systems, they are not enabled in a sensitive state. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	**1B-4.2.4** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.

Domain 2: Application Security

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 2: Application Security Secure applications in the P2PE environment.	▪ Applications on a PCI-approved POI device. ▪ All applications are assessed as part of the validated P2PE solution	**2A** Protect PAN and SAD. **2B** Develop and maintain secure applications. **2C** Implement secure application-management processes.	▪ Application Vendor ▪ P2PE Solution Provider

Although POIs are often considered as "hardware" devices, many POIs will allow for the loading and execution of software applications that are added after the PTS evaluation and approval (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 applications have been assessed to confirm their secure operation. To this end, P2PE requirements specify both the confirmation that a PCI-approved POI device is in use (Domain 1), as well as the independent assessment of all software applications that are resident within the POI (Domain 2). However, it is also recognized that "simple" POIs may exist that do not provide for any applications and that implement all functionality within the PCI-approved POI device hardware and firmware combination; in these cases Domain 2 may be not applicable to those POI devices.

The PTS evaluation of a PCI-approved POI device includes all firmware in the device. When used in a P2PE solution, all software implemented on the POI must also be assessed and confirmed to be secure. These Domain 2 "applications" may not be "payment applications" as traditionally defined by PA-DSS since they may not store, process, or transmit account data as part of authorization or settlement. Rather, these applications, which are installed on the POI according to the POI device vendor's security guidance, may be developed specifically for each solution provider for tasks performed before authorization begins. For example, the PCI-approved firmware may release clear-text account data to an application for formatting of the payment message for routing or other purposes. Once the application processing is completed, the account data is returned to the secure controller of the device for encryption or secure deletion.

As part of a P2PE solution validation, all applications with access to clear-text account data must undergo validation per Domain 2 requirements. "Traditional" payment applications as defined by PA-DSS would also require validation against Domain 2 if they are present on a PCI-approved POI device as part of a P2PE solution. Requirements in Domain 2 must be assessed by a PA-QSA (P2PE) and entail protecting PAN and SAD, developing and maintaining secure applications, and incorporating secure application-management processes.

In certain circumstances, where a POI is also used to accept non-PCI payment-branded accounts/cards such as loyalty cards, it may be necessary for the POI to allow for the output of this account data in clear text. This is acceptable if—and only if—there is a secure method implemented within the POI to allow for the differentiation of PCI payment-branded accounts/cards, which require encryption, from other types of cards, which may be output as clear text.

Note: *For applications on PCI-approved POI devices that* ***never have access to account data,*** *only Requirement 2A-3 is applicable—this will validate that these applications are not accessing account data, and are not bypassing or overriding any security features provided by the other approved components of the device.*

Note that the Domain 2 Testing Procedures are presented in two columns below: one for the application vendor assessment and one for the solution provider assessment.

Applications with access to clear-text account data must undergo validation per Domain 2 requirements, and either: 1) become listed on the list of validated P2PE applications (if the application will be used in multiple solutions); or 2) optionally be listed only as a component of a validated P2PE solution. There are essentially three approaches for a Domain 2 assessment:

1. For a P2PE application to be included on PCI SSC's list of validated P2PE applications, a PA-QSA (P2PE) would, at a minimum, perform the procedures noted in the "Application Vendor" column and submit the resulting Domain 2 Application P2PE Report on Validation (P-ROV) to PCI SSC for review and listing.
2. When an already-listed application is implemented into a P2PE solution, the P2PE assessor would only perform the procedures noted in the "Solution Provider" column as part of the solution validation. The resulting P2PE solution listing will include all applications included in the assessment.
3. For applications either not already on the list of validated P2PE applications or not intended to be included on that list (for example, if that application is unique or customized for only one solution), then the P2PE assessor(s) would perform both columns as part of a single P2PE solution review. Again, the resulting P2PE solution listing will include all applications included in the assessment. Whether applications reviewed as part of the full P2PE solution assessment are also separately listed as a validated P2PE application is up to the application vendor.

In all cases, the P2PE assessor submits the resulting P2PE P-ROV and any separate Domain 2 Application P-ROVs to PCI SSC in accordance with the *P2PE Program Guide*.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
Requirement 2A: Protect PAN and SAD.		
The application protects PAN and SAD.		
2A-1 The application does not retain PAN or SAD after application processing is completed.		
2A-1.1 The application does not store PAN or SAD data after processing is completed (even if encrypted). *Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (for example, offline transactions). However, at all times, SAD is not stored after the completion of the transaction.*	**2A-1.1.a** Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains a detailed description of the function of the application, including: • How it uses PAN or SAD for its application processing, and • How it ensures the application does not store PAN or SAD after the application's processing is complete.	**2A-1.1** 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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that PAN and SAD are not stored after application processing is completed.
	2A-1.1.b Perform a source-code review to verify that the application is coded such that PAN and SAD are not stored after application processing is completed.	
	2A-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 examine all output created by the application and verify that, by following the *Implementation Guide* instructions, PAN and SAD are not stored after application processing is completed.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-1.2 A process is in place to securely delete any PAN or SAD stored during application processing.	**2A-1.2.a** Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it describes the methodology or process used by the application to securely delete any PAN or SAD if stored during application processing.	**2A-1.2** 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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that all stored PAN and SAD are rendered irrecoverable.
	2A-1.2.b Perform a source-code review and verify that the methodology or process provided by the application vendor renders all stored PAN and SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data.	
	2A-1.2.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 examine all output created by the application and verify that, by following the *Implementation Guide* instructions, that the methodology or process provided by the application vendor renders all PAN and SAD data irrecoverable, in accordance with industry-accepted standards for secure deletion of data, once the business process of the application is completed.	
2A-2 The application does not transmit clear-text PAN or SAD outside of the device, and only uses communications methods included in the scope of the PCI-approved POI device evaluation.		

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-2.1 The application only exports PAN or SAD data that has been encrypted by the firmware of the PCI-approved POI device, and does not export clear-text PAN or SAD outside of the 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-2.4.*	**2A-2.1.a** Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains a description of the application's function including the following: • That the application does not output clear-text account data outside of the device; • Whether the application passes encrypted account data outside of the device; and • If the application passes encrypted account data outside of the device, that the application only exports PAN or SAD that has been encrypted by the approved SRED functions of the PCI-approved POI device.	**2A-2.1** 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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that the application does not output clear-text account data outside of the device.
	2A-2.1.b Perform a source-code review and verify that the application never outputs clear-text account data outside of the device.	
	2A-2.1.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 examine all output created by the application and verify that, by following the *Implementation Guide* instructions, the application does not output clear-text account data outside of the device.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-2.2 The application only uses internal communication methods (including all inter-process communication and authentication methods) included in the PCI-approved POI device evaluation. These internal communication methods must be documented. ***Note:*** *This applies to all internal communications within the device, including when account data is passed between applications, or to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI.*	**2A-2.2.a** Examine the POI device vendor's security guidance to determine which internal communication methods (including for authentication) are approved in the PCI-approved POI device evaluation. Review the application's *Implementation Guide* required at 2C-3 of this document and confirm that it includes the following: • A list of internal communication methods included in the POI device vendor's security guidance • A list of which approved internal communications methods are used by the application. • A description of where internal communications are used by the application to pass clear-text account data within the device (for example, from the application to other applications, to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI) • How to configure the application to use the approved internal communication methods • Guidance that use of any other method for internal communication is not allowed.	**2A-2.2.a** Examine solution provider's documentation that shows all applications, data flows, interactions, etc., within POI devices to verify that all internal communication and authentication methods are documented in accordance with the application's *Implementation Guide*.
	2A-2.2.b Perform a source-code review and verify that the application only uses those inter-process communication methods approved as part of the PCI-approved POI device evaluation.	**2A-2.2.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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine the dataflow during transactions to verify that the application only uses inter-process communication methods approved as part of the PCI-approved POI device evaluation.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2A-2.2.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 examine all output created by the application and verify that, by following the *Implementation Guide*, the application only uses approved inter-process communications methods (including authentication methods) for all communications within the device, including; • All flows and storage of clear-text account data, between applications • All flows and storage of clear-text account data between the application and the approved firmware of the POI.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-2.3 The application only uses external communication methods included in the PCI-approved POI device evaluation. *For example, the POI may provide an IP stack approved per the PTS Open Protocols module that allows for the use of the SSL/TLS protocol, 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.* Security of applications where the POI device implements an IP stack is covered at Requirement 2B-2.1.	**2A-2.3.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 *Implementation Guide* required at 2C-3 of this document and verify that it contains the following instructions and that they are consistent with the POI device vendor's security guidance: • A list of the external communication methods included in the POI device vendor's security guidance • A list of which approved external communications methods are used by the application • A description of where external communications are used by the application • Instructions for how to configure the application to use only those approved methods • Guidance that use of any other methods for external communications is not allowed	**2A-2.3.a** Examine solution provider's documentation that shows all applications, data flows, interactions, etc., within POI device to verify that all external communication methods are documented and in accordance with the application's *Implementation Guide*.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2A-2.3.b Perform a source-code review and verify that the application does not implement its own external communication methods (for example, does not implement its own IP stack).	**2A-2.3.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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine communication methods to verify that the application does not use any communication methods that were not approved as part of the PCI-approved POI device evaluation.
	2A-2.3.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 examine all output created by the application and verify that, by following the *Implementation Guide*: • The application uses only the external communication methods included in the POI device vendor's security guidance for all external communications.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-2.4 Ensure that any application functions (for example, "whitelists") that allow for the output of clear-text data limits that output to *only* non-PCI payment brand accounts/cards, and that additions or changes to application functions are implemented as follows: • Cryptographically authenticated by the PCI-approved POI device's firmware • Implemented only by authorized personnel • Documented as to purpose and justification • Reviewed and approved prior to implementation ***Note:*** *Requirement 2C-2.1.2 prohibits unauthenticated changes or updates to applications or application functions (for example, "whitelists").*	**2A-2.4.a** Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains details to describe any application functions that allow for the output of clear-text card data (for example, through the use of "whitelists" of BIN ranges), and provides instructions as follows: • Any such application functions are *only allowed* for non-PCI payment brand accounts/cards. • How to establish application authentication using strong cryptography, with the approved SRED firmware of the POI device. • Only authorized personnel must be used for signing and adding application functions for output of clear-text data.	**2A-2.4.a** Interview solution-provider personnel and review documented procedures to verify that any application functions that output clear-text card data are implemented as follows: • Only non-PCI payment brand accounts/cards are output in clear-text from such application functions • Cryptographic authentication between the device and the application functions are established in accordance with device vendor's security guidance. • Only authorized personnel are allowed to initiate cryptographic authentication to sign or add application functions for output of clear-text data. • Records are maintained of any changes/additions, including description and justification for the function added, who authorized it, and confirmation that it was reviewed to only output non-PCI payment accounts/cards.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2A-2.4.b Perform a source-code review and verify that the application functions are limited as follows: • The application is able to limit output to non-PCI payment brand accounts/cards only. • The application requires use of the PCI-approved POI device's firmware for cryptographic authentication.	**2A-2.4.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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device output sources to verify the application meets the following: • Only outputs clear-text data for non-PCI payment brand accounts/cards. • Cryptographic authentication is correctly established for any application functions, using the PCI-approved POI device's firmware for cryptographic authentication.
	2A-2.4.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 examine all output created by the application and verify that, when the *Implementation Guide* is followed, the following is in place: • Output of clear-text data is allowed only for non-PCI payment brand accounts/cards. • Application functions are authenticated using strong cryptography by the approved SRED firmware of the POI device.	**2A-2.4.c** Review records of changes/additions, and confirm that all changes/additions to application functions are documented, and that the documentation includes description and justification for the function added, who authorized it, and confirmation that it was reviewed to only output non-PCI payment accounts/cards.
2A-3 All applications without a business need do not have access to account data. ***Note:*** *Requirements at 2A-3 are the only requirements applicable to applications on PCI-approved POI devices with no access to account data (for example, a loyalty or advertising application).*		

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2A-3.1 Applications on the device that do not have a business need to access account data must only communicate with the device via application program interfaces (APIs) provided by the SRED firmware that do not provide access to account data.		**2A-3.1.a** Examine the POI device vendor's security guidance to identify which APIs are intended for use by applications that do not need access to account data. Review the solution provider's documented processes, and confirm the following is included: • A list of all APIs and their functions, including which give access to account data and which do not • Confirmation that the function of each API in the solution provider's documentation matches the POI device vendor's security guidance • A list of all applications and which APIs each use • Documented business need for all applications on the device with access to account data • Confirmation that any applications without a business need for access to account data only use those APIs that do not give access to account data
		2A-3.1.b Interview solution-provider personnel and observe device operations to verify that that any applications that do not have a need to access clear-text account data only use the APIs specified in the POI device vendor's security guidance that do not provide access to clear-text account data.
2A-3.2 All applications on the device that do not have a business need to access account data are authenticated with an approved security protocol of the POI.		**2A-3.2.a** Review the solution provider's documented processes to confirm that applications with no need to see clear-text data must be authenticated using an approved security protocol of the POI.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
		2A-3.2.b Interview solution-provider personnel and observe device operations to verify that applications with no need to access clear-text account data are authenticated to the device using an approved security protocol.
2A-3.3 For applications that do not need access to account data, dual control is required for the application-signing process.		**2A-3.3.a** Review the solution provider's documented processes to confirm that dual control is required to authenticate applications with no need to see clear-text data.
		2A-3.3.b Interview solution-provider personnel and observe an application update to confirm that application signing is done under dual control.

Requirement 2B: Develop and maintain secure applications.

The application is developed securely and in accordance with industry standards.		
2B-1 The application is developed according to industry-standard software development life cycle practices that incorporate information security.		
2B-1.1 Applications are 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 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	**2B-1.1** Review the solution provider's documented processes, and confirm they follow any guidance specified in the *Implementation Guide* related to configuring the application on the device.
	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.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	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 (for example, 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 • Interview software developers • Examine the application product	
2B-1.1.1 Live PANs are not used for testing or development.	**2B-1.1.1** Live PANs or SAD are not used for testing or development.	
2B-1.1.2 Test data and accounts are removed before release to customer.	**2B-1.1.2** Test data and accounts are removed before release to customer.	
2B-1.1.3 Custom application accounts, user IDs, and passwords are removed before applications are released to customers	**2B-1.1.3** Custom application accounts, user IDs, and passwords are removed before applications are released to customers.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-1.2 Application code and any non-code configuration options, such as "whitelists," are reviewed prior to release and after any significant change, using manual or automated vulnerability-assessment processes to identify any potential vulnerabilities or security flaws. The review process includes the following:	**2B-1.2** Confirm the developer performs reviews for all significant application code changes and alterations to code that manages security-sensitive configuration options, such as card "whitelists" (either using manual or automated processes), as follows:	**2B-1.2** Review the solution provider's documented processes and interview solution-provider personnel, and confirm the following processes are in place: • Changes to application "whitelists" are reviewed prior to release and after any significant change to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Changes to application "whitelists" are reviewed for any potential vulnerabilities or security flaws, using manual or automated vulnerability-assessment processes. • Found vulnerabilities are corrected and updated for applications in the field (installed on devices) after vulnerabilities are found, when the application vendor provides an update, or when the software vendor notifies the solution provider of a vulnerability that the solution provider needs to address.
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** Code changes are reviewed 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** 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, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device output sources to verify that any changes to "whitelists" do not result in the exposure of PCI payment-brand accounts/cards.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-1.2.2 Review of changes to security-sensitive configuration options, such as whitelists, to confirm that they will not result in the exposure of PCI payment-brand accounts/cards.	**2B-1.2.2** Changes to code that manages security-sensitive configuration options, such as whitelists, are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards.	
2B-1.2.3 Performing code reviews to ensure code is developed according to secure coding guidelines.	**2B-1.2.3** Code reviews ensure code is developed according to secure coding guidelines.	
2B-1.2.4 Confirming that appropriate corrections are implemented prior to release.	**2B-1.2.4** Appropriate corrections are implemented prior to release.	
2B-1.2.5 Review and approval of review results by management prior to release.	**2B-1.2.5** Review results are reviewed and approved by management prior to release.	
2B-1.3 Develop applications based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes.	**2B-1.3.a** Obtain and review software development processes for applications. Verify the process includes training in secure coding techniques for developers, based on industry best practices and guidance.	**2B-1.3** 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, all applications are installed on the device). Verify that the device and applications are not vulnerable to common 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-1.3.b Interview a sample of developers to confirm that they are knowledgeable in secure coding techniques.	
	2B-1.3.c 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).	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-1.4 All changes to application must follow change-control procedures. The procedures must include the following:	**2B-1.4.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	**2B-1.4** 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. • Any changes to applications include documented approval by appropriate authorized solution-provider personnel. • Any changes to applications are documented as to reason and impact of the change.
	2B-1.4.b Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it includes the following: • Documentation about the impact of the change • Instructions about how to back out or de-install applications.	
	2B-1.4.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-1.4.1 Documentation of impact	**2B-1.4.1** Verify that documentation of customer impact is included in the change-control documentation for each change.	
2B-1.4.2 Documented approval of change by appropriate authorized parties	**2B-1.4.2** Verify that documented approval by appropriate authorized parties is present for each change.	
2B-1.4.3 Functionality testing to verify that the change does not adversely impact the security of the device	**2B-1.4.3.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.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2B-1.4.3.b Verify that all changes (including patches) are tested per secure coding guidance before being released.	
2B-1.4.4 Back-out or application de-installation procedures	**2B-1.4.4** Verify that back-out or product de-installation procedures are prepared for each change.	
2B-2 The application is implemented securely, including the secure use of any resources shared between different applications.		
2B-2.1 The application is developed in accordance with the POI device vendor's security guidance, including specifying that If an application uses an IP stack, it must use the IP stack approved as part of the PCI-approved POI device evaluation. ***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** Examine the POI device vendor's security guidance to determine which IP stack was approved via the PCI-approved POI device evaluation. Review the application's *Implementation Guide* required at 2C-3 of this document and confirm it includes the following: • A description of the IP stack implemented in the POI device • Confirmation that the IP stack used by the application is the same one included in the POI device vendor's security guidance.	**2B-2.1** Interview solution-provider personnel to determine that they have used only the approved IP stack, and that they have implemented the application in accordance with the *Implementation Guide.*

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-2.1.1 If an application uses the POI device's IP stack and any of the related OP services, the application must securely use, and integrate with, the following device platform components in accordance with the POI device vendor's security guidance, including but not limited to the following: • IP and link layer (where implemented by the POI) • IP protocols (where implemented by the POI) • Security protocols, including specific mention if specific security protocols or specific configurations of security protocols are not to be used for financial applications and/or platform management • IP services, including specific mention if specific IP services or specific configurations of IP services are not to be used for financial applications and/or platform management (where implemented by the POI) • For each platform component listed above, follow the POI device vendor's security guidance, as applicable to the application's specific business processing, with respect to the following: ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication	**2B-2.1.1.a** Examine the POI device vendor's security guidance to determine the following: • The IP stack approved via the PCI-approved POI device evaluation • Any specific guidance from the POI device vendor's security guidance that needs to be implemented for the application 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: • A description of the IP stack implemented in the POI device and included in 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, including: ○ Vulnerability assessment ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication • Any guidance that the device vendor intended for integrators/ resellers, solution providers, and/or end-users • Guidance that only IP stacks approved as part of the PTS review can be used	**2B-2.1.1** Interview solution-provider personnel to determine that they have used only the approved IP stack, and that they have implemented the application in accordance with the *Implementation Guide.*

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2B-2.1.1.b Perform a source-code review and verify that the application: • Only uses the IP stack approved as part of the PCI-approved POI device evaluation • Was developed according to the device vendor's security guidance • Is securely integrated with the POI device's IP stack and any OP services in accordance with the POI device vendor's security guidance, including the following areas for each platform component used by the POI as it relates to the application's specific processing: ○ Vulnerability assessment ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication	
	2B-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 examine all output created by the application and verify that, by following the *Implementation Guide*, the application only uses the IP stack included in the PCI-approved POI device evaluation.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-2.2 The application-development process includes 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* required at 2C-3 of this document. Confirm that the application's *Implementation Guide* is in accordance 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.a** Review the solution provider's documentation to confirm that any shared resources they integrated into the application meet the following: • That any guidance from the *Implementation Guide* is included • Shared resources are identified and documented • Instructions for how the application should be configured to ensure secure integration with shared resources (where the integration has been done by the solution provider).
	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 device vendor's security guidance.	**2B-2.2.b** Interview solution-provider personnel to determine that they have integrated any shared resources in accordance with the *Implementation Guide.*
	2B-2.2.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 examine all output created by the application and verify that, by following the *Implementation Guide*, any connections to or use of shared resources are done securely and in accordance with the device vendor's security guidance.	
2B-2.3 Applications do not bypass or render ineffective any application segregation that is enforced by the POI.	**2B-2.3** Perform a source-code review and verify that applications do not bypass or render ineffective any application segregation which is enforced by the POI, in accordance with the device vendor's security guidance.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-2.4 Applications do not bypass or render ineffective any OS hardening implemented by the POI.	**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, 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.	**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, in accordance with the device vendor's security guidance.	
2B-3 The application vendor uses secure protocols, provides guidance on their use, and has performed integration testing on the final application.		
2B-3.1 The application developer's process includes 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 provides key-management security guidance describing how keys and certificates have to be used. *Examples of guidance include what SSL certificates to load, how to load account-data keys (through the firmware of the device), when to roll keys, etc., The application does not perform account-data encryption since that is performed only in the firmware of the PCI-approved POI device.*	**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 keys and certificates have to be used.	**2B-3.1.1.a** Review the solution provider's documentation and confirm their documented processes include application developer key-management security guidance. **2B-3.1.1.b** Interview solution-provider personnel to confirm that they follow key-management security guidance in accordance with the *Implementation Guide*

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
2B-3.1.2 The application developer has performed 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.	
2B-4 Applications do not implement any encryption or key-management functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the device. ***Note:*** *The application may add, for example, SSL encryption to existing SRED encryption, but cannot bypass or replace SRED encryption.*		
2B-4.1 Applications do not bypass or render ineffective any encryption or key-management functions implemented by the approved SRED functions of the device. *At no time should clear-text keys or account data be passed through an application that has not undergone SRED evaluation.*	**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 account-data encryption, nor does it replace the device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption • Instructions on how to install the application correctly	**2B-4.1** Interview solution-provider personnel and observe implementation processes to confirm that the application is installed in accordance with the *Implementation Guide.*
	2B-4.1.b Perform a source-code review to verify that the application's encryption and key-management functions utilize an approved function of the SRED device, and are not implemented within the application itself.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2B-4.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide* and confirm that, by following the *Implementation Guide,* the application does not perform account-data encryption that replaces the SRED encryption performed by the device.	

Requirement 2C: Implement secure application-management processes.

The application addresses security vulnerabilities and provides all updates in a secure manner.		
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.	**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.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
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.a** Obtain and examine processes for deploying application security upgrades, and verify they include deployment of critical security updates within 30 days of receipt from the software vendor.
	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-1.2.b** Interview responsible solution-provider personnel to confirm that critical application security updates are deployed within 30 days of receipt from the software vendor.
2C-2 Applications are installed and updates are implemented only via trusted, signed, authenticated processes using an approved security protocol evaluated for the PCI-approved POI device.		
2C-2.1 Ensure that all application installations and updates are authenticated as follows:	**2C-2.1** To confirm that all application installations and updates are authenticated, verify the following:	
2C-2.1.1 All application installations and updates only use an approved security protocol of the POI.	**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 uses the approved security protocol of the POI 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	**2C-2.1.1.a** 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.
	2C-2.1.1.b Perform a source-code review to verify that the application only allows installations and updates using the approved security protocol of the POI.	**2C-2.1.1.b** Interview responsible personnel and observe installation and update processes to confirm that installations and updates are only done using an approved security protocol.

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	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 protocol of the POI.	
	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 protocol, and verify that the application will not allow the installation or update to occur.	
2C-2.1.2 Unauthenticated changes are not allowed (for example, all changes to code that manages "whitelists" must be authenticated).	**2C-2.1.2.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 prevents unauthenticated changes or updates • A statement that unauthenticated changes or updates to applications or application functions (like "whitelists") are not allowed	
	2C-2.1.2.b Perform a source-code review to verify that the application does not allow unauthenticated changes or updates.	
	2C-2.1.2.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 does not allow unauthenticated changes or updates.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
	2C-2.1.2.d After the application is installed and configured in accordance with the *Implementation Guide,* attempt to add an unauthenticated "whitelist" and verify that the application will not allow the update to occur.	
2C-2.1.3 The application developer includes guidance for whoever signs the application (including for whitelists), including requirements for dual control over the application-signing process.	**2C-2.1.3** 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 (including "whitelists") • 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-2.1.3** Confirm the following through interview with solution provider and by observing an application update: • Application-signing processes specified in the *Implementation Guide* are followed. • Updates to applications are signed. • Application-signing is done under dual control.
The application developer provides documentation and training.		
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** Confirm that the solution provider has a current copy of the *Implementation Guide*.
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.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
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 (for example, 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.a** Interview solution-provider personnel to confirm they have read a current copy of the *Implementation Guide* and are familiar with the contents and instructions therein.
	2C-3.1.2.b Verify the *Implementation Guide* is updated as needed to keep the documentation current with: • Any changes to the application (for example, 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 (for example, 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-3.1.3** Confirm the following via interviews with solution-provider personnel: • The solution provider receives periodic updates of the *Implementation Guide* from the software vendor. • The solution provider has distributed the Implementation Guide to any outsourced integrators/resellers they use for their P2PE solution.
2C-3.2 Develop and implement training and communication programs to ensure application installers (for example, 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.	

Domain 2 Requirements	Testing Procedures: Application Vendor Assessment	Testing Procedures: Solution Provider Assessment
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.	**2C-3.2.1** For the training materials provided by the software vendor for integrators/resellers, confirm the following via interviews with solution-provider personnel: • The solution provider has read and understands the training material. • The solution provider has distributed the training material to any outsourced integrators/resellers they use for their P2PE solution.

Domain 2 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-1.1	The application does not store PAN or SAD data after processing is completed (even if encrypted).	• A detailed description of the function of the application, including how it uses PAN or SAD for its application processing • A detailed description of how it ensures the application does not store PAN or SAD after the application's processing is complete
2A-1.2	A process is in place to securely delete any PAN or SAD stored during application processing.	Methodology or process used by the application to securely delete any PAN or SAD if stored during application processing
2A-2.1	The application only exports PAN or SAD data that has been encrypted by the firmware of the PCI-approved POI device and does not export clear-text PAN or SAD outside of the device.	A description of the application's function including the following: • That the application does not output clear-text data outside of the device • Whether the application passes encrypted account data outside of the device • If the application passes encrypted account data outside of the device, that the application only exports PAN or SAD that has been encrypted by the approved SRED functions of the PCI-approved POI device
2A-2.2	The application only uses internal communication methods (including all inter-process communication and authentication methods) included in the PCI-approved POI device evaluation.	• A list of internal communication methods included in the device vendor's security guidance • A list of which approved internal communications methods are used by the application • A description of where internal communications are used by the application to pass clear-text account data within the device (for example, from the application to other applications, to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI) • How to configure the application to use the approved internal communication methods • Guidance that use of any other methods for internal communication is not allowed

Domain 2 Requirement		Required Content for the Implementation Guide
2A-2.3	The application only uses external communication methods included in the PCI-approved POI device evaluation and has not implemented its own external communication stack.	The following instructions are included and are consistent with the POI device vendor's security guidance: • A list of the external communication methods included in the POI device vendor's security guidance • A list of which approved external communications methods are used by the application. • A description of where external communications are used by the application. • Instructions for how to configure the application to use only those approved methods. • Guidance that use of any other methods for external communications is not allowed.
2A-2.4	Ensure that any application functions (for example, "whitelists") that allow for the output of clear-text data limits that output to *only* non-PCI payment brand accounts/cards, and that additions or changes to application functions are implemented as follows: • Cryptographically authenticated by the PCI-approved POI device's firmware • Implemented only by authorized personnel • Documented as to purpose and justification • Reviewed and approved prior to implementation	Details to describe any application functions that allow for the output of clear-text card data (for example, through the use of "whitelists" of BIN ranges), and provides instructions as follows: • That any such application functions are only allowed for non-PCI payment brand accounts/cards. • How to establish application authentication using strong cryptography, with the approved SRED firmware of the POI device. • Only authorized personnel must be used for signing and adding application functions for output of clear-text data.
2B-1.1	Applications are 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 (for example, application configuration settings which are necessary for the application to function with the device).
2B-1.4	All changes to application must follow change-control procedures.	• Documentation about the impact of the change • Instructions about how to back out or de-install applications
2B-2.1	The application is developed in accordance with the POI device vendor's security guidance, including specifying that if an application uses an IP stack, it must use the IP stack approved as part of the PCI-approved POI device evaluation.	• A description of the IP stack implemented in the POI device, and • Confirmation that the IP stack used by the application is the same one included in the device vendor's security guidance.

	Domain 2 Requirement	Required Content for the Implementation Guide
2B-2.1.1	If an application uses the POI device's IP stack and any of the related OP services, the application must securely use, and integrate with, the following device platform components in accordance with the POI device vendor's security guidance, including but not limited to the following: • IP and link layer (where implemented by the POI) • IP protocols (where implemented by the POI) • Security protocols, including specific mention if specific security protocols or specific configurations of security protocols are not to be used for financial applications and/or platform management • IP services, including specific mention if specific IP services or specific configurations of IP services are not to be used for financial applications and/or platform management (where implemented by the POI) • For each platform component listed above, follow the POI device vendor's security guidance, as applicable to the application's specific business processing, with respect to the following: ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication	• A description of the IP stack implemented in the POI device and included in 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, including: ○ Vulnerability assessment ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication • Any guidance that the device vendor intended for integrators/ resellers, solution providers, and/or end-users • Guidance that use of any IP stack that was not approved as part of the PTS review cannot be used
2B-2.2	The application development process includes 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 provides key-management security guidance describing how keys and certificates have to be used.	Key-management security guidance for solution providers, describing how keys and certificates have to be used

Domain 2 Requirement		Required Content for the Implementation Guide
2B-4.1	Applications do not bypass or render ineffective any encryption or key-management functions implemented by the approved SRED functions of the device.	The description of the application's function that includes the following: • Confirmation that the application does not perform account-data encryption, nor does it replace the device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption • Instructions on how to install the application correctly
2C-2.1.1	All application installations and updates only use an approved security protocol of the POI.	• A description of how the application uses the approved security protocol of the POI 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.
2C-2.1.2	Unauthenticated changes are not allowed (for example, all changes to "whitelists" must be authenticated).	• A description of how the application prevents unauthenticated changes or updates. • A statement that unauthenticated changes or updates to applications or application functions (like "whitelists") are not allowed.
2C-2.1.3	The application developer includes guidance for whoever signs the application (including for whitelists), including requirements for dual control over the application-signing process.	• Instructions for how to sign the application (including "whitelists") • 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: Encryption Environment

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 3: Encryption Environment Secure environments where POI devices are present.	▪ No storage of CHD after transaction processes are complete. ▪ Within the segmented P2PE environment, no CHD stored, processed or transmitted through channels or methods external from an approved SCD. ▪ All device-administration and cryptographic operations are managed by solution provider. ▪ POI devices are implemented and maintained in accordance with the P2PE Instruction Manual (PIM).	**3A** Secure POI devices throughout the device lifecycle. **3B** Implement secure device-management processes. **3C** Maintain *P2PE Instruction Manual* for merchants.	▪ P2PE Solution Provider

In this scenario for hardware/hybrid, the only merchant system that stores, processes, or transmits account data is the PCI-approved POI device, which also isolates all account data from the merchant environment. All account-data processing and cryptographic operations are managed by the validated solution provider.

All POI devices used in the P2PE solution must be PCI-approved POI devices, and the customer account data, including PAN, may be inputted from the card's magnetic stripe or chip. Alternatively, the PAN may be entered into the POI by manual input using a PTS-approved capture mechanism.

Requirements in Domain 3 include physically securing POIs throughout the device lifecycle and implementing secure device-management processes. For the hardware/hybrid scenario, all requirements in Domain 3 are the responsibility of the P2PE solution provider, who must also provide detailed instructions for the merchant in the *P2PE Instruction Manual (PIM).*

Domain 3 Requirements	Testing Procedures
Requirement 3A: Secure POI devices throughout the device lifecycle.	
Secure POI devices throughout the device lifecycle.	
3A-1 Solution provider maintains inventory-control and monitoring procedures to accurately track POI devices in their possession, and provides related instructions to merchants.	
3A-1.1 Maintain inventory-control and monitoring procedures to identify and locate all POI devices, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	**3A-1.1.a** Examine documented inventory-control procedures to confirm the solution provider has defined methods to identify and locate all POI devices, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit
	3A-1.1.b For a sample of devices, examine the documented device inventory and observe device locations to verify that the inventory-control and monitoring procedures identify and locate all POI devices.
3A-1.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain inventory-control and monitoring procedures to identify and locate all devices, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	**3A-1.1.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to maintain inventory-control and monitoring procedures to identify and locate all devices, including those where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit
3A-1.2 Perform POI device inventories at least annually to detect removal or substitution of devices.	**3A-1.2.a** Examine documented procedures to verify device inventories are required to be performed at least annually to detect removal or substitution of devices.
	3A-1.2.b Examine records of device inventories and interview personnel to verify that device inventories are performed at least annually.

Domain 3 Requirements	Testing Procedures
3A-1.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to perform POI device inventories at least annually.	**3A-1.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes: • Detailed procedures for merchants to perform device inventories to detect removal or substitution of devices • Recommended frequency for performing device inventories, not to exceed annually
3A-1.3 Maintain a documented inventory of all POI devices to include at least the following: • Make, model of device • Location (site/facility, and/or identity of merchant) • Serial number • General description • Photograph of device that clearly shows device type and model (to assist with identification of different devices • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Firmware version • Hardware version • Applications (including versions)	**3A-1.3.a** Verify through observation that a documented inventory of all POI devices is maintained.
	3A-1.3.b Verify the documented inventory includes at least the following: • Make, model of device • Location (site/facility, and/or identity of merchant) • Serial number • General description • Photograph of device that clearly shows device type and model (to assist with identification of different devices • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory • Firmware version • Hardware version • Any applications (including versions)
3A-1.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain an inventory of all POI devices used for P2PE, to include at least those items described in 3A-1.3.	**3A-1.3.1.a** Examine the *P2PE Instruction Manual (PIM)* to verify it includes procedures and guidance for merchants to maintain an inventory of POI devices.

Domain 3 Requirements	Testing Procedures
	3A-1.3.1.b Verify the instructions include maintaining at least the following details: • Make, model of device • Location (including site/facility, if applicable) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Firmware version • Hardware version
3A-1.3.2 Secure the documented inventory of POI devices from unauthorized access.	**3A-1.3.2** Observe implemented controls and interview personnel to verify the documented inventory of devices is secured from unauthorized access.
3A-1.3.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to secure the documented inventory of POI devices from unauthorized access.	**3A-1.3.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes procedures and guidance for merchants to secure their documented inventory of devices from unauthorized access.
3A-1.4 Implement procedures for detecting and responding to variances in the annual inventory, including missing or substituted POI devices. Response procedures must include inclusion of any procedures defined by all applicable PCI payment brands, including timeframes for incident reporting, and providing a point of contact for merchants to report missing/substituted devices.	**3A-1.4.a** Examine documented procedures to verify that procedures are defined for responding to variances in the annual inventory, including: • Procedures to detect missing or substituted devices • Procedures for responding to missing or substituted devices, including any procedures defined by all applicable PCI payment brands, including timeframes for incident reporting • A point of contact for reporting missing/substituted devices.
	3A-1.4.b Interview personnel to verify that procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted devices, are implemented.
3A-1.4.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to detect and report variances in the annual inventory, including missing or substituted POI devices.	**3A-1.4.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes: • Procedures for merchants to detect and report variances in the annual inventory, including missing or substituted device • Point of contact for merchants to report missing or substituted devices

Domain 3 Requirements	Testing Procedures
3A-2 Solution provider physically secures POI devices in their possession when not deployed or being used, and provides related instructions to merchants.	
3A-2.1 Physically secure the storage of POI devices awaiting deployment.	**3A-2.1.a** Examine documented procedures to verify they include storing POI devices awaiting deployment in a physically secure location.
	3A-2.1.b Inspect storage locations for POI devices awaiting deployment, to verify that the location is physically secure.
3A-2.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices awaiting deployment.	**3A-2.1.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices awaiting deployment in a physically secure location.
3A-2.2 Physically secure the storage of POI devices undergoing repair or otherwise not in use.	**3A-2.2.a** Examine documented procedures to verify they include storing POI devices undergoing repair, or otherwise not in use, in a physically secure location.
	3A-2.2.b Inspect storage locations for POI devices undergoing repair or otherwise not in use, to verify that the location is physically secure.
3A-2.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices undergoing repair or otherwise not in use.	**3A-2.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices undergoing repair or otherwise not in use in a physically secure location.
3A-2.3 Physically secure the storage of POI devices awaiting transport between sites/locations.	**3A-2.3.a** Examine documented procedures to verify they include storing POI devices awaiting transport between sites/locations in a physically secure location.
	3A-2.3.b Inspect storage locations for decryption devices awaiting transport between sites/locations, to verify that the location is secure.
3A-2.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices awaiting transport between sites/locations.	**3A-2.3.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices awaiting transport between sites/locations in a physically secure location.

Domain 3 Requirements	Testing Procedures
3A-2.4 Physically secure POI devices in transit, including: • Packing devices in tamper-evident packaging prior to transit. • Implementing procedures for determining whether device packaging has been tampered with. • Use of a defined secure transport method, such as bonded carrier or secure courier.	**3A-2.4.a** Examine documented procedures for the transportation of POI devices and verify that procedures include the following: • Procedures for packing POI devices in tamper-evident packaging prior to transit • Procedures for determining whether device packaging has been tampered with • Procedures for using a defined secure transport method, such as bonded carrier or secure courier
	3A-2.4.b For a sample of device shipments, examine records of device transportation and interview personnel to verify that the following procedures are implemented: • POI devices are packed in tamper-evident packaging prior to transit • Procedures are followed for determining whether device packaging has been tampered with • Use of a defined secure transport method, such as bonded carrier or secure courier
3A-2.4.1 Provide instructions to the merchant via the *P2PE Instruction Manual* for the merchant to physically secure POI devices in transit, to include at least those items described in 3A-2.4.	**3A-2.4.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to physically secure POI devices being transported, including: • Procedures for packing the device using tamper-evident packaging prior to transit • Procedures for inspecting device packaging to determine whether it has been tampered with, including specific details on how tamper-evidence may appear on the packaging used • Defined secure transport method, such as bonded carrier or secure courier
3A-2.4.2 Implement procedures to be followed upon determining that POI device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Escalation procedures and contact details for reporting tamper-detection	**3A-2.4.2.a** Examine documented procedures to verify they include procedures to be followed upon determining that device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection

Domain 3 Requirements	Testing Procedures
	3A-2.4.2.b Interview personnel to verify that, upon determining that device packaging has been tampered with, the following procedures are implemented: • Devices are not deployed or used • Procedures are followed for returning device to authorized party for investigation • Reporting of tamper-detection to defined contact details
3A-2.4.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow upon determining that POI device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection	**3A-2.4.3** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchant to follow upon determining that device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection

3A-2.5 Ensure POI devices are transported only between trusted sites/locations as follows:
• A list of trusted sites (e.g., vendor / maintenance provider, etc.) is maintained.
• Only devices received from trusted sites/locations are accepted for use.
• Procedures are defined in the event that devices are received from untrusted or unknown locations, including:
  ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent
  ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted
• Devices are sent only to trusted sites/locations.
	3A-2.5.a Examine documented procedures to verify they include:
	• A list of trusted sites (e.g., vendor / maintenance provider, etc.) between which devices may be transported
	• Procedures to ensure that only devices received from trusted sites/locations are accepted for use
	• Procedures to be followed in the event that a device is received from an untrusted or unknown location, including:
	  ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent
	  ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted.
	• Procedures to ensure that devices are only sent to trusted sites/locations

Domain 3 Requirements	Testing Procedures

	3A-2.5.b For a sample of device shipments, examine records of device transportation and interview personnel to verify:
	• Only devices received from trusted sites/ locations are accepted for use.
	• Procedures are followed in the event that a device is received from an untrusted or unknown location, including:
	  ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent
	  ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted
	• Devices are only sent to trusted sites/locations

3A-2.5.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to only transport POI devices between trusted sites/locations, as described in 3A-2.5.	**3A-2.5.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for transporting devices including:
	• A list of trusted sites (e.g., vendor / maintenance provider, etc.) from which devices may be accepted for use
	• Procedures to ensure that only devices received from trusted sites/locations are accepted for use
	• Procedures to be followed in the event that a device is received from an untrusted or unknown source location, including:
	  ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent
	  ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted
	• A list of trusted sites (e.g., vendor / maintenance provider, etc.) to which devices may be sent

3A-3 Solution provider has procedures to prevent and detect the unauthorized alteration or replacement of POI devices in their possession prior to and during deployment, and provides related instructions to merchants.	
3A-3.1 Implement procedures to prevent and detect unauthorized modification, substitution, or tampering of POI devices prior to use. Procedures must include the following:	

Domain 3 Requirements	Testing Procedures
3A-3.1.1 Validate that serial numbers of received devices match sender records, and maintain records of serial-number verification. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document.*	**3A-3.1.1.a** Examine documented procedures to verify they include: • Procedures for comparing device serial numbers to the serial numbers documented by the sender • Procedures for maintaining records of serial-number verifications
	3A-3.1.1.b For a sample of received POIs, observe records of serial-number validations and interview personnel to verify: • Device serial numbers for the received device were verified to match that documented by the sender. • Records of serial-number verifications are maintained.
3A-3.1.2 Documentation used for validating device serial numbers must be received via a separate communication channel and must not have arrived with the device shipment.	**3A-3.1.2.a** Examine documented procedures to verify that documentation used for validating device serial numbers must be received via a separate communication channel and must not arrive with the device shipment
	3A-3.1.2.b For a sample of received POIs, review delivery records and interview personnel to verify that documentation used to validate the device serial number was received via a separate communication channel than the device and was not received in the same shipment as the device.
3A-3.1.3 Perform pre-installation inspection procedures, including physical and functional tests and visual inspection, to confirm devices have not been tampered with or compromised.	**3A-3.1.3.a** Examine documented procedures to verify that pre-installation inspection procedures are defined, including physical and functional tests and visual inspection, to confirm devices have not been tampered with or compromised.
	3A-3.1.3.b Examine records of inspections, interview personnel performing device inspections and observe inspection process to confirm that POIs are subject to physical and functional tests as well as visual inspection prior to installation to confirm devices have not been tampered with or compromised.
3A-3.1.4 Maintain devices in original, tamper-evident packaging or store devices in a physically secured location, until ready for use.	**3A-3.1.4.a** Examine documented procedures to verify they require devices be maintained in original, tamper-evident packaging or stored in a physically secured location, until ready for use.
	3A-3.1.4.b Observe devices to verify they are maintained in original, tamper-evident packaging or stored in a physically secured location, until ready for use.

Domain 3 Requirements	Testing Procedures
3A-3.1.5 Record device serial number in inventory-control system as soon as possible upon receipt and prior to installation	**3A-3.1.5.a** Examine documented procedures to verify they require devices be entered into an inventory-control system as soon as possible upon receipt and prior to installation.
	3A-3.1.5.b Review documented device inventories and interview responsible personnel to verity devices are entered into an inventory-control system as soon as possible after receipt of the device, and before installation.
3A-3.1.6 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures, including those items described in 3A-3.1.1 through 3A-3.1.5, to prevent and detect unauthorized alteration or replacement of POI devices prior to installation and use.	**3A-3.1.6** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchants to implement procedures for preventing and detecting unauthorized modification, substitution, or tampering of POI devices prior to installation and use, including: • Procedures for matching device serial numbers to the serial numbers documented by the sender • Procedures for maintaining records of serial-number verifications • Defined method for transporting documents used for validating device serial numbers, via a separate communication channel and not with the device shipment • Instructions for performing pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify devices have not been tampered with or compromised • Instructions for maintaining devices in original, tamper-evident packaging or in physically secure storage until ready for use • Instructions for recording device serial numbers in merchant inventory-control system as soon as possible
3A-3.2 Implement procedures to control and document all physical access to devices prior to deployment. Procedures to include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out. Retain access log for at least one year.	**3A-3.2.a** Examine documented access procedures and verify they require controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out • Retaining access logs for at least one year

Domain 3 Requirements	Testing Procedures
	3A-3.2.b Observe physical access controls to verify they include controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in/out
	3A-3.2.c Examine access logs/records to verify it is retained for at least one year and contains, at a minimum, the following details: • Personnel name • Company • Reason for access • Time in and out
3A-3.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to control and document all physical access to devices prior to deployment. Procedures to include those items described in 3A-3.2.	**3A-3.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchants to implement procedures for controlling and documenting all physical access to devices prior to deployment, including: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out
3A-3.3 Implement a documented audit trail to demonstrate that devices are controlled, and are not left unprotected, at all times from receipt through to installation.	**3A-3.3.a** Examine documented procedures to verify a documented audit trail must be maintained to demonstrate that devices are controlled, and not left unprotected, at all times from receipt through to installation.
	3A-3.3.b Examine audit trail records to verify a documented audit trail is maintained and demonstrates that devices are controlled, and not left unprotected, at all times from receipt through to installation.
3A-3.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement an audit trail to demonstrate that a device is controlled, and not left unprotected, at all times from receipt through to installation	**3A-3.3.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to maintain an audit trail to demonstrate that devices are controlled, and not left unprotected, at all times from receipt through to installation.

Domain 3 Requirements	Testing Procedures
3A-4 Solution provider provides instructions to merchants to physically secure devices to prevent unauthorized access, modification, or substitution while devices are deployed for use. This includes both attended and unattended devices (for example, kiosks, "pay-at-the-pump," etc.).	
3A-4.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to select appropriate locations for deployed devices, for example: • Control public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locate devices so they can be observed and/or monitored by authorized personnel (for example, during daily device checks performed by store/security staff). • Locate devices in an environment that deters compromise attempts (for example, through use of appropriate lighting, access paths, visible security measures, etc.)	**3A-4.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to select appropriate locations for deployed devices, for example: • Controlling public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction • Locating devices so they can be observed and/or monitored by authorized personnel • Locating devices in an environment that deters compromise attempts
3A-4.2 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured.	**3A-4.2** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including specific examples of how devices can be physically secured.
3A-4.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured (such as wireless or handheld devices). *For example, secure devices in a locked room when not in use, assign responsibility to specific individuals when in use, observe devices at all times, sign devices in/out, etc.*	**3A-4.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured, such as wireless or handheld devices.
3A-5 Solution provider prevents unauthorized physical access to devices undergoing repair or maintenance while in their possession, and provides related instructions to merchants.	
3A-5.1 Implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access. Procedures must include the following:	**3A-5.1.a** Examine documented procedures to verify they include identification and authorization of third-party personnel prior to granting access. **3A-5.1.b** Verify documented procedures include 3A-5.1.1 through 3A-5.1.5 below.

Domain 3 Requirements	Testing Procedures
3A-5.1.1 Verify the identity and authorization of third-party personnel prior to granting access to devices.	**3A-5.1.1** Interview responsible personnel and observe processes to confirm that the identity and authorization of third-party personnel is verified prior to granting access to devices.
3A-5.1.2 Unexpected personnel must be denied access until fully validated and authorized.	**3A-5.1.2** Interview responsible personnel and observe processes to verify that unexpected personnel are denied access until fully validated and authorized.
3A-5.1.3 Once authorized, third-party personnel must be escorted and monitored at all times.	**3A-5.1.3** Interview responsible personnel and observe processes to verify that, once authorized, third-party personnel are escorted and monitored at all times.
3A-5.1.4 A log of all third-party personnel access is maintained.	**3A-5.1.4** Examine access logs/records to verify that a log of all third-party personnel access is maintained in accordance with logging requirements defined in 3A-3.2.
3A-5.1.5 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access. Procedures to include those items described in 3A-5.1.1 through 3A-5.1.4.	**3A-5.1.5** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access, including: • Procedures for verifying the identity and authorization of third-party personnel prior to granting access to devices • Instructions that unexpected personnel must be denied access unless fully validated and authorized • Escorting and monitoring authorized personnel at all times • Maintaining a log of all third-party personnel access

Requirement 3B: Implement secure device-management processes.

3B-1 Solution provider securely maintains devices being returned, replaced, or disposed of, and provides related instructions to merchants.	
3B-1.1 Implement procedures to ensure that devices to be removed from service, retired, or returned for repair, are not intercepted and used in an unauthorized manner, as follows.	**3B-1.1.a** Examine documented procedures to verify that procedures are defined for any devices to be removed from service, retired, or returned for repair
	3B-1.1.b Verify documented procedures include 3B-1.1.1 through 3B-1.1.5

Domain 3 Requirements	Testing Procedures
3B-1.1.1 Affected entities are notified before devices are returned.	**3B-1.1.1** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
3B-1.1.2 Devices are transported via trusted carrier service—for example, bonded carrier.	**3B-1.1.2** Interview responsible personnel and examine device-return records to verify that devices are transported via trusted carrier service—for example, bonded carrier.
3B-1.1.3 Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	**3B-1.1.3** Interview responsible personnel and observe device-return processes and packaging to verify that devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.
3B-1.1.4 Devices are tracked during the return process.	**3B-1.1.4** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
3B-1.1.5 Once received, devices remain in their packaging (as defined in 3B-1.1.3) until ready for repair or destruction.	**3B-1.1.5** Interview responsible personnel and examine device-return processes to verify that, once received, devices remain in their packaging (defined in 3B-1.1.3) until ready for repair or destruction.
3B-1.1.6 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for securing devices being removed from service, retired, or returned for repair.	**3B-1.1.6** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for the merchant to secure devices being returned or replaced, including: • Procedures and contact details for notifying affected entities—including the entity to which the device is being returned—before devices are returned • Procedures for transporting devices via a trusted carrier service • Procedures for packing and sending devices in serialized, counterfeit-resistant, and tamper-evident packaging • Procedures to ensure the solution provider can track devices during the return process
3B-1.2 Implement procedures for secure disposal of devices, to include the following:	**3B-1.2** Examine documented procedures to verify procedures are defined for secure disposal of devices and include 3B-1.2.1 through 3B-1.2.2.
3B-1.2.1 Return devices to authorized parties for disposal.	**3B-1.2.1** Interview responsible personnel and examine device-return processes to verify devices are returned only to authorized parties for disposal.

Domain 3 Requirements	Testing Procedures
3B-1.2.2 Keys and data storage (including account data) must be rendered irrecoverable (for example, zeroized) prior to device disposal. If data cannot be rendered irrecoverable, the device must be physically destroyed to prevent the disclosure of any sensitive data or keys.	**3B-1.2.2** Interview personnel and observe processes for removing devices from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized) prior to disposal, or that devices are physically destroyed to prevent the disclosure of any sensitive data or keys.
3B-1.2.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for the secure disposal of devices.	**3B-1.2.3** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to implement procedures for the secure disposal of devices, including: • Returning devices only to authorized parties for destruction (including a list of authorized parties) • Procedures to render sensitive data irrecoverable, prior to device being shipped for disposal.
3B-2 Solution provider configures devices to fail closed if encryption mechanism fails, until either the P2PE encryption is restored or merchant opts out of using solution.	
3B-2.1 Upon failure of the encryption mechanism, the device must immediately fail closed and/or be immediately removed, shut down, or taken offline until the P2PE encryption is restored. ***Note:*** *Domain 5 requires that solution providers actively monitor traffic that is received into the decryption environment to confirm that the POI equipment in the merchant's encryption environment is not outputting clear-text CHD through some error or misconfiguration. Refer to 5D-2.*	**3B-2.1.a** Review documented procedures and interview responsible personnel to verify that upon failure of the encryption mechanism, POI devices are configured to immediately fail closed, and/or be immediately removed, shut down, or taken offline.
	3B-2.1.b Observe POI device configurations to verify that POI devices are configured to, upon failure of the encryption mechanism, immediately fail closed, and/or be immediately shut down or taken offline.
	3B-2.1.c Observe devices during a simulated encryption failure to verify that devices immediately fail closed and/or are immediately removed/shut down/taken offline upon failure of the encryption mechanism.
3B-2.1.1 The device cannot 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 formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using alternative controls and/or processing method.	**3B-2.1.1.a** Examine documented procedures 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 formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using an alternative controls and/or processing method.

Domain 3 Requirements	Testing Procedures
	3B-2.1.1.b Verify the documented procedures include verifying that encryption functionality is restored before devices are re-enabled.

	3B-2.1.1.c Interview responsible personnel and observe implemented processes to verify that:
	• POI devices are not 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 formally opted out from using the P2PE solution, according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using an alternative processing method.
	• Encryption functionality is verified as being restored before devices are re-enabled.

	3B-2.1.1.d Observe device configurations to verify devices are configured to remain closed until re-enabled by authorized personnel.
3B-2.1.2 The solution provider must maintain a record of all encryption failures, 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 encryption failure • Date/time and duration of device downtime • Date/time that encryption functionality was verified as being restored • Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled	**3B-2.1.2.a** Examine documented procedures to verify they require a record of all encryption failures to be maintained, 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 encryption failure • Date/time and duration of device downtime • Date/time that encryption functionality was verified as being restored • Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled

Domain 3 Requirements	Testing Procedures
	3B-2.1.2.b Interview responsible personnel and observe implemented processes to verify that a record of all encryption failures is maintained, 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 encryption failure • Date/time and duration of device downtime • Date/time that encryption functionality was verified as being restored • Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled
3B-2.1.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow in the event of a device encryption failure.	**3B-2.1.3** Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to follow in the event of a device encryption failure. Verify the detailed instructions include ensuring that devices are not re-enabled for use until merchant has confirmed with solution provider that either: • The issue has been resolved and P2PE-encryption functionality is restored and re-enabled, or • The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using alternative controls and/or processing method.
3B-2.2 The solution provider must document and implement an opt-out process for merchants to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection. The process must include the following:	**3B-2.2.a** Examine documented procedures to verify the solution provider has a documented opt-out process for merchants to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.
	3B-2.2.b Verify documented opt-out procedures include 3B-2.2.1 through 3B-2.2.4
3B-2.2.1 Defined method of communication for merchants to advise the solution provider that they wish to opt out of the P2PE solution.	**3B-2.2.1** Interview responsible personnel and observe processes to verify the defined method of communication is in place for merchants to advise the solution provider that they wish to opt out of the P2PE solution.

Domain 3 Requirements	Testing Procedures
3B-2.2.2 Upon receipt of a merchant request to opt out of the P2PE solution, the solution provider must formally communicate to the merchant the procedures to be followed, and advise the merchant of the following: • The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. • The merchant is responsible for implementing alternative controls to protect account data in lieu of the P2PE solution (such as the applicable PCI DSS requirements for secure data transmission, network security, etc.). • The merchant is no longer eligible for the PCI DSS scope reduction which was afforded by the P2PE solution. • The merchant is obligated to advise their acquirer that they are no longer using the P2PE solution. • Processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation, and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. • If the merchant wishes to opt out of the P2PE solution, the merchant must provide formal acknowledgment and acceptance of the above and formally request that transactions be accepted without P2PE encryption. • A defined method of communication for the merchant to provide their acknowledgement and acceptance of the above.	**3B-2.2.2** Interview responsible personnel and observe implemented processes and communications to verify that upon receipt of a merchant request to opt out of the P2PE solution, the solution provider formally communicates to the merchant the procedures to be followed, and advises the merchant of the following: • The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. • The merchant is responsible for implementing alternative controls to protect account data in lieu of the P2PE solution (such as the applicable PCI DSS requirements for secure data transmission, network security, etc.) • The merchant is no longer eligible for the PCI DSS scope reduction which was afforded by the P2PE solution. • The merchant is obligated to advise their acquirer that they are no longer using the P2PE solution. • Processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. • If the merchant wishes to opt out of the P2PE solution, the merchant must provide formal acknowledgment and acceptance of the above and formally request that transactions be accepted without P2PE encryption. • A defined method of communication for the merchant to provide their acknowledgement and acceptance of the above.
3B-2.2.3 The process for merchants to acknowledge their acceptance of the opt-out conditions must include a mechanism for the solution provider to verify the authenticity of the acknowledgment, including: • Verification that the acknowledgement originated from the merchant using the affected devices • Verification that the acknowledgement was approved by merchant personnel authorized to make such an acknowledgement	**3B-2.2.3** Observe implemented processes and interview responsible personnel to confirm that the authenticity of the acknowledgment is verified, including: • Verification that the acknowledgement originated from the merchant using the affected devices • Verification that the acknowledgement was approved by merchant personnel authorized to make such an acknowledgement

Domain 3 Requirements	Testing Procedures

3B-2.2.4 The solution provider must maintain a record of all opt-out requests received, including the following:
• Identification of merchant submitting request
• Date initial request received
• Result of request (that is, the merchant chose to either accept the conditions and opt out of the solution, or chose to continue with the solution using P2PE devices)
• If merchant chose to accept the conditions and opt out of the solution:
  ○ Date formal acknowledgement received
  ○ Identification of device(s) in use by the merchant that are no longer covered by the P2PE solution
	3B-2.2.4 Observe implemented processes and interview responsible personnel to verify a record of all received opt-out requests is maintained and includes:
	• Identification of merchant submitting request
	• Date initial request received
	• Result of request
	• If merchant chose to accept the conditions and opt out of the solution:
	  ○ Date formal acknowledgement received
	  ○ Identification of device(s) in use by the merchant that are no longer covered by the P2PE solution

Domain 3 Requirements	Testing Procedures

3B-2.3 Provide instructions via the *P2PE Instruction Manual*, including details of the opt-out process and instructions for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.	**3B-2.3** Examine the *P2PE Instruction Manual (PIM)* to verify it clearly describes the opt-out process and provides detailed instructions, including:
	• Procedures for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.
	• The method of communication for merchants to advise the solution provider that they wish to opt out of the P2PE solution.
	• That if they choose to opt out, the merchant must formally acknowledge that they accept responsibility for the following:
	  ○ The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection.
	  ○ Responsibility for implementing alternative controls to protect account data in lieu of the P2PE solution.
	  ○ That the merchant is no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution.
	  ○ Advising their acquirer that they are no longer using the P2PE solution.
	  ○ That processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.
	  ○ Formal request that transactions be accepted without P2PE encryption.
	• The method of communication that will be used for the merchant to provide their formal acknowledgement and acceptance of the above.

Domain 3 Requirements	Testing Procedures
Secure logical access to POI devices.	
3B-3 Solution provider restricts access to devices to authorized personnel.	
3B-3.1 Solution provider ensures merchant has no administrative access to the device and cannot change anything on the device that could impact the security settings of the device. Merchant access, if needed, must meet the following: • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.	**3B-3.1.a** Examine documented device configuration procedures and account privilege assignments to verify that merchant accounts are defined to meet the following access requirements: • No administrative access to the device is allowed. • Cannot change anything on the device that could impact the security settings of the device. • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.
	3B-3.1.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 access meets the following: • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.

Domain 3 Requirements	Testing Procedures
	3B-3.1.c Observe a sample of device configurations and interview responsible personnel to verify that the defined merchant-access requirements are configured for all devices used in the solution.
3B-3.2 All solution-provider personnel with access to POI devices are documented in a formal list and authorized by management. The list of authorized personnel is reviewed at least annually.	**3B-3.2.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.
	3B-3.2.b For a sample of all POI devices used in the solution, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to devices.
3B-3.3 Access and permissions on devices are granted based on least privilege and need to know.	**3B-3.3.a** Examine documented access-control policies and procedures to verify that access and permissions must be assigned according to least privilege and need to know.
	3B-3.3.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 access and permission granted are according to least privilege and need to know.
3B-4 Solution provider provides features for secure remote access to devices deployed at merchant locations.	
3B-4.1 Solution provider's authorized personnel use two-factor or cryptographic authentication for all remote access to merchant POIs over a public network (Internet). ***Note:*** *If cryptographic authentication is used, the update or file must be cryptographically signed under dual control.*	**3B-4.1.a** Examine documented procedures to verify that either two-factor or cryptographic authentication must be used for all remote access to POI devices.
	3B-4.1.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.
	3B-4.1.c Interview personnel and observe authorized remote connection to verify that either two-factor or cryptographic authentication is used for all remote access to POI devices.
3B-4.2 POIs must be configured to ensure that remote access is only permitted from the solution provider's authorized systems and only from the solution provider's secure decryption environment/network.	**3B-4.2.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, and only from the solution provider's secure decryption environment/network.

Domain 3 Requirements	Testing Procedures
	3B-4.2.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, and only from the solution provider's secure decryption environment/network.
3B-4.3 Merchants do not have remote access to the merchant POIs.	**3B-4.3.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 POIs.
	3B-4.3.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 POIs.
3B-4.4 Solution provider implements secure identification and authentication procedures for access to devices deployed at merchant locations, including: ***Note:*** *This applies to non-console and console access.*	**3B-4.4.a** Examine documented identification and authentication procedures to verify secure identification and authentication procedures are defined for remote access to devices deployed at merchant locations.
	3B-4.4.b Verify documented procedures are defined for 3B-4.4.1 through 3B-4.4.3
3B-4.4.1 Authentication credentials for solution-provider personnel that are unique for each merchant site	**3B-4.4.1** Examine device configurations and authentication mechanisms to verify that solution-provider personnel have unique authentication credentials for each merchant site.
3B-4.4.2 Tracing all logical access to devices by solution-provider personnel to an individual user.	**3B-4.4.2.a** Examine device configurations and authentication mechanisms to verify that all logical access to devices can be traced to an individual user.
	3B-4.4.2.b Observe authorized logical accesses and examine access records/logs to verify that all logical access is traced to an individual user.
3B-4.4.3 Maintaining audit logs of all logical access to devices, and retaining access logs for at least one year.	**3B-4.4.3.a** Observe authorized logical accesses and examine access records/logs to verify that an audit log of all logical access to devices is maintained.
	3B-4.4.3.b Examine access records/logs to verify that access logs are retained for at least one year.
3B-5 The solution provider protects POI devices from known vulnerabilities and implements procedures for secure updates to devices.	

Domain 3 Requirements	Testing Procedures
3B-5.1 Implement secure update processes for all firmware and software updates, including: • Integrity check of update • Authentication of origin of the update	**3B-5.1.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
	3B-5.1.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
3B-5.2 Maintain an up-to-date inventory of POI system builds and conduct vulnerability assessments against all builds at least annually and upon any changes to the build.	**3B-5.2.a** Examine documented procedures to verify they include: • Procedures for maintaining an up-to-date inventory of POI system builds • Procedures for conducting vulnerability assessments against all builds at least annually and upon any changes to the build
	3B-5.2.b Review documented inventory of devices (as required in 3A-1.3), and examine the inventory of system builds to verify: • The inventory includes all POI system builds. • The inventory of POI system builds is up-to-date.
	3B-5.2.c Observe results of vulnerability assessments and interview responsible personnel to verify vulnerability assessments are performed against all POI builds: • At least annually and • Upon any changes to the build
3B-5.3 Develop and deploy patches and other device updates in a timely manner.	**3B-5.3.a** Examine documented procedures to verify they include defined procedures for patches and other device updates to be developed and deployed in a timely manner.
	3B-5.3.b Examine patch-deployment records and device logs, and interview responsible personnel to verify that patches and other device updates are developed and deployed in a timely manner.
3B-5.4 Deliver updates in a secure manner with a known chain-of-trust.	**3B-5.4.a** Examine documented procedures for device updates to verify they include delivering updates in a secure manner with a known chain-of-trust.

Domain 3 Requirements	Testing Procedures
	3B-5.4.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.
3B-5.5 Maintain the integrity of patch and update code during delivery and deployment.	**3B-5.5.a** Examine documented procedures for device updates to verify they define controls to maintain the integrity of all patch and update code during delivery and deployment.
	3B-5.5.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.
	3B-5.5.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.
3B-6 Secure account data when troubleshooting	
3B-6.1 Securely delete any PAN or SAD used for debugging or troubleshooting purposes. 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.	**3B-6.1.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 environment • 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 account data while stored • Secure deletion of such data immediately after use
	3B-6.1.b For a sample of recent troubleshooting requests, observe data collection and storage locations, and interview responsible personnel to verify the procedures identified at 3B-6.1.a were followed.

Domain 3 Requirements	Testing Procedures
3B-6.2 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow secure troubleshooting procedures.	**3B-6.2** Examine the *P2PE Instruction Manual (PIM)* to verify it includes information for the merchant regarding the solution provider's troubleshooting processes, including that the solution provider ensures the following: • PAN and/or SAD is never output to the merchant environment • Collection of PAN and/or SAD only when needed to solve a specific problem. • Storage of such data only in specific, known locations with limited access. • Collection of only a limited amount of data needed to solve a specific problem. • Encryption of account data while stored • Secure deletion of such data immediately after use
The P2PE solution provides logging of critical processes.	
3B-7 The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).	
3B-7.1 Ensure that any changes to the critical functions of the POI are logged—either on the device or within the remote-management systems of the P2PE solution provider. Critical functions include application and firmware updates as well as changes to security-sensitive configuration options, such as whitelists or debug modes.	**3B-7.1.a** Examine device and/or system configurations to verify that any changes to the critical functions of the POI 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)
	3B-7.1.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)

Domain 3 Requirements	Testing Procedures
Monitor and inspect POI devices.	
3B-8 Solution provider implements tamper-detection mechanisms for devices in their possession, and provides related instructions to merchants.	
3B-8.1 Perform periodic physical inspections of devices in solution provider's possession to detect tampering or modification of devices. ***Note:*** *Frequency of inspection should be appropriate for device location and usage. For example, it may be suitable to inspect POIs in secure storage at least quarterly.*	**3B-8.1.a** Examine documented procedures to verify they define: • Procedures for performing periodic inspections of devices to detect signs of tampering or modification, for all POI devices in the solution provider's possession • The frequency of inspections
	3B-8.1.b Observe inspection processes to verify that inspections detect tampering or modification of POI devices.
	3B-8.1.c Examine inspection records and interview personnel to verify that inspections are periodically performed according to the defined frequency for all POI devices in the solution provider's possession.

Domain 3 Requirements	Testing Procedures

3B-8.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to perform periodic physical inspections of devices to detect tampering or modification of devices. Detailed procedures for performing periodic physical inspections to include:
• Description of tamper-detection mechanisms
• Guidance for physical inspections, including photographs or drawings of the device illustrating what the merchant is to inspect, for example:
  ○ Missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering.
  ○ Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices
• Recommendations for frequency of inspections
Note: *Frequency of inspection should be appropriate for device location and usage. For example, it may be suitable for merchants to inspect POIs in secure storage at least quarterly, and to inspect POIs in use at least weekly. If POIs cannot easily be inspected—for example, due to remote or inaccessible locations—alternative controls should be implemented to mitigate the risk of less-frequent inspections.*
	3B-8.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to perform periodic physical inspections of devices to detect tampering or modification. Verify instructions include:
	• Description of tamper-detection mechanisms
	• Guidance for physical inspections, including photographs or drawings of the device illustrating what the merchant is to inspect, for example:
	  ○ Missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering.
	  ○ Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices
	• Recommendations for frequency of inspections

3B-8.2 Implement tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations—for example, use cameras or other physical mechanisms to alert personnel to physical breach.	**3B-8.2.a** Examine documented procedures to verify tamper-detection mechanisms and/or processes are defined for devices deployed in remote or unattended locations.
	3B-8.2.b Observe tamper-detection mechanisms and/or processes in use to verify detection mechanisms and/or processes are implemented for devices deployed in remote or unattended locations.
3B-8.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations—for example, the use of cameras or other physical mechanisms to alert personnel to physical breach.	**3B-8.2.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for implementing tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations.

Domain 3 Requirements	Testing Procedures
3B-8.3 Implement procedures for responding to tampered devices.	**3B-8.3.a** Examine documented procedures to verify procedures are defined for responding to tampered devices.
	3B-8.3.b Observe response processes and interview response personnel to verify procedures for responding to tampered devices are implemented.
3B-8.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for responding to tampered devices.	**3B-8.3.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes response procedures and contact details for merchants to report and respond to tampered devices.
3B-9 Solution provider implements mechanisms to monitor and respond to suspicious activity on POI devices deployed at merchant locations.	
3B-9.1 Implement mechanisms to provide immediate notification of suspicious activity, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control	**3B-9.1.a** Examine documented procedures to verify mechanisms are defined to provide immediate notification of potential security breaches, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control
	3B-9.1.b Observe notification mechanisms and interview response personnel to verify the mechanisms provide immediate notification of suspicious activity, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control
3B-9.1.1 Provide instructions and contact details via the *P2PE Instruction Manual* for the merchant to notify the solution provider of suspicious activity.	**3B-9.1.1** Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions and contact details for the merchant to notify the solution provider of suspicious activity.

Domain 3 Requirements	Testing Procedures
3B-9.2 Prepare incident-response procedures to respond to detection of potential security breaches, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control	**3B-9.2.a** Examine documented incident-response procedures and verify that procedures are defined for responding to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control
	3B-9.2.b Observe incident-response processes and interview response personnel to verify procedures are implemented for responding to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control

Requirement 3C: Maintain P2PE Instruction Manual for merchants.

3C-1 Solution provider develops, maintains, and disseminates a *P2PE Instruction Manual (PIM)* to merchants	
3C-1.1 Develop and maintain *P2PE Instruction Manual (PIM)* and distribute PIM to merchants. Ensure PIM is available to merchants upon request. PIM must address the following:	**3C-1.1.a** Examine documented procedures to verify mechanisms are defined to distribute the PIM to all merchants using the P2PE solution, and to provide PIM to merchants upon request.
	3C-1.1.b Interview responsible personnel and observe processes to verify PIM is distributed to all merchants using the P2PE solution and PIM is provided to merchants upon request.
3C-1.1.1 All requirements in this document wherever the *P2PE Instruction Manual (PIM)* is referenced.	**3C-1.1.1** Examine the *P2PE Instruction Manual (PIM)* to verify it covers all related instructions, guidance and requirements in this document (summarized in Domain 3 PIM Annex).
3C-1.1.2 Specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices.	**3C-1.1.2** Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices.
3C-1.1.3 Specific details of all PCI-approved POI components used in the P2PE solution.	**3C-1.1.3** Examine the *P2PE Instruction Manual (PIM)* to verify it includes details of all PCI-approved POI components used in the P2PE solution.

Domain 3 Requirements	Testing Procedures
3C-1.1.4 If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.	**3C-1.1.4** If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), verify the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.
3C-1.1.5 Specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism (for example, if a PCI-approved SCR was connected to a non PCI-approved keypad), the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device. ***Note**: P2PE Requirement 1A-1.1 allows only PCI-approved POI devices to be used for accepting and processing P2PE transactions.*	**3C-1.1.5** Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.
3C-1.1.6 Provides specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: • Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device • Attempting to alter security configurations or authentication controls • Physically opening the device • Attempting to install applications onto the device	**3C-1.1.6** Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: • Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device • Attempting to alter security configurations or authentication controls • Physically opening the device • Attempting to install applications onto the device

3C-1.2 Review *P2PE Instruction Manual (PIM)* at least annually and upon changes to the solution or the PCI P2PE requirements. Update PIM as needed to keep the documentation current with:
• Any changes to the P2PE solution, 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 PCI P2PE requirements
	• PIM must be updated as needed to keep the document current with:
	  ○ Any changes to the P2PE solution, and
	  ○ Any changes to the PCI P2PE requirements.

Domain 3 Requirements	Testing Procedures

	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, and
	  ○ Any changes to the PCI P2PE requirements.

3C-1.2.1 Communicate PIM updates to affected merchants, and provide merchants with 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 3 Annex: Summary of Contents for the P2PE Instruction Manual (PIM)

This Annex contains a summary of required content for the *P2PE Instruction Manual (PIM)*, as required in Domain 3 (Hardware/Hybrid). This Annex contains only those Domain 3 requirements that have related *P2PE Instruction Manual (PIM)* topics and explains the content for the *P2PE Instruction Manual (PIM)*.

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3A-1.1.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain inventory-control and monitoring procedures, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	Detailed procedures for merchants to maintain a device-tracking system to identify and locate all devices: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit
3A-1.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to perform POI device inventories at least annually.	• Detailed procedures for merchants to perform device inventories to detect removal or substitution of devices • Recommended frequency that device inventories are to be performed, not to exceed annually
3A-1.3.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain an inventory of all PCI-approved POI devices, to include at least those items described in 3A-1.3.	Instructions and guidance for merchants to maintain an inventory of POI devices including maintaining at least the following details: • Make, model of device • Location (site/facility) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inspection • Firmware version • Hardware version
3A-1.3.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to secure the documented inventory of devices from unauthorized access.	Procedures and guidance for merchants to secure their device inventory from unauthorized access.

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3A-1.4.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to detect and report variances in the annual inventory, including missing or substituted POI devices.	• Procedures for merchants to detect and report variances in the annual inventory, including missing or substituted device • Point of contact for merchants to report missing or substituted devices
3A-2.1.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of devices awaiting deployment.	Instructions for storing POI devices awaiting deployment in a physically secure location
3A-2.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of devices undergoing repair or otherwise not in use.	Instructions for storing POI devices undergoing repair or otherwise not in use in a physically secure location
3A-2.3.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of devices awaiting transport between sites/locations.	Instructions for storing POI devices awaiting transport between sites/locations in a physically secure location
3A-2.4.1	Provide instructions to the merchant via the *P2PE Instruction Manual* for the merchant to physically secure devices in transit, to include at least those items described in 3A-2.4.	Detailed procedures for transporting devices, including: • Procedures for packing the device using tamper-evident packaging prior to transit • Procedures for inspecting device packaging to determine if it has been tampered with, including specific details on how tamper-evidence may appear on the packaging used • Defined secure transport method, such as bonded carrier or secure courier
3A-2.4.3	Provide instructions to the merchant via the *P2PE Instruction Manual* to be followed upon determination that device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection	Details instructions to be followed upon determination that device packaging has been tampered with, including: • Devices must not be deployed or used • Procedures for returning device to authorized party for investigation • Contact details for reporting tamper-detection

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*

3A-2.5.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to only transport devices between trusted/predefined sites/locations, as described in 3A-2.5.	Detailed instructions for transporting devices including:
		• A list of trusted sites (e.g., vendor / maintenance provider, etc.) from which devices may be accepted for use.
		• Procedures to ensure that only devices received from trusted sites/locations are accepted for use
		• Procedures to be followed in the event that a device is received from an untrusted or unknown source location, including:
		  ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent
		  ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted
		• A list of trusted sites (e.g., vendor / maintenance provider, etc.) to which devices may be sent

3A-3.1.6	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures, including those items described in 3A-3.1.1 through 3A-3.1.5, to prevent and detect unauthorized alteration or replacement of the device prior to use.	Detailed instructions for merchants to implement procedures for preventing and detecting unauthorized modification, substitution, or tampering of POI devices prior to use, including: • Procedures for matching device serial numbers to the serial numbers documented by the sender • Procedures for maintaining records of serial-number verifications • Defined method for transporting documents used for validating device serial numbers, via a separate communication channel and not with the device shipment • Instructions for performing pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify devices have not been tampered with or compromised • Instructions for maintaining devices in original, tamper-evident packaging or in physically secure storage until ready for use • Instructions for recording device serial numbers in merchant inventory-control system as soon as possible

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3A-3.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to control and document all physical access to devices prior to deployment. Procedures to include those items described in 3A-3.2.	Detailed instructions for merchants to implement procedures for controlling and documenting all physical access to devices prior to deployment, including: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out
3A-3.3.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement an audit trail to demonstrate that a device is controlled, and not left unprotected, at all times from receipt through to installation	Detailed instructions for the merchant to maintain an audit trail to demonstrate that devices are controlled, and not left unprotected, at all times from receipt through to installation.
3A-4.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to select appropriate locations for deployed devices, for example: • Control public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locate devices so they can be observed/monitored by authorized personnel (for example, during daily store checks of the devices performed by store/security staff). • Locate devices in an environment that deters compromise attempts (for example, through lighting, access paths, visible security measures, etc.)	Detailed instructions for the merchant to select appropriate locations for deployed devices, for example: • Controlling public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locating devices so they can be observed/monitored by authorized personnel (for example, during daily store checks of the devices performed by store/security staff). • Locating devices in an environment that deters compromise attempts (for example, through lighting, access paths, visible security measures, etc.)
3A-4.2	Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured.	Detailed instructions for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including specific examples of how devices can be physically secured.

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3A-4.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured (such as wireless, handheld, etc.) *For example, secure devices in a locked room when not in use, assign responsibility to specific individuals when in use, observe devices at all times, sign devices in/out, etc.*	Instructions for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured, such as wireless or handheld devices.
3A-5.1.5	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access. Procedures to include those items are described in 3A-5.1.1 through 3A-5.1.4	Detailed instructions for the merchant to implement procedures for identification and authorization of repair/maintenance personnel and third parties prior to granting access, including: • Procedures for verifying the identity and authorization of third-party personnel prior to granting access • Instructions that unexpected personnel must be denied access unless fully validated and authorized • Escorting and monitoring authorized personnel at all times • Maintaining a log of all third-party personnel access
3B-1.1.6	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for securing devices being removed from service, retired, or returned for repair.	Detailed procedures for the merchant to secure devices being returned or replaced, including: • Procedures and contact details for notifying affected entities—including the entity to which the device is being returned—before devices are returned • Procedures for transporting devices via a trusted carrier service • Procedures for packing and sending devices in serialized, counterfeit-resistant, and tamper-evident packaging • Procedures to ensure the solution provider can track devices during the return process
3B-1.2.3	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for the secure disposal of devices.	Detailed instructions for the merchant to implement procedures for the secure disposal of devices, including: • Returning devices only to authorized parties for destruction (including a list of authorized parties) • Procedures to render sensitive data irrecoverable, prior to device being shipped for disposal

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3B-2.1.3	Provide instructions via the *P2PE Instruction Manual* for the merchant outlining processes to follow in the event of a device encryption failure.	Detailed instructions for the merchant to follow in the event of a device encryption failure, including ensuring that devices are not re-enabled for use until merchant has confirmed with solution provider that either: • The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or • The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using alternative controls and/or processing method.
3B-2.3	Provide instructions via the *P2PE Instruction Manual*, including details of the opt-out process and instructions for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.	A clear description of the opt-out process and provides detailed instructions, including: • Procedures for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection • The method of communication for merchants to advise the solution provider that they wish to opt out of the P2PE solution • That if they choose to opt out, the merchant must formally acknowledge that they accept responsibility for the following: ○ The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. ○ Responsibility for implementing alternative controls to protect account data in lieu of the P2PE solution ○ That the merchant is no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution ○ Advising their acquirer that they are no longer using the P2PE solution ○ That processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. ○ Formal request that transactions be accepted without P2PE encryption • The method of communication that will be used for the merchant to provide their formal acknowledgement and acceptance of the above

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3B-6.2	Provide instructions via the *P2PE Instruction Manual* for the merchant to follow secure troubleshooting procedures.	Information for the merchant regarding the solution provider's troubleshooting processes, including that the solution provider ensures the following: • PAN and/or SAD is never output to the merchant environment • Collection of PAN and/or SAD only when needed to solve a specific problem • Storage of such data only in specific, known locations with limited access • Collection of only a limited amount of data needed to solve a specific problem • Encryption of account data while stored • Secure deletion of such data immediately after use
3B-8.1.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to perform periodic physical inspections of devices to detect tampering or modification of devices. Detailed procedures for performing periodic physical inspections to include: • Description of tamper-detection mechanisms • Guidance for physical inspections including photographs or drawings of the device illustrating what the merchant is to inspect, for example: ○ Missing or altered seals or screws, extraneous wiring, holes in the device or the addition of labels or other covering material that could be used to mask damage from device tampering). ○ Instructions for weighing the POI equipment, on receipt and then periodically, for comparison with vendor specification weight to identify potential insertion of tapping mechanisms within devices. • Recommendations for frequency of inspections	Detailed procedures for merchants to perform periodic physical inspections of devices to detect tampering or modification. Verify instructions include: • Description of tamper-detection mechanisms • Guidance for physical inspections including photographs or drawings of the device illustrating what the merchant is to inspect, for example: ○ Missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering) ○ Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices • Recommendations for frequency of inspections
3B-8.2.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement tamper-detection processes for devices deployed in remote or unattended locations—for example, the use of cameras or other physical mechanisms to alert personnel to physical breach.	Instructions for implementing tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3B-8.3.1	Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for responding to tampered devices.	Response procedures and contact details for reporting and responding to tampered devices
3B-9.1.1	Provide instructions and contact details via the *P2PE Instruction Manual* for the merchant to notify the solution provider of suspicious activity.	Instructions and contact details for the merchant to notify the solution provider of suspicious activity
3C-1.1.2	Provide specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices.	Specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices
3C-1.1.3	Provides specific details of all PCI-approved POI components used in the P2PE solution.	Details of all PCI-approved POI components used in the P2PE solution
3C-1.1.4	If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.	If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.
3C-1.1.5	Provide specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism (for example, if a PCI-approved SCR was connected to a non-PCI-approved keypad), the non PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.	Specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.

Domain 3 Requirement		Required Content for the *P2PE Instruction Manual*
3C-1.1.6	Provide specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: • Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device • Attempting to alter security configurations or authentication controls • Physically opening the device • Attempting to install applications onto the device	Specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: • Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device • Attempting to alter security configurations or authentication controls • Physically opening the device • Attempting to install applications onto the device

Domain 4: Segmentation between Encryption and Decryption Environments

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 4: Segmentation between Encryption and Decryption Environments Segregate duties and functions between encryption and decryption environments	▪ All decryption operations managed by solution provider. ▪ Merchant has no access to the encryption environment (within POI device) or decryption environment. ▪ Merchant has no involvement in encryption or decryption operations.	***Note that this domain has no applicable requirements for this hardware/hybrid scenario.***	

For these hardware/hybrid environments, segregation of functions and duties between the encryption and decryption zones is achieved since the merchant POI device and merchant environment are clearly separated from the solution provider's decryption environment. There are no people or processes outside of the solution provider's secure decryption zone that have access to any cryptographic keys or the ability to decrypt data.

For the above reason, this domain has no applicable requirements for this hardware/hybrid scenario, where all account-data processing and cryptographic operations are managed by a third-party solution provider.

Domain 5: Decryption Environment, Device and Systems Management

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 5: Decryption Environment, Device and Systems Management Secure decryption environments and decryption systems/devices.	▪ Decryption environment implemented at and managed by solution provider. ▪ Merchant has no access to the decryption environment. ▪ Decryption environment must be PCI DSS compliant.	**5A** Use approved HSMs. **5B** Secure all decryption systems and devices. **5C** Implement secure device and systems management processes. **5D** Maintain secure decryption environment. **5E** Implement secure hybrid decryption process.	▪ P2PE Solution Provider

A critical point of security is the environment where account data is decrypted and returned to clear text. To ensure that any systems responsible for key-management operations are developed and implemented securely, the key-management function and the environment into which it is deployed must satisfy the Point-to-Point Encryption Solution Requirements and undergo an annual PCI DSS assessment. Requirements in Domain 5 entail securing all decryption systems and devices and implementing monitoring and response procedures.

Note: *References to "**decryption devices and systems**" within this section is 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.

Unlike a hardware/hardware P2PE solution, the decryption of account data for a Hybrid P2PE solution is performed outside of an HSM on the Host System. In addition to the decryption of account data, the Host System may also be used for transaction processing; however, it should be not used for any purpose unrelated to these functions.

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

The solution provider's decryption environment may consist of multiple Host Systems in one or more locations. The Host System may take a variety of forms, for example, the Host System may be a dedicated PC with single or multiple processors, or a combination of hardware components operating as a single system. Where a Host System is comprised of multiple hardware components (for example, a server chassis containing multiple processors, servers, etc.), the connectivity between this hardware must be made through physical connections rather than using a network connection. Alternatively, the Host System may be comprised of a partition on a mainframe computing system. The solution provider's decryption environment may consist of multiple Host Systems in one or more locations.

The Host System is connected to one or more HSMs to securely protect the data-decryption keys (DDKs) when not in use. The HSM(s) is a fundamental component of a hardware/hybrid P2PE solution; however, unlike hardware/hardware solutions, the decryption of account data is performed outside of the HSM on the Host System. When the Host System is required to decrypt encrypted account data received from POI, the DDK is retrieved from a key store protected by the HSM, then passed to the Host System. The Host System then uses the DDK to decrypt the account in the software of the Host System. The Host System will temporarily retain DDKs in volatile memory for the purpose of decrypting account data. When the DDK reaches the end of its cryptoperiod, it will be erased from memory

The Host System and HSM(s) must reside on a network that is dedicated to decryption operations and transaction processing, which may also include services required to support these functions. The decryption network must be segmented from any other network or system that is not performing or supporting decryption operations or transaction processing.

Many parts of this section refer to the monitoring and tracking of decryption devices and systems throughout their lifecycle, regardless of whether or not they have previously been loaded with cryptographic keys or are being used to maintain the security of cryptographic keys. This is important as it provides assurance that the decryption devices and systems have not been tampered with, replaced, or modified in some way that could result in the leakage of cryptographic keys once they are loaded into the decryption devices and systems.

Domain 5 Requirements	Testing Procedures
Requirement 5A: Use approved HSMs	
5A-1 Use approved HSMs	
5A-1.1 Ensure that all hardware security modules (HSMs) are either: • FIPS140-2 Level 3 or higher certified, or • A PCI-approved HSM.	**5A-1.1.a** For all HSMs used in the solution, 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, or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.
	5A-1.1.b Examine documented procedures and interview personnel to verify that HSM 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 HSM(s) in the following characteristics: • Model name and number • Hardware version number • Firmware version number • For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment	**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 PCI PTS Devices to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Model name/number • Hardware version number • Firmware version number • Any applications, including application version number, resident within the device which were included in the PTS assessment
	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: • Model name/number • Hardware version number • Firmware version number

Domain 5 Requirements	Testing Procedures
5A-1.1.2 If FIPS-approved HSMs are used, the FIPS approval must cover all required functions used for the P2PE solution, including cryptographic algorithms, data-protection mechanisms, and key-management processes.	**5A-1.1.2** Examine FIPS approval documentation and HSM operational procedures to verify that the FIPS approval covers all HSM components and functions used for the P2PE solution, including cryptographic algorithms, data-protection mechanisms, and key-management processes.
5A-1.1.3 If FIPS-approved HSMs are used, the HSM must be configured to operate in the FIPS-approved mode for all operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.	**5A-1.1.3.a** Examine documented HSM operational procedures to verify they require HSMs to be configured to operate in the FIPS-approved mode for all P2PE operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.
	5A-1.1.3.b Examine HSM configurations for all P2PE solution functions to verify that HSMs are configured to operate in the FIPS-approved mode for all operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.
5A-1.2 HSMs must be deployed according to the security policy to which they have been approved. ***Note:*** *Both FIPS140-2 and the PCI PTS HSM standard require that the HSM manufacturer makes available a security policy document to end users, which provides information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.*	**5A-1.2** Examine the security policies for the HSMs and observe device implementations to verify HSMs are deployed in accordance with the security policy to which they have been approved.

Domain 5 Requirements	Testing Procedures
Requirement 5B: Secure all decryption systems and devices.	
Secure decryption devices and systems throughout their lifecycle.	
5B-1 Maintain inventory-control and monitoring procedures for decryption devices.	
5B-1.1 Maintain inventory-control and monitoring procedures to accurately track decryption devices and systems from receipt until decommissioning, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit The inventory-control and monitoring procedures must provide for the following:	**5B-1.1.a** Examine documented inventory-control procedures to confirm that they define methods for tracking decryption devices and systems from receipt through to decommissioning, including where devices, or systems, are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit
	5B-1.1.b Verify documented procedures include 5B-1.1.1 through 5B-1.1.3 below.
	5B-1.1.c Examine the documented decryption devices and systems inventory and observe the device and system locations to verify that the inventory-control and monitoring procedures accurately track the device and system locations.
5B-1.1.1 Record decryption device and system serial numbers in inventory-control system as soon as possible upon receipt and prior to installation.	**5B-1.1.1** Review documented device inventories and interview personnel to verify that decryption devices and systems are entered into the inventory-control system as soon as possible upon receipt of the device, and prior to installation.
5B-1.1.2 Decryption devices and systems must be protected against unauthorized substitution or modification until all applicable keys have been loaded.	**5B-1.1.2** Observe implemented controls and interview personnel to verify that decryption devices and systems are protected against unauthorized substitution or modification until all applicable keys have been loaded.
5B-1.1.3 Control and monitoring procedures must provide for detection of lost or stolen decryption devices and systems and notification to authorized personnel	**5B-1.1.3** Observe implemented controls and interview personnel to verify that procedures are implemented to detect lost or stolen decryption devices and systems, and notify authorized personnel.
5B-1.2 Perform decryption device and system inventories at least annually to detect removal or substitution of devices.	**5B-1.2.a** Examine documented procedures to verify decryption device and system inventories are required to be performed at least annually to detect removal or substitution of devices.
	5B-1.2.b Examine records of decryption device and system inventories and interview personnel to verify that decryption device and system inventories are performed at least annually.

Domain 5 Requirements	Testing Procedures
5B-1.3 Maintain a documented inventory of all decryption devices and systems to include at least the following: • Make, model, and hardware version of device • Location (including site/facility, if applicable) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Firmware version • Hardware version • Applications (including versions)	**5B-1.3.a** Verify through observation that a documented inventory of all decryption devices and systems is maintained.
	5B-1.3.b Verify the documented inventory includes at least the following: • Make, model, and hardware version of device • Location (including site/facility, if applicable) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Hardware version • Firmware version • Applications and versions
5B-1.3.1 Secure the documented inventory of decryption devices and systems from unauthorized access.	**5B-1.3.1** Observe implemented controls and interview personnel to verify the documented inventory of decryption devices and systems is secured from unauthorized access.
5B-1.4 Implement procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted decryption devices and systems.	**5B-1.4.a** Examine documented procedures to verify procedures are defined for detecting and responding to variances in the annual inventory, including identification of missing or substituted decryption devices and systems.
	5B-1.4.b Interview personnel to verify procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted decryption devices and systems, are implemented.
5B-2 Physically secure decryption devices and systems when not in use.	
5B-2.1 Physically secure the storage of decryption devices and systems awaiting deployment.	**5B-2.1.a** Examine documented procedures to verify they include storing decryption devices and systems awaiting deployment in a physically secure location.
	5B-2.1.b Inspect storage locations for decryption devices and systems awaiting deployment, to verify that the location is physically secure.

Domain 5 Requirements	Testing Procedures
5B-2.2 Physically secure the storage of decryption devices and systems/system components undergoing repair or otherwise not in use.	**5B-2.2.a** Examine documented procedures to verify they include storing decryption devices and systems/system components undergoing repair or otherwise not in use in a physically secure location.
	5B-2.2.b Inspect storage locations for decryption devices and systems/system components undergoing repair or otherwise not in use to verify that the location is physically secure.
5B-2.3 Physically secure the storage of decryption devices and systems awaiting transport between sites/locations.	**5B-2.3.a** Examine documented procedures to verify they include storing decryption devices and systems awaiting transport between sites/locations in a physically secure location.
	5B-2.3.b Inspect storage locations for decryption devices and systems awaiting transport between sites/locations to verify that the location is secure.
5B-2.4 Physically secure decryption devices and systems in transit, including: • Packing SCDs in tamper-evident packaging prior to transit • Implementing procedures for determining whether device or system packaging has been tampered with • Use of a defined, secure transport method, such as bonded carrier or secure courier	**5B-2.4.a** Examine documented procedures for the transportation of decryption devices and systems to verify they include: • Procedures for packing SCDs in tamper-evident packaging prior to transit • Procedures for determining whether device or system packaging has been tampered with • Procedures for using a defined, secure transport method, such as bonded carrier or secure courier
	5B-2.4.b For a sample of device shipments, examine records of decryption devices and systems transportation and interview personnel to verify that the following procedures are implemented: • SCDs are packed in tamper-evident packaging prior to transit. • Procedures are followed for determining if device and system packaging has been tampered with. • Use of a defined secure transport method, such as bonded carrier or secure courier.

Domain 5 Requirements	Testing Procedures
5B-2.4.1 Implement procedures to be followed upon determining that decryption device and system packaging has been tampered with, including: • Decryption devices and systems must not be deployed or used • Procedures for returning devices and system to authorized party for investigation • Escalation procedures and contact details for reporting tamper-detection	**5B-2.4.1.a** Examine documented procedures to verify they include procedures to be followed upon determining that decryption device and system packaging has been tampered with, including: • Decryption devices and systems must not be deployed or used • Procedures for returning decryption devices and systems to authorized party for investigation • Contact details for reporting tamper-detection
	5B-2.4.1.b Interview responsible personnel to verify that, upon determining that decryption device and system packaging has been tampered with, the following procedures are implemented: • Decryption devices and systems are not deployed or used. • Procedures are followed for returning devices and systems to authorized party for investigation. • Reporting of tamper-detection to defined contact details.

5B-2.5 Ensure decryption devices and systems are only transported between trusted sites/locations, as follows:
• A list of trusted sites (e.g., vendor / maintenance provider, etc.) is maintained.
• Only devices and systems received from trusted sites/locations are accepted for use.
• Procedures are defined in the event that devices and systems are received from untrusted or unknown locations, including:
  ○ Procedures (including contact details for authorized parties) for verifying location from which device or systems was sent
  ○ Procedures to ensure devices and systems are not used unless and until the source location is verified as trusted
• Decryption devices and systems are sent only to trusted sites/locations.
	5B-2.5.a Examine documented procedures to verify they include:
	• A list of trusted sites (e.g., vendor / maintenance provider, etc.) between which decryption devices and systems may be transported
	• Procedures to ensure that only devices and systems received from trusted sites/locations are accepted for use
	• Procedures to be followed in the event that devices and systems are received from an untrusted or unknown location, including:
	  ○ Procedures (including contact details for authorized parties) for verifying location from which device or system was sent
	  ○ Procedures to ensure devices and systems are not used unless and until the source location is verified as trusted
	• Procedures to ensure that decryption devices and systems are only sent to trusted sites/locations

Domain 5 Requirements	Testing Procedures

	5B-2.5.b For a sample of decryption device and system shipments, examine records of devices and system transportation and interview personnel to verify:
	• Only devices and systems received from trusted sites/locations are accepted for use.
	• Procedures are followed in the event that devices or systems are received from an untrusted or unknown location, including:
	  ○ Procedures (including contact details for authorized parties) for verifying the location from which a device or system was sent
	  ○ Procedures to ensure devices and systems are not used unless and until the source location is verified as trusted
	• Decryption devices and systems are only sent to trusted sites/locations

5B-3 Prevent and detect the unauthorized alteration or replacement of decryption devices and systems prior to and during deployment.	
5B-3.1 Ensure decryption devices and systems are placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering prior to being put into use.	**5B-3.1a** Review documented procedures to confirm that processes are defined to provide assurance that decryption devices and systems have not been substituted or subjected to unauthorized modifications or tampering prior to being put into use.
	5B-3.1b Observe processes and interview personnel to verify that processes are followed to provide assurance that decryption devices and systems have not been substituted or subjected to unauthorized modifications or tampering prior to being put into use.
5B-3.1.1 Implement controls to protect decryption devices and systems from unauthorized access up to deployment. Controls must include the following:	**5B-3.1.1.a** Review documented procedures to verify they include protecting decryption devices and systems from unauthorized access up to deployment.
	5B-3.1.1.b Verify documented procedures include 5B-3.1.1.1 through 5B-3.1.1.3 below.
	5B-3.1.1.c Verify procedures are implemented as follows:
5B-3.1.1.1 Ensure access to all decryption devices and systems is documented, defined, logged, and controlled.	**5B-3.1.1.1.a** Examine access-control documentation and system configurations to verify that access to all decryption devices and systems is defined and documented.
	5B-3.1.1.1.b For a sample of decryption devices and systems, observe authorized personnel accessing the devices and systems, and examine access logs to verify that all access is logged.

Domain 5 Requirements	Testing Procedures
	5B-3.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any decryption device or system.
5B-3.1.1.2 Decryption devices and systems must not use default keys (such as keys that are pre-installed for testing purposes), passwords, or data.	**5B-3.1.1.2** 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.
5B-3.1.1.3 All personnel with access to decryption devices and systems are documented in a formal list and authorized by management. The list of authorized personnel is reviewed at least annually.	**5B-3.1.1.3.a** Examine documented authorizations to verify: • All personnel with access to decryption devices and systems are documented in a formal list. • All personnel with access to decryption devices and systems are authorized by management. • The list of authorized personnel is reviewed at least annually.
	5B-3.1.1.3.b For a sample of decryption devices and systems, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to decryption devices and systems.
5B-3.1.2 Implement a documented "chain-of-custody" to ensure that all decryption devices and systems are controlled from receipt through to installation and use. The chain-of-custody must include records to identify responsible personnel for each interaction with the decryption devices and systems.	**5B-3.1.2.a** Examine documented processes to verify that the chain of custody is required for decryption devices and systems from receipt to installation and use.
	5B-3.1.2.b For a sample of decryption devices and systems, review documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to installation and use.
	5B-3.1.2.c Verify the chain of custody records identify responsible personnel for each interaction with the decryption device or system.
5B-3.1.3 Implement controls, including the following, to ensure that all received decryption devices and systems are from a legitimate source:	**5B-3.1.3.a** Examine documented purchasing, receipt, and deployment procedures to confirm that they include verifying all received decryption devices and systems are from a legitimate source.
	5B-3.1.3.b Confirm that the documented procedures include 5B-3.1.3.1 through 5B-3.1.3.2 below.
5B-3.1.3.1 SCD serial numbers must be compared to the serial numbers documented by the sender to ensure device substitution	**5B-3.1.3.1.a** Interview responsible personnel to verify that SCD serial numbers are compared to the serial number documented by the sender.

Domain 5 Requirements	Testing Procedures
has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document*	**5B-3.1.3.1.b** For a sample of received SCDs, review sender documentation (for example, the purchase order, shipping waybill, manufacturer's invoice, or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial numbers for the received device were verified to match that documented by the sender.
5B-3.1.3.2 Documentation used for this process must be received via a separate communication channel and must not have arrived with the shipment.	**5B-3.1.3.2** For a sample of received SCDs, review delivery records and interview responsible personnel to verify that documentation used to validate the device serial number was received via a separate communication channel than the device and was not received in the same shipment as the device.
5B-3.1.4 Implement physical protection of SCDs 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 (for example, via bonded carrier). The devices are then securely stored until key-insertion occurs. • Use of physically secure and trackable packaging (for example, pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored is 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. 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.	**5B-3.1.4.a** Examine documented procedures to confirm that they require physical protection of SCDs from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the defined methods.
	5B-3.1.4.b Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for SCDs, from the manufacturer's facility up to the point of key-insertion.
5B-3.1.5 Inspect and test all decryption devices and systems prior to installation to verify they have not been tampered with or compromised. Processes must include:	**5B-3.1.5.a** Examine documented procedures to verify they require inspection and testing of decryption devices and systems prior to installation to verify integrity of device or system.
	5B-3.1.5.b Verify documented procedures include 5B-3.1.5.1 through 5B-3.1.5.4, below.
5B-3.1.5.1 Running self-tests to ensure the correct operation of the decryption device and system.	**5B-3.1.5.1** Examine records of device inspections and tests, and observe tests in progress to verify that self-tests are run on decryption devices and systems to ensure the correct operation of the hardware.

Domain 5 Requirements	Testing Procedures
5B-3.1.5.2 Installing (or re-installing) decryption devices and systems only after confirming that the device or system has not been tampered with or compromised	**5B-3.1.5.2** Observe inspection processes and interview responsible personnel to verify that decryption devices and systems are installed, or reinstalled, only after confirming that the device or system has not been tampered with or compromised.
5B-3.1.5.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed.	**5B-3.1.5.3** 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.
5B-3.1.5.4 Maintaining records of the tests and inspections, and retaining records for at least one year.	**5B-3.1.5.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	5B-3.1.5.4.b Examine records of inspections to verify records are retained for at least one year.
5B-3.1.6 Maintain SCDs in original, tamper-evident packaging until ready for installation.	**5B-3.1.6.a** Examine documented procedures to verify they require SCD be maintained in original, tamper-evident packaging until ready for installation.
	5B-3.1.6.b Observe a sample of received SCDs to verify they are maintained in original, tamper-evident packaging until ready for installation.
5B-4 Physically secure decryption devices and systems to prevent unauthorized access, modification, or substitution of deployed devices.	
5B-4.1 Physically secure deployed decryption devices and systems to prevent unauthorized removal or substitution.	**5B-4.1.a** Examine physical security policy and procedures to verify decryption devices and systems must be physically secured to prevent unauthorized removal or substitution.
	5B-4.1.b Inspect the secure location in which the decryption devices and systems are deployed and verify that these devices and systems are physically secured to prevent unauthorized removal or substitution.
5B-4.2 Implement dual-control mechanisms to help prevent substitution of decryption devices and systems, both in-service and spare or backup devices and systems.	**5B-4.2.a** Examine documented procedures to verify that dual-control mechanisms are defined to prevent substitution of decryption devices and systems, both in-service and spare or backup devices and systems.
	5B-4.2.b Examine dual-control mechanisms in use, for both in-service and spare or backup decryption devices and systems, to verify that the mechanisms prevent substitution of devices and systems.

Domain 5 Requirements	Testing Procedures
5B-5 Prevent unauthorized physical access to decryption devices and systems in use.	
5B-5.1 Restrict physical access to decryption devices and systems to minimum required personnel.	**5B-5.1.a** Examine documented access privileges and procedures to verify that physical access to decryption devices and systems is restricted to minimum required personnel.
	5B-5.1.b Observe access controls and processes and interview personnel to verify that physical access to decryption devices and systems is restricted to the minimum required personnel.
5B-5.2 Implement procedures to control and document all physical access to decryption devices and systems in use. Procedures to include: • Identifying personnel authorized to access decryption devices and systems; • Restricting access to authorized personnel; • Maintaining a log of all access including personnel name, company, reason for access, time in and out. Retain access log for at least one year.	**5B-5.2.a** Examine documented access procedures and verify they require controlling and documenting all physical access to decryption devices and systems, and include: • Identifying personnel authorized to access decryption devices and systems • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out • Retaining access logs for at least one year
	5B-5.2.b Observe physical access controls to verify they include controlling and documenting all physical access to decryption devices and systems , and include: • Identifying personnel authorized to access decryption devices and systems • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out
	5B-5.2.c Examine the access logs/records to verify they are retained for at least one year and contain, at a minimum, the following details: • Personnel name • Company • Reason for access • Time in and out
5B-5.3 Implement procedures for identification and authorization of third-party personnel (including repair /maintenance personnel) prior to granting access to decryption devices and systems.	**5B-5.3.a** Examine documented procedures to verify they include identification and authorization of third-party personnel prior to granting access to decryption devices and systems.

Domain 5 Requirements	Testing Procedures
Procedures must include the following:	**5B-5.3.b** Verify documented procedures include 5B-5.3.1 through 5B-5.3.4 below.
5B-5.3.1 Procedures to verify the identity and authorization of third-party personnel prior to granting access to decryption devices and systems.	**5B-5.3.1** Interview personnel and observe processes to confirm that the identity and authorization of third-party personnel is verified prior to granting access to decryption devices and systems.
5B-5.3.2 Unexpected personnel must be denied access unless fully validated and authorized.	**5B-5.3.2** Interview responsible personnel and observe processes to verify that unexpected personnel are denied access until fully validated and authorized.
5B-5.3.3 Once authorized, third-party personnel must be escorted and monitored at all times.	**5B-5.3.3** Interview responsible personnel and observe processes to verify that, once authorized, third-party personnel are escorted and monitored at all times.
5B-5.3.4 A log of all third-party personnel access is maintained in accordance with 5B-5.2.	**5B-5.3.4** Examine access logs/records to verify that a log of all third-party personnel access is maintained in accordance with logging requirements defined in 5B-5.2.
5B-6 Maintain secure updates for decryption devices and systems.	
5B-6.1 Implement secure update processes for all firmware and software updates, to include: • Integrity check of the update • Authentication of origin of the update	**5B-6.1.a** Examine documented procedures to verify secure update processes are defined for all firmware and software updates, and include: • Integrity check of the update • Authentication of origin of the update
	5B-6.1b 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

Domain 5 Requirements	Testing Procedures
Requirement 5C: Implement secure decryption device and system management processes.	
5C-1 Securely maintain decryption devices and systems.	
5C-1.1 Document operational security procedures for physical security controls and operational activities throughout decryption device and system lifecycle, including but not limited to: • Installation procedures • Maintenance and repair procedures • Production procedures • Replacement procedures • Destruction procedures	**5C-1.1** Verify operational security procedures are documented for physical security controls and operational activities throughout decryption device and system lifecycle, including but not limited to. • Installation procedures • Maintenance and repair procedures • Production procedures • Replacement procedures • Destruction procedures
5C-1.2 Procedures must be in place and implemented to protect decryption devices and systems, and ensure the destruction of any cryptographic keys or key material within such decryption devices and systems when removed from service, retired at the end of the deployment lifecycle, or returned for repair.	
5C-1.2.1 Procedures are in place to ensure that any decryption devices and systems to be removed from service, retired, or returned for repair are not intercepted or used in an unauthorized manner, as follows:	**5C-1.2.1.a** Examine documented procedures to verify that procedures are defined for any decryption devices and systems to be removed from service, retired, or returned for repair.
	5C-1.2.1.b Verify documented procedures include 5B-1.2.1.1 through 5B-1.2.1.5 below.
5C-1.2.1.1 Affected entities are notified before decryption devices and systems are returned.	**5C-1.2.1.1** Interview responsible personnel and examine decryption device and system return records to verify that affected entities are notified before decryption devices and systems are returned.
5C-1.2.1.2 Decryption devices and systems are transported via trusted carrier service—for example, bonded carrier.	**5C-1.2.1.2** Interview responsible personnel and examine decryption device and system return records to verify that decryption devices and systems are transported via trusted carrier service—for example, bonded carrier.

Domain 5 Requirements	Testing Procedures
5C-1.2.1.3 Decryption devices and systems are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	**5C-1.2.1.3** Interview responsible personnel and observe decryption device and system return processes and packaging to verify that decryption devices and systems are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.
5C-1.2.1.4 Decryption devices and systems are tracked during the return process.	**5C-1.2.1.4** Interview responsible personnel and examine decryption device and system return records to verify that devices are tracked during the return process.
5C-1.2.1.5 Once received decryption devices and systems remain in their packaging (as defined in 5C-1.2.1.3) until ready for repair or destruction.	**5C-1.2.1.5** Interview responsible personnel and observe decryption device and systems return processes to verify that once received, decryption devices and systems remain in their packaging (defined in 5C-1.2.1.3) until ready for destruction.
5C-1.2.2 When decryption devices and systems are removed from service permanently or for repair, all keys and key material, and all account data stored within the device or system must be rendered irrecoverable. Processes must include the following:	**5C-1.2.2** Verify that documented procedures for removing decryption devices and systems from service include the following: • Procedures require that all keys and key material, and all account data stored within the device or system be securely destroyed. • Procedures cover all devices and systems removed from service permanently or for repair. • Procedures include 5C-1.2.2.1 through 5C-1.2.2.4 below.
5C-1.2.2.1 Dual control is implemented for all critical decommissioning processes.	**5C-1.2.2.1** Interview personnel and observe processes for removing decryption devices and systems from service to verify dual control is implemented for all critical decommissioning processes.
5C-1.2.2.2 Key and data storage (including account data) are rendered irrecoverable (for example, zeroized). If data cannot be rendered irrecoverable, the decryption device or system/system component must be physically destroyed to prevent the disclosure of any sensitive data or keys.	**5C-1.2.2.2** Interview personnel and observe processes for removing decryption devices and systems from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized), or that devices and systems/system components are physically destroyed to prevent the disclosure of any sensitive data or keys.
5C-1.2.2.3 Decryption devices and systems being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	**5C-1.2.2.3** Interview personnel and observe processes for removing decryption devices and systems from service to verify that tests and inspections of decryption devices and systems are performed to confirm that keys and account data have been rendered irrecoverable.

Domain 5 Requirements	Testing Procedures
5C-1.2.2.4 Records of the tests and inspections are maintained for at least one year.	**5C-1.2.2.4** Interview personnel and examine records to verify that records of the tests and inspections (as required in 5C-1.2.2.3) are maintained for at least one year.
5C-1.2.3 Document and log the removal process for the repair or decommissioning of decryption devices and systems.	**5C-1.2.3** For a sample of decryption devices and systems removed for repair or decommissioning, examine records of devices and systems removal to verify that the process is documented and logged.
5C-1.2.4 Implement procedures for secure disposal of decryption devices and systems, including return of devices and systems to an authorized party for destruction.	**5C-1.2.4.a** Examine documented procedures to verify they include the secure disposal of decryption devices and systems, including return of devices and systems to an authorized party for destruction.
	5C-1.2.4.b For a sample of decryption devices and systems removed for disposal, examine records of devices and systems removal to verify that devices and systems are returned to an authorized party for destruction.
Logically secure decryption equipment.	
5C-2 Implement administration procedures for logically securing decryption devices and systems.	
5C-2.1 Implement procedures to provide secure administration of decryption devices and systems including but not limited to: • Management of user interface • Password/smart card management • Console and non-console administration • Access to physical keys • Use of HSM commands	**5C-2.1.a** Examine documented procedures to verify secure administration procedures are defined for decryption devices and systems including: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands
	5C-2.1.b Observe authorized personnel performing decryption device and system-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

Domain 5 Requirements	Testing Procedures
5C-2.2 Implement a process/mechanism to protect the HSM's Application Program Interfaces (APIs) from misuse. *For example, require authentication between the API and the HSM and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate access to the API, the process should limit the exposure of the HSM to a host via connection by a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (for example, high speed serial or dedicated Ethernet).*	**5C-2.2.a** Examine documented procedures and processes to verify that a process/mechanism is defined to protect the HSM's Application Program Interfaces (APIs) from misuse.
	5C-2.2.b Interview responsible personnel and observe HSM system configurations and processes to verify that the defined process/mechanism is implemented and protects the HSM's Application Program Interfaces (APIs) from misuse.
5C-3 Restrict logical access to decryption devices and systems to authorized personnel.	
5C-3.1 Logical access controls must be implemented to ensure only authorized personnel have access to decryption devices and systems.	**5C-3.1.a** Examine documentation to verify that a list of personnel authorized to access decryption devices and systems is defined.
	5C-3.1.b For a sample of decryption devices and systems, observe access controls and privilege assignments on decryption devices and systems to verify only authorized personnel (as defined in 5B-3.1.a) have access to the decryption device or system.
5C-3.2 Access and permissions must be granted based on least privilege and need to know.	**5C-3.2.a** Examine documented access-control policies and procedures to verify that access and permissions must be assigned according to least privilege and need to know.
	5C-3.2.b For a sample of decryption devices and systems and personnel, observe configured accounts and permissions, and interview responsible personnel to verify that the level of access and permission granted are according to least privilege and need to know.
5C-4 Provide a mechanism for POI device authentication.	
5C-4.1 POI devices are 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.*	**5C-4.1.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.

Domain 5 Requirements	Testing Procedures
	5C-4.1.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
	5C-4.1.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.
5C-5 Implement tamper-detection mechanisms.	
5C-5.1 Perform periodic physical inspections of decryption devices and systems at least monthly to detect tampering or modification of devices. Inspections to include: • The device and system itself • Cabling/connection points • Physically connected devices	**5C-5.1.a** Examine documented procedure to verify that periodic inspection of decryption devices and systems is required at least monthly to detect signs of tampering or modification, and that inspection procedures include: • The device and system itself • Cabling/connection points • Physically connected devices
	5C-5.1.b Interview personnel performing inspections and observe inspection processes to verify that inspections include: • The device and system itself • Cabling/connection points • Physically connected devices
	5C-5.1.c Interview personnel performing inspections and review supporting documentation to verify that physical inspections are performed at least monthly.
5C-6 Documented procedures exist and are demonstrably in use to ensure the security and integrity of decryption devices and systems placed into service, initialized, deployed, used, and decommissioned.	
5C-6.1 All affected parties are aware of required processes and provided suitable guidance on the secure procedures for decryption devices and systems placed into service, initialized, deployed, used, and decommissioned.	**5C-6.1** Examine documented procedures and processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for decryption devices and systems placed into service, initialized, deployed, used, and decommissioned

Domain 5 Requirements	Testing Procedures
5C-6.2 Procedures that govern access HSMs must be documented, implemented, and known to data-center personnel and any others involved with the physical security of such devices. HSM protections must include at least the following:	**5C-6.2.a** Examine documented procedures to verify that procedures are defined to govern access to all HSMs, and include Requirements 5C-6.2.1– 5C-6.2.4 below.
	5C-6.2.b Interview data-center personnel and others responsible for the physical security of the HSMs to verify that the documented procedures are known.
5C-6.2.1 Any physical keys needed to activate the HSM are stored securely.	**5C-6.2.1** Interview responsible personnel and observe key-storage locations and security controls to verify that any physical keys needed to activate the HSM are stored securely.
5C-6.2.2 If multiple physical keys are needed to activate the HSM: • They are assigned to separate designated custodians; and • Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.	**5C-6.2.2** If multiple physical keys are needed to activate the HSM, interview responsible personnel and observe key operations to verify that: • Keys are assigned to separate designated custodians; and • Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.
5C-6.2.3 Anti-tamper sensors are enabled as required by the security policy of the HSM.	**5C-6.2.3** Examine HSM security policy and HSM anti-tamper controls to verify that anti-tamper sensors are enabled as required by the security policy of the HSM.
5C-6.2.4 When HSMs are connected to online systems, they are not enabled in a sensitive state. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	**5C-6.2.4** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems

Requirement 5D: Maintain Secure Decryption Environment

Monitor decryption environment.	
5D-1 Perform logging and monitor decryption environment for suspicious activity.	

Domain 5 Requirements	Testing Procedures
5D-1.1 Ensure that changes to the critical functions of the decryption devices and systems are logged. ***Note:*** *Critical functions include but are not limited to application and firmware updates, as well as changes to security-sensitive configurations.*	**5D-1.1** Examine system configurations and correlating log files to verify that any changes to the critical functions of decryption devices and systems are logged, including: • Changes to the applications • Changes to the firmware • Changes to any security-sensitive configurations
5D-1.2 Implement mechanisms to provide immediate notification of potential security breaches, including but not limited to: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API	**5D-1.2.a** Examine documented procedures to verify mechanisms are defined to provide immediate notification of potential security breaches, including: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API
	5D-1.2.b Interview personnel and observe implemented mechanisms to verify they provide immediate notification of potential security breaches in the following instances: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API
5D-2 Detect encryption failures.	
5D-2.1 Implement controls to detect encryption failures and provide immediate notification. Controls must include at least the following: ***Note:*** *Although Domain 5 is concerned with the decryption environment, not the encryption environment, it is the duty of the solution provider to actively monitor traffic received into the decryption environment to confirm that the POI equipment in the merchant environment is not outputting clear-text CHD through error or misconfiguration.*	**5D-2.1** Examine documented procedures to verify controls are defined for the following: • Procedures are defined to detect encryption failures, and include 5D-2.1.1 through 5D-2.1.4 below. • Procedures include immediate notification upon detection of an encryption failure, for each 5D-2.1.1 through 5D-2.1.4 below.

Domain 5 Requirements	Testing Procedures
5D-2.1.1 Checking for incoming clear-text account data.	**5D-2.1.1.a** Observe implemented processes to verify controls are in place to check for incoming clear-text account data.
	5D-2.1.1.b Observe implemented controls and notification mechanisms, and interview personnel to verify that personnel are immediately notified upon detection of incoming clear-text account data.
5D-2.1.2 Reviewing any decryption errors reported by the HSM or the Host System, which may be caused by inputting clear-text data when only encrypted data is expected.	**5D-2.1.2.a** Observe implemented processes to verify controls are in place to review any decryption errors reported by the HSM or the Host System, which may be caused by inputting clear-text data when only encrypted data is expected.
	5D-2.1.2.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of decryption errors reported by the HSM or Host System caused by inputting clear-text data when only encrypted data is expected.
5D-2.1.3 Reviewing any unexpected transaction data received. *For example, transaction data received without an expected authentication data block (such as a MAC or signature).*	**5D-2.1.3.a** Observe implemented processes to verify controls are in place to review any unexpected transaction data received.
	5D-2.1.3.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of encryption failures in any unexpected transaction data received.
5D-2.1.4 Reviewing data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.	**5D-2.1.4.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.
	5D-2.1.4.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of encryption failures from POI devices that are causing an unusually high rate of transaction authorization rejections.
5D-2.2 Identify source of encryption failure (device, function).	**5D-2.2.a** Examine documented procedures to verify they include procedures for identifying the source of encryption failures.
	5D-2.2.b Observe implemented controls and interview personnel to verify that the source of any encryption failures is identified (device, function).
5D-3 Implement incident-response procedures.	

Domain 5 Requirements	Testing Procedures
5D-3.1 Implement procedures for responding to security incidents, including the following:	
5D-3.1.1 Implement procedures for responding to tampered decryption devices and systems.	**5D-3.1.1.a** Examine documented incident-response procedures to verify that procedures are defined for responding to tampered decryption devices and systems.
	5D-3.1.1.b Interview response personnel to verify that procedures for responding to tampered decryption devices and systems are known and implemented.
5D-3.1.2 Implement procedures for responding to missing or substituted decryption devices and systems.	**5D-3.1.2.a** Examine documented incident-response procedures to verify that procedures are defined for responding to missing or substituted decryption devices and systems.
	5D-3.1.2.b Interview response personnel to verify that procedures for responding to missing or substituted decryption devices and systems are known and implemented.
5D-3.1.3 Implement procedures for responding to unauthorized key-management procedures or configuration changes.	**5D-3.1.3.a** Examine documented incident-response procedures to verify that procedures are defined for responding to unauthorized key-management procedures or configuration changes.
	5D-3.1.3.b Interview response personnel to verify that procedures for responding to unauthorized key-management procedures or configuration changes are known and implemented.
5D-3.1.4 Implement procedures for responding to disconnect/reconnect of decryption devices and systems.	**5D-3.1.4.a** Examine documented incident-response procedures to verify that procedures are defined for responding to disconnect/reconnect of decryption devices and systems.
	5D-3.1.4.b Interview response personnel to verify that procedures for responding to disconnect/reconnect of decryption devices and systems are known and implemented.
5D-3.1.5 Implement procedures for responding to failure of any decryption device and system security control.	**5D-3.1.5.a** Examine documented incident-response procedures to verify that procedures are defined for responding to failure of any decryption device and system security control.
	5D-3.1.5.b Interview response personnel to verify that procedures for responding to failure of any decryption device and system security control are known and implemented.

Domain 5 Requirements	Testing Procedures
5D-3.1.6 Implement procedures for responding to encryption/decryption failures.	**5D-3.1.6.a** Examine documented incident-response procedures to verify that procedures are defined for responding to encryption failure.
	5D-3.1.6.b Interview response personnel to verify that procedures for responding to encryption failure are known and implemented.
5D-3.2 Procedures must incorporate any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.	**5D-3.2.a** Examine documented incident-response procedures to verify that procedures incorporate any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.
	5D-3.2.b Interview response personnel to verify that any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents, are known and implemented.
Secure the decryption environment.	
5D-4 PCI DSS compliance of decryption environment.	
5D-4.1 Decryption environment must be secured according to PCI DSS.	**5D-4.1.a** Review the "Scope of Work" 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.
	5D-4.1.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.
	5D-4.1.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.
	5D-4.1.d Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that the P2PE solution provider's decryption environment was assessed as meeting PCI DSS requirements within the previous 12 months.

Domain 5 Requirements	Testing Procedures
Requirement 5E: Implement secure hybrid decryption process	
5E-1 Configure Host System securely	
5E-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.	**5E-1.1.a** Interview relevant 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.
	5E-1.1.b Interview relevant 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 the decryption environment, to verify that the document is current.
	5E-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 within the decryption environment, to verify that it accurately represents the decryption environment.
5E-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.*	**5E-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.
	5E-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.
5E-1.3 The Host System and HSM must reside on a network that is dedicated to decryption operations and/or transaction processing, and must be segmented from any other network or system that is not performing or supporting decryption operations or transaction processing.	**5E-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.

Domain 5 Requirements	Testing Procedures
	5E-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.
5E-1.4 All application software installed on the Host System must be authorized and have a business justification.	**5E-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.
	5E-1.4.b Examine change control and system configuration records to verify that all application software installed on the Host System is authorized.
	5E-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.
5E-1.5 A process, either automated or manual, must be in place to either prevent, or detect and alert, any unauthorized changes to applications/software on the Host System.	**5E-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.
	5E-1.5.b Interview personnel and observe system configurations to verify that controls are implemented either prevent, or detect and alert personnel, upon any unauthorized changes to applications/software.
	5E-1.5.c Examine output from the implemented process to verify that any unauthorized changes to applications/software are either prevented or detected and personnel alerted.
5E-1.6 The Host System must perform a self-test when it is powered up to ensure it is functioning properly 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 • Testing of any operating system software on which decryption operations are dependent	**5E-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 it is functioning properly before use. As a minimum, the self-test must include 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 • Testing of any operating system software on which decryption operations are dependent

Domain 5 Requirements	Testing Procedures
	5E-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 it is functioning properly before use. The self-test must include, as a minimum, the tests described in 5E-1.6.a.
5E-1.7 The Host System must perform a self-test when a security-impacting function or operation is modified (for example, an integrity check of the software/firmware must be performed upon loading of a software/firmware update).	**5E-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.
	5E-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.
5E-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 5E-1.6 and 5E-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.*	**5E-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 5E-1.6 and 5E-1.7 • Failure of a security function or mechanism
	5E-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 any of the conditions described in 5E-1.8.a.
5E-1.9 Alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate response procedure.	**5E-1.9.a** Review documented procedures to verify alerts generated from Host System must be documented and result in notification to authorized personnel and initiate response procedure.
	5E-1.9.b Examine system configurations and records of documented alert events to verify alerts generated from the Host System are documented.
	5E-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.

Domain 5 Requirements	Testing Procedures
5E-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 5E-1.8 • During self-tests, as described in Requirements 5E-1.6 and 5E-1.7 • During diagnostics of cryptographic operations	**5E-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 5E-1.8 • During self-tests, as described in Requirements 5E-1.6 and 5E-1.7 • During diagnostics operations
	5E-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 5E-1.8 • During self-tests, as described in Requirements 5E-1.6 and 5E-1.7 • During diagnostics operations
5E-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.	**5E-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.
	5E-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.
5E-1.12 The clear-text data-decryption keys must not be accessible to any processes or functions not directly required for decryption operations.	**5E-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.
	5E-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.
5E-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	**5E-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.
	5E-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.

Domain 5 Requirements	Testing Procedures
5E-1.14 The Host System must not write clear-text cryptographic keys to persistent storage (for example, hard drives, removable storage, flash drives etc.) except for the following: • Memory "swap/page" file purposes • "Core dumps" of memory required for trouble-shooting	**5E-1.14.a** Examine documented configuration procedures to verify that the Host System must not write clear-text cryptographic keys to persistent storage (for example, hard drives, removable storage, flash drives etc.) except for the following: • Memory "swap/page" file purposes • "Core dumps" of memory required for trouble-shooting
In the above circumstances, the following conditions apply:	**5E-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
	5E-1.14.c Verify documented procedures include Requirements 5E-1.14.1 through 5E-1.14.5 below.
5E-1.14.1 The locations must be predefined and documented.	**5E-1.14.1.a** Review Host System configuration standards to verify that storage locations of any "swap/page" files and "core dumps" are defined.
	5E-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.
5E-1.14.2 Storage can only be made to a dedicated hard drive (on its own bus) within the Host System.	**5E-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 within the Host System.
5E-1.14.3 The swap/page files and/or core dumps must never be backed up or copied.	**5E-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:
	5E-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.
5E-1.14.4 Access to, and the use of any tools used for trouble-shooting or forensics must be strictly controlled.	**5E-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.
	5E-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.

Domain 5 Requirements	Testing Procedures
	5E-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.
5E-1.14.5 All files must be securely deleted: • Core dumps must be securely deleted immediately after analysis. • Memory "swap/page" files must be securely deleted upon system shut down or reset.	**5E-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.
	5E-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.
5E-2 Configure access controls for Host System	
5E-2.1 Change host user passwords at least every 30 days. ***Note:*** *This requirement applies to all user roles associated to persons with access to the Host System.*	**5E-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.
	5E-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.
5E-2.2 User Passwords must meet the following: • Consist of a minimum of eight characters in length. • Consist of a combination of numeric, alphabetic and special characters. Or have equivalent (or better) strength/complexity.	**5E-2.2.a** Examine documented policies and procedures to verify that user passwords must: • Consist of a minimum of eight characters in length. • Consist of a combination of numeric, alphabetic and special characters. Or have equivalent (or better) strength/complexity.
	5E-2.2.b Inspect Host System(s) configuration settings to verify that user passwords: • Consist of a minimum of eight characters in length. • Consist of a combination of numeric, alphabetic and special characters. Or have equivalent (or better) strength/complexity.
5E-2.3 Where log-on security tokens (for example, 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/pass phrase to enable their usage. The PIN/pass phrase must be at least ten decimal characters in length, or equivalent.	**5E-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/pass phrase to enable their usage.
	5E-2.3.b Examine token-configuration settings to verify parameters are set to require PINs/passwords be at least ten decimal characters in length, or equivalent.

Domain 5 Requirements	Testing Procedures
5E-2.4 User accounts must be locked out of the Host System after no more than five failed logon attempts.	**5E-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 failed logon attempts.
	5E-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 failed logon attempts.
5E-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	**5E-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
	5E-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.
	5E-2.5.c Interview a sample of users for each role to verify the assigned role is appropriate for their job function.
5E-2.6 The segregation of duties must be enforced between roles, through automated or manual processes, to ensure that no one person 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:	

Domain 5 Requirements	Testing Procedures
5E-2.6.1 A Host System user is not permitted to have more than one of the following roles, as described in Requirement 5E-2.5: • Host System administrator role • Cryptographic administrator role • Host System security role	**5E-2.6.1.a** Examine documented access-control procedures to verify that a Host System user is not permitted to have more than one of the following roles, as described in Requirement 5E-2.5: • Host System administrator role • Cryptographic administrator role • Host System security role
	5E-2.6.1.b Inspect the Host System(s) configuration settings and/or documented records to verify that a Host System user is not permitted to have more than one of the following roles, as described in Requirement 5E-2.5: • Host System administrator role • Cryptographic administrator role • Host System security role
5E-2.6.2 A Host System user is not permitted to audit their own activity on the Host System.	**5E-2.6.2.a** Examine documented procedures to verify that a Host System user is not permitted to audit their own activity on the Host System.
	5E-2.6.2.b Interview audit personnel to verify that a Host System user is not permitted to audit their own activity on the Host System.
5E-2.6.3 A Host System administrator must use their operator-level account (see Requirement 5E-2.5) when performing non-administrative functions.	**5E-2.6.3.a** Review documented policies and procedures to verify a Host System administrator must use their operator-level account when performing non-administrative functions.
	5E-2.6.3.b Interview and observe Host System administrators to verify they use their operator-level account when performing non-administrative functions.
5E-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.	**5E-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.

Domain 5 Requirements	Testing Procedures
	5E-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.
	5E-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.
5E-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.	**5E-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.
	5E-2.8.b Examine records and interview personnel to verify that access privileges are reviewed, as a minimum, on a quarterly basis.
5E-2.9 Tamper detection mechanisms must be implemented on the host, to include an alert generation upon opening of Host System case, covers and/or doors.	**5E-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 Host System case, covers and/or doors.
	5E-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 Host System case, covers and/or doors.
	5E-2.9.c Review records of alerts and interview personnel to verify an alert is generated upon opening of the Host System case, covers and/or doors.
5E-3 Configure non-console access to Host System	
The term "non-console access" refers to any authorized access to the Host System performed by a person who is not physically present at the host processing system located within the secure room.	
5E-3.1 All non-console access to the Host System must use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.).	**5E-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 (for example, SSL/TLS, IPSec, SSH, etc.)

Domain 5 Requirements	Testing Procedures
	5E-3.1.b Inspect the configuration settings of system components to verify that all traffic transmitted over the secure channel uses strong cryptography.
5E-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 System, for example, "split tunneling".	**5E-3.2.a** Inspect the configuration settings of the secure channel, to verify that "split tunneling" is prohibited.
	5E-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.
5E-3.3 All non-console access to the Host System must use two-factor authentication.	**5E-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.
	5E-3.3.b Observe a Host System administrator log on to the device which provides non-console access to the Host System, to verify that two-factor authentication is required.
5E-3.4 Non-console connections to the Host System must only be permitted from authorized systems.	**5E-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.
	5E-3.4.b For a sample of systems, examine device configurations to verify that non-console access is permitted only from the authorized systems.
5E-3.5 Non-console access to the Host System must only be permitted from a PCI DSS compliant environment.	**5E-3.5** Verify that non-console access to the Host System is only permitted from a PCI-compliant environment, including 5E-3.5.1 through 5E-3.5.2. Review solution provider documentation, including data flow diagrams. Perform the following:
5E-3.5.1 The authorized system from which non-console access originates must meet all applicable PCI DSS requirements. For example, system hardening, patching, anti-virus protection and a local firewall etc.	**5E-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.
5E-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.	**5E-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.

Domain 5 Requirements	Testing Procedures
5E-3.6 Users with access to non-console connections to the Host System must be authorized to use non-console connections.	**5E-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.
	5E-3.6.b Examine a sample of access control records and compare them to the Host System settings to verify that non-console access to the Host System is only provided to authorized users.
5E-3.7 Non-console inactive sessions to the Host System must be terminated after 15 minutes of inactivity.	**5E-3.7.a** Review documented policies and procedures to verify that the Host System parameters are set to terminate non-console sessions after 15 minutes of inactivity.
	5E-3.7.b Inspect the system configuration settings to verify that the Host System parameters are set to terminate non-console sessions after 15 minutes of inactivity.
5E-4 Secure the Host System physical environment	
5E-4.1 The Host System must be located within a physically secure room that is dedicated to decryption operations and transaction processing.	**5E-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.
5E-4.2 All individuals must be identified and authenticated before being granted access to the secure room – e.g. badge-control system, biometrics.	**5E-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.
	5E-4.2.b Examine physical access controls to verify that all individuals are identified and authenticated before being granted access to the secure room.
	5E-4.2.c Observe authorized personnel entering the secure room to verify that all individuals are identified and authenticated before being granted access.
5E-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 all types of access, including badge access systems and/or manual sign-in sheets, as applicable.	**5E-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 all types of access, including badge access systems and/or manual sign-in sheets, as applicable.

Domain 5 Requirements	Testing Procedures
	5E-4.3.b Examine a sample logs of 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 all types of access, including badge access systems and/or manual sign-in sheets, as applicable.
	5E-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
5E-4.4 Dual access is required for the secure room housing the Host System.	**5E-4.4.a** Inspect physical access controls to verify that dual access is enforced.
	5E-4.4.b Observe authorized personnel entering the secure room to verify that dual access is enforced.
5E-4.5 Dual occupancy is required for the secure room, such that the room is never be occupied by a single individual for more than 30 seconds. ***For example:*** *The secure room is never occupied by a single individual except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.*	**5E-4.5.a** Examine documented policies and procedures to verify that the secure room requires dual occupancy such that the room is never occupied by a single individual for more than 30 seconds.
	5E-4.5.b Examine security-system configurations to verify that the secure room must never be occupied by a single individual for more than 30 seconds.
5E-4.6 Anytime a single occupancy exceeds 30 seconds, the system must automatically generate an audit event that is followed up by security personnel.	**5E-4.6.a** Examine documented policies and procedures to verify that the system must automatically generate an audit event that is followed up by security personnel, any time a single occupancy exceeds 30 seconds.
	5E-4.6.b Observe mechanisms in use to verify that the system automatically generates an audit event when single occupancy exceeds 30 seconds.
	5E-4.6.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.
5E-4.7 Physical access is only permitted to designated personnel with defined business needs and duties.	**5E-4.7.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.

Domain 5 Requirements	Testing Procedures
	5E-4.7.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.
	5E-4.7.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.
5E-4.8 Access to the secure room must be recorded by CCTV on a 24 hour basis. This must include, as a minimum, the following areas: • All entrances and exits • Access to the Host System and HSM(s) ***Note:*** *Motion-activated systems that are separate from the intrusion-detection system may be used.*	**5E-4.8.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 exits • Access to the Host System and HSM(s)
	5E-4.8.b If CCTV is motion-activated, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.
5E-4.9 Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, or other systems which may expose sensitive data.	**5E-4.9** 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.
5E-4.10 CCTV recorded images must be securely archived for at least 45 days.	**5E-4.10.a** Examine a sample of recordings to verify that at least the most recent 45 days of images are securely archived.
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.	**5E-4.10.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.
5E-4.11 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.	**5E-4.11.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.
	5E-4.11.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
5E-4.12 Continuous or motion-activated, appropriate lighting must be provided for the cameras monitoring the secure room.	**5E-4.12.a** Observe the secure room to verify that continuous or motion-activated lighting is provided for the cameras monitoring the secure room.

Domain 5 Requirements	Testing Procedures
Note: *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (for example, if intra-red cameras are use).*	**5E-4.12.b** Examine a sample of recorded CCTV images to verify that appropriate lighting is provided when persons are present in the secure room.
5E-4.13 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.	**5E-4.13.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.
	5E-4.13.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.
5E-4.14 Any windows in the secure room must be locked, protected by alarmed sensors, or otherwise similarly secured.	**5E-4.14.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	5E-4.14.b Examine configuration of window sensors to verify that the alarm mechanism is active.
5E-4.15 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**5E-4.15** Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
5E-4.16 Access-control and monitoring systems must be connected to an uninterruptible power source (UPS) to prevent outages.	**5E-4.16** Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems are powered through the UPS.
5E-4.17 All alarm events must be logged.	**5E-4.17.a** Examine security policies and procedures to verify they require that all alarm events are logged.
	5E-4.17.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
5E-4.18 Documented alarm events must be signed off by an authorized person who was not involved in the event.	**5E-4.18.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.

Domain 5 Requirements	Testing Procedures
	5E-4.18.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.
5E-4.19 Use of an emergency entry or exit mechanism must cause an alarm event.	**5E-4.19** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
5E-4.20 Authorized personnel must respond to all physical intrusion alarms within 30 minutes.	**5E-4.20.a** Examine documented policies and procedures to verify they define that all alarm events are responded to by authorized personnel within 30 minutes.
	5E-4.20.b Examine documented alarm events and interview personnel to verify that all alarm events were responded to by authorized personnel, within 30 minutes.
5E-4.21 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.*	**5E-4.21.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.
	5E-4.21.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	5E-4.21.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
5E-4.21.1 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.	**5E-4.21.1.a** If a manual synchronization process is implemented, interview responsible personnel an examine records of synchronization to verify the mechanism is performed at least quarterly.
	5E-4.21.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.
5E-4.22 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.*	**5E-4.22** Observe authorized personnel entering the secure room to verify that a mechanism 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.*
5E-4.23 An audible alarm must sound if the entrance to the secure room remains open for more than 30 seconds.	**5E-4.23.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.

Domain 5 Requirements	Testing Procedures
	5E-4.23.b Observe authorized personnel entering the secure room and request the door is held open. Verify that an audible alarm sounds after a period of no longer than 30 seconds.

Domain 6: P2PE Cryptographic Key Operations

	P2PE Hardware/Hybrid		
Domain	**Characteristics**	**P2PE validation**	
		Requirements	**Responsibility**
Domain 6: P2PE Cryptographic Key Operations Use strong cryptographic keys and secure key-management functions.	▪ All key-management functions implemented and managed by solution provider. ▪ Merchant has no involvement in key-management operations.	**6A** Use secure encryption methodologies. **6B** Use secure key-generation methodologies. **6C** Distribute cryptographic keys in a secure manner. **6D** Load cryptographic keys in a secure manner. **6E** Ensure secure usage of cryptographic keys. **6F** Ensure secure administration of cryptographic keys. **6G** Implement secure hybrid key management.	▪ P2PE Solution Provider

Domain 6 covers the use of strong cryptographic keys and secure key-management functions. Implementation of these procedures is fundamental to the security of a P2PE solution. Domain 6 includes detailed key-management procedures derived from existing industry standards for PIN key management. These procedures include criteria for managing keys and performing cryptographic operations, including encryption methodologies, key generation, key distribution, key loading, key usage, and key administration.

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 key-management operations for the encryption environment (Domain 1) and the decryption environment (Domain 5), as well as key-injection and distribution environments (Domain 6 Annexes A and 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 (for example, 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.

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 creating digital signatures or decryption operations. No one private key should be used for both purposes (except for transaction-originating SCDs).
- Public Key = asymmetric key used only for verifying digital signatures or encryption operations. No one public key should be used for both purposes (except for transaction-originating SCDs).

Appendix A provides the minimum key sizes, and equivalent key strengths, for the encryption of data and other cryptographic keys.

Domain 6 Annexes A and B contain requirements for loading and distributing keys onto devices. The solution provider will need to meet requirements in either Annex A or Annex B, or possibly both, depending on how all keys used in the solution are loaded/distributed to POI devices and Host Systems. The Domain 6 Annexes address different methods of key loading/distribution as follows:

- **Domain 6 Annex A – Symmetric-Key Distribution using Asymmetric Techniques**
  This Annex contains specific requirements pertaining to the use of symmetric-key distribution using asymmetric keys (remote key distribution) and the operation of Certification Authorities for such purposes. Entities using remote key distribution are subject both to the requirements stipulated in Domain 6 and the additional criteria stipulated in Annex A.
- **Domain 6 Annex B – Key-Injection Facilities**
  This Annex contains specific requirements pertaining to key-injection of POI devices.
  Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer or vendor.

Note: *One or both of these Annexes would always be applicable to a P2PE solution as part of Domain 6 validation.*

Domain 6 Requirements	Testing Procedures
Requirement 6A: Use secure encryption methodologies.	
Account data must be processed using cryptographic methodologies that ensure account data is kept secure.	
6A-1 Key management, cryptographic algorithms and cryptographic-key lengths must be consistent with international and/or regional standards.	
6A-1.1 Cryptographic keys must be managed in accordance with internationally recognized key-management standards (for example, ISO 11568 (all parts) or ANSI X9.24 (all parts) or equivalent).	**6A-1.1** Interview responsible personnel and examine technical documentation to verify that all keys are managed in accordance with internationally recognized key-management standards—for example, ISO 11568 (all parts) or ANSI X9.24 (all parts) or equivalent.
6A-1.1.1 Account data, cryptographic keys, and components must be encrypted using only approved encryption algorithms and key lengths, as listed in Appendix A: Minimum Key Sizes and Equivalent Key Strengths.	**6A-1.1.1.a** Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms and key lengths in accordance with Appendix A: Minimum Key Sizes and Equivalent Key Strengths.
	6A-1.1.1.b Observe key-management operations and devices to verify that all cryptographic algorithms and key lengths are in accordance with Appendix A: Minimum Key Sizes and Equivalent Key Strengths.
6A-1.1.2 Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (for example, 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 (for example, *NIST Special Publication 800-57*). *See Appendix A: Minimum Key Sizes and Equivalent Key Strengths for minimum required key lengths for commonly used algorithms.*	**6A-1.1.2.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 (for example, *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-1.1.2.b Through observation of key-management operations and inspection of SCDs, verify that crypto-periods are defined for every type of key in use.
6A-1.1.3 Ensure that any key-management requirements of the mode of operation used for encryption of account data are enforced. *For example, if a stream-cipher mode of operation is used, ensure that the same key stream cannot be re-used for different sets of data.*	**6A-1.1.3.a** For each mode of operation in use, review the applicable ISO or ANSI standard to identify any key-management requirements for that mode.
	6A-1.1.3.b Verify that all such requirements are enforced for each mode of operation

Domain 6 Requirements	Testing Procedures
6A-1.1.4 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-1.1.4.a** Verify documentation exists describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution.
	6A-1.1.4.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.

Requirement 6B: Use secure key-generation methodologies.

Cryptographic keys used for protecting account data, or for protecting other keys, are generated using secure processes.

6B-1 All keys and key components are generated using an approved random (or pseudo-random) process to ensure the integrity and security of cryptographic systems.	
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 • 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 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 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 • 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 • An approved random that has been certified by an independent qualified laboratory according to *NIST SP 800-22*

Domain 6 Requirements	Testing Procedures
	6B-1.1.c Observe device performing key-generation functions to verify that all cryptographic keys or key components are generated using the method that is approved/certified.
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, system 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 at least two authorized individuals. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device, system or medium receiving the key or key component.
	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 at least two authorized individuals. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device, system 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.	**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 monitor the key-generation processes.
6B-2.1.3 Key-generation devices must be logged off when not in use.	**6B-2.1.3.a** Examine documented procedures for all key-generation methods. Verify procedures require that key-generation devices are logged off when not in use.
	6B-2.1.3.b Observe key-generation processes and devices to verify that key-generation devices are logged off when not in use.

Domain 6 Requirements	Testing Procedures
6B-2.1.4 Key-generation equipment must not show any signs of tampering (for example, 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 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.
6B-2.1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area and observing the key-component/key-generation process.	**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 that has not been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed for key loading and are not used for any other purpose are permitted for use if all other requirements can be met. Additionally, this requirement is not intended to include in 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.*	**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 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-2.3 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 detected.	**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 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.

Domain 6 Requirements	Testing Procedures
	6B-2.3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be detected.
6B-2.4 Any residue that may contain clear-text keys or components must be destroyed immediately after generation of that key to prevent disclosure of a key or key component. *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 immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, 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, 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-2.5 Policy and procedures must ensure the following is not performed: • Dictate keys or components • Record key or component values on voicemail • Fax, e-mail, or otherwise convey clear-text keys or components • Write key or component values into startup instructions • Tape key or component values to or inside devices • Write key or component values in procedure manuals	**6B-2.5.a** Examine documented policy and procedures to verify that key components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual

Domain 6 Requirements	Testing Procedures
	6B-2.5.b From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • 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 be known by all affected parties (key custodians, supervisory staff, technical management, etc.).	**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 and verify that the documented procedures are demonstrably in use.
6B-3.2 All key-generation events must be logged. *Keys that are generated on the POI device do not need to generate an audit-log entry, but the creation of any keys to decrypt data sent from such a POI must be logged at the solution provider.*	**6B-3.2.a** Examine documented key-generation procedures to verify that all key-generation events must be 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 all events have been recorded.

Domain 6 Requirements	Testing Procedures
Requirement 6C: Distribute cryptographic keys in a secure manner.	
Cryptographic keys used for protecting account data, or for protecting other keys, are conveyed using secure processes.	
6C-1 Cryptographic keys must be conveyed or transmitted securely.	
6C-1.1 No single person can ever have access to more than one component of a particular cryptographic key. A person with access to one component/share of a key, or to the media conveying this component/share, must not have access to any other component/share of this key or to any other medium conveying any other component of this key.	**6C-1.1.a** Examine documented procedures to verify they include controls to ensure that no single person can ever have access to more than one component of a particular cryptographic key. Verify procedures include: • Any person with access to one component/share of a key must not have access to any other component/share of this key, or to any other medium conveying any other component of this key. • Any person with access to the media conveying a component/share of a key must not have access to any other component/share of this key, or to any other medium conveying any other component of this key.
	6C-1.1.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 more than one component of a particular cryptographic key. Verify the implemented controls ensure the following: • An individual with access to a key component or key share does not have access to any other component/share of this key or to any other medium conveying any other component of this key. • Any person with access to the media conveying a key component or key share must not have access to any other component/share of this key or to any other medium conveying any other component of this key.
6C-1.2 Components of cryptographic keys must be transferred using different communication channels, such as different courier services. ***Note:*** *It is not sufficient to send key components for a specific key on different days using the same communication channel.*	**6C-1.2.a** Examine documented procedures to verify that cryptographic-key components are transferred using different communications channels.
	6C-1.2.b Examine records of key transfers and interview responsible personnel to verify that cryptographic key components are transferred using different communications channels.
6C-1.3 Ensure that the method used does not allow any personnel to have access to all components—for example, key custodians, mail room and courier staff.	**6C-1.3.a** 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.

Domain 6 Requirements	Testing Procedures
	6C-1.3.b 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-1.4 Where key components are transmitted in clear-text using tamper-evident mailers, ensure that details of the serial number of the package are transmitted separately from the package itself.	**6C-1.4** If key components are ever transmitted in clear-text using tamper-evident mailers, perform the following:
	6C-1.4.a Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself.
	6C-1.4.b 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-1.5 Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of a key check value that can be verified using a separate channel • Use of public-key certificates created by a trusted CA • A hash of the public key sent by a separate channel (for example, mail or phone) • A new public-key certificate signed by an existing authenticated key ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.*	**6C-1.5** For all methods used to convey public keys, perform the following:
	6C-1.5.a Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity.
	6C-1.5.b 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.
	6C-1.5.c Verify that the mechanism used to validate the integrity and authenticity of the public key is independent of the conveyance method.
6C-2 Key components must be protected at all times during transmission, conveyance, or movement between locations.	
6C-2.1 Any single clear-text key component must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.	**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 key component must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.

Domain 6 Requirements	Testing Procedures
	6C-2.1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text key component is at all times either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.
6C-2.2 Packaging or mailers containing clear-text key components are examined for evidence of tampering before being used.	**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 used.
	6C-2.2.b Interview responsible personnel and observe process to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being used.
6C-2.2.1 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-2.2.1.a** 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-2.2.1.b Interview responsible personnel and observe process 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 No one but 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)) that are 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.

Domain 6 Requirements	Testing Procedures
6C-2.4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into tamper-evident packaging for transmittal. • Open tamper-evident packaging containing key components upon receipt. • 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 tamper-evident packaging for transmittal. • Open tamper-evident packaging containing the key component upon receipt. • 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 tamper-evident packaging for transmittal. • Open tamper-evident packaging containing the key component upon receipt. • Check the serial number of the tamper-evident packing upon receipt of a component package.
6C-3 Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.	
6C-3.1 Written procedures must exist and be known to all affected parties.	**6C-3.1.a** Verify documented procedures exist for all key transmission and conveyance processing.
	6C-3.1.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-3.2 Methods used for the conveyance or receipt of keys must be documented.	**6C-3.2** Verify documented procedures include all methods used for the conveyance or receipt of keys.

Domain 6 Requirements	Testing Procedures
Requirement 6D: Load cryptographic keys in a secure manner.	
Key loading to cryptographic devices must be handled in a secure manner, using the principles of dual control and split knowledge.	
6D-1 Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.	
6D-1.1 The loading of clear-text cryptographic keys requires dual control to authorize any key-loading session. *For example: Dual control can be implemented using two or more passwords of five characters or more, multiple cryptographic tokens (such as smartcards), or physical keys.*	**6D-1.1.a** Examine documented procedures for loading of clear-text cryptographic keys to verify they require dual control to authorize any key-loading session.
	6D-1.1.b For all types of SCDs, observe processes for loading clear-text cryptographic keys to verify that dual control is required to authorize any key-loading session.
	6D-1.1.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.
	6D-1.1.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-1.2 For loading of secret or private cryptographic keys, split knowledge is enforced by either: • Manual entry of the key as multiple key-components, using a different custodian for each component • The use of a key-loading device managed under dual control ***Note:*** *Manual key loading may involve the use of media such as paper, magnetic stripe or smart cards, or other physical tokens.*	**6D-1.2.a** Examine documented procedures for loading of secret and private cryptographic keys to verify they require split knowledge be enforced through: • Manual entry of the key as multiple-key components, using a different custodian for each component • The use of a key-loading device managed under dual control
	6D-1.2.b For all types of SCDs, observe processes for loading secret and private cryptographic keys to verify that split knowledge is enforced through: • Manual entry of the key as multiple-key components, using a different custodian for each component • The use of a key-loading device managed under dual control
6D-1.3 For any given set of key components, each device shall compose the same final key from the reverse of the process used to create the components.	**6D-1.3** 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, and that this is the reverse of the process used to create the key components.

Domain 6 Requirements	Testing Procedures
6D-1.4 If key-establishment protocols using public-key cryptography are used to distribute secret keys, these must meet the requirements detailed in Annex A of this document.	**6D-1.4** If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that the requirements detailed in Annex A of this document are met.
6D-1.5 If keys are injected into a POI either by the solution provider or a third-party key-injection facility (KIF), these must also meet the additional requirements set out in Annex B of this document.	**6D-1.5** If POI keys are injected in a key-injection facility (KIF), verify that the KIF also meets the additional requirements set out in Annex B of this document.
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 a cryptographic device only when it can be ensured that: • Any cameras in the environment are positioned to ensure they cannot monitor the entering of clear-text key components. • There is no unauthorized mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. • The device has not been subject to any prior tampering that could lead to the disclosure of keys or account data.	**6D-2.1** Observe key-loading environments, processes, and mechanisms (for example, terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: **6D-2.1.a** Ensure cameras are positioned to ensure they cannot monitor the entering of clear-text key components. **6D-2.1.b** Verify that keys and components are transferred into a cryptographic device only after an inspection of the devices and mechanism ensures: • There is no unauthorized mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. • The device has not been subject to any prior tampering that could lead to the disclosure of keys or account data.
6D-2.2 The injection of secret or private key components from 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-insertion of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.	**6D-2.2.a** Examine documented procedures for the injection of secret or private key components from electronic medium to a cryptographic device. Verify 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-insertion of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.

Domain 6 Requirements	Testing Procedures
	6D-2.2.b Observe key-injection 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-insertion 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 For electronic key-loading devices used to inject keys into POIs, the following must be in place:	**6D-2.3** Review documented procedures and observe processes for the use of key-loading devices. Perform the following:
6D-2.3.1 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-2.3.1** 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-2.3.2 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-2.3.2** 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-2.3.3 The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.	**6D-2.3.3.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-2.3.3.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.
6D-2.3.4 The key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred.	**6D-2.3.4** Verify the key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred.
6D-2.4 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).	**6D-2.4.a** Inspect all media (electronic or otherwise) containing key components used in the loading of cryptographic keys to verify that any such media is maintained in a secure location.
	6D-2.4.b Interview personnel and observe media locations to verify that the media is accessible only to custodian(s) authorized to access the key components.

Domain 6 Requirements	Testing Procedures
6D-2.5 When removed from secure storage, 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. *Key components that can be read/displayed (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are visible only at one point in time to only one designated key custodian.*	**6D-2.5.a** Examine documented procedures for removing media or devices containing key components, or that are otherwise used for the injection of cryptographic keys, from secure storage. 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.b 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.c 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 Written or printed key component must not be opened until immediately prior to use.	**6D-2.6.a** Review documented procedures and confirm that printed/written key components are not opened until immediately prior to use.
	6D-2.6.b Observe key-loading processes and verify that printed/written key components are not opened until immediately prior to use.

Domain 6 Requirements	Testing Procedures
6D-3 All hardware and access/authentication mechanisms used for key loading or the signing of authenticated applications (for example, 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. ***Note:*** *Where key-loading is performed for POIs, the secure environment is defined in Annex B.*	**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 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.
	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 passwords used for key-loading functions and for the signing of authenticated applications are controlled and maintained in a secure environment under dual control.
6D-3.1.1 Dual-control practices must be specified in emergency procedures and in place during emergency situations. ***Note:*** *Emergency procedures may include but are not limited to incident-response and disaster-recovery procedures.*	**6D-3.1.1.a** Examine documented emergency procedures to verify dual-control practices are specified in emergency procedures.
	6D-3.1.1.b Interview responsible personnel to verify that dual-control practices are maintained during emergency situations.
6D-3.1.2 Default dual-control mechanisms must be changed.	**6D-3.1.2.a** Verify that documented procedures require default dual-control mechanisms be changed.
	6D-3.1.2.b Interview personnel and observe dual-control mechanisms for key-loading functions to verify there are no default dual-control mechanisms (for example, default passwords) used for key loading or the signing of authenticated applications.
6D-3.2 All cable attachments must be examined before each key-loading or 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 function or signing operation.
	6D-3.2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to a key-loading function or signing operation.

Domain 6 Requirements	Testing Procedures
6D-3.3 Any physical tokens used to enable key loading or the signing of authenticated applications—for example, physical (brass) keys, or smartcards—must not be in the control or possession of any one individual who could use those tokens to load secret cryptographic keys or sign applications under single control.	**6D-3.3.a** Examine documented procedures for the use of physical tokens 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.
	6D-3.3.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.
6D-3.4 Use of the equipment must be monitored and a log of all key-loading and application-signing activities maintained for audit purposes.	**6D-3.4.a** Observe key-loading and application-signing activities to verify that use of the equipment is monitored.
	6D-3.4.b Verify logs of all key-loading and application-signing activities are maintained.
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 is in place to ensure the authenticity and integrity of keys and components (for example, testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded).	**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 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.
6D-4.1.1 Methods used for key validation are consistent with ISO 11568 and prevent exposure of the actual key values.	**6D-4.1.1.a** Verify that the methods used for key validation are consistent with ISO 11568 (for example, if check values are used, they should return a value of no more than 4-6 hexadecimal characters).
	6D-4.1.1.b Verify that the implemented methods prevent exposure of the actual key values.

Domain 6 Requirements	Testing Procedures

6D-4.2 Public keys must only be stored in the following approved forms:
• Within a certificate,
• Within a secure cryptographic device,
• Encrypted using strong cryptography, or
• Authenticated with strong cryptography using one of the following methods:
  ○ ISO16608-2004 compliant MAC
  ○ NIST SP800-38B CMAC
  ○ PKCS #7 compliant public-key signature
	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-4.2.1 Procedures exist to ensure the integrity and authenticity of public keys prior to storage (for example, during transmission as part of a certificate request operation).	**6D-4.2.1.a** Interview personnel and review documentation to verify that procedures exist to ensure the integrity and authenticity of public keys prior to storage.
	6D-4.2.1.b Observe public-key transmissions and processes to verify the implemented procedures ensure the integrity and authenticity of public keys prior to storage.
6D-5 Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.	
6D-5.1 Procedures must be documented for all key-loading operations, be known to all affected parties and demonstrably be in use.	**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 and verify that the documented procedures are demonstrably in use.
6D-5.2 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.

Domain 6 Requirements	Testing Procedures
Requirement 6E: Ensure secure usage of cryptographic keys.	
Keys must be used in a manner that prevents or detects their unauthorized usage.	
6E-1 Unique secret cryptographic keys must be in use for each identifiable link between encryption and decryption points.	
6E-1.1 Where two organizations share a key for securing account data (including a key-encryption key used to encrypt a data-encryption key), that key must meet the following: • Be unique to those two entities and • Not be given to, or used by, any other entity.	**6E-1.1.a** Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations. For all keys shared between two organizations (including data-encryption keys for account data, and key-encryption keys used to encrypt a data-encryption key) perform the following:
	6E-1.1.b Obtain key check values for any master file keys to verify key uniqueness between the two organizations. 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.c For internally developed systems, review system-design documentation or source code for uniqueness of cryptograms and/or hash values/fingerprints and/or public keys.
	6E-1.1.d For application packages, examine parameter files where the cryptograms of keys shared with other network nodes are specified. If a remote key-establishment and distribution scheme is implemented between networks, examine the parameter files where the public keys of keys shared with other network nodes are specified and ensure the correct number of public keys exist (a unique one for each network link implemented).
	6E-1.1.e Compare key check values against those for known or default keys to verify that known or default key values are not used.
6E-1.2 Key-generation keys (such as a base derivation key) that are used to derive multiple keys for different devices must never be output from a secure cryptographic device in clear text.	**6E-1.2.a** Examine documented procedures to confirm that key-generation keys (such as a base derivation key), that are used to derive multiple keys for different devices, are never output from a secure cryptographic device in clear text.

Domain 6 Requirements	Testing Procedures
	6E-1.2.b Observe the process for managing key-generation keys (such as a base derivation key), that are used to derive multiple keys for different devices, to ensure they are never output from a secure cryptographic device in clear text.
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 The unauthorized replacement or substitution of one stored key for another or the replacement or substitution of any portion of a key, whether encrypted or unencrypted, must be prevented or detected.	**6E-2.1** Examine documented procedures and technical documentation to confirm that procedures exist to prevent or detect • The unauthorized replacement or substitution of any stored key for another • The replacement or substitution of any portion of a key, whether encrypted or unencrypted
6E-2.1.1 TDEA cryptographic keys must be managed as key bundles (for example, using ANSI TR-31) at all times when external to an SCD. Management of key bundles and the individual keys must include: • Assurance of key integrity • Appropriate usage as specified by the particular mode • Preventing manipulation of individual keys • Keys cannot be unbundled for any purpose	**6E-2.1.1.a** Examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key bundles at all times.
	6E-2.1.1.b Verify that key bundles and the individual keys are managed as follows: • Key integrity ensures that each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source. • Keys are used in the appropriate order as specified by the particular mode. • Key bundles are a "fixed quantity," such that an individual key cannot be manipulated while leaving the other two keys unchanged; and • Key bundles cannot be unbundled for any purpose.

Domain 6 Requirements	Testing Procedures
6E-2.2 Documented procedures must exist and be demonstrably in use describing how the replacement and/or substitution of one key for another is prevented. These procedures must specifically include the following:	**6E-2.2** Verify documented procedures exist defining how the replacement and/or substitution of one key for another is prevented, including 6E-2.2.1 through 6E-2.2.4, below. Perform the following:
6E-2.2.1 HSMs (including CA's HSMs) must not remain in a "sensitive" state when connected to online production systems. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	**6E-2.2.1.a** Examine HSMs to ensure they do not remain in a "sensitive" state when connected to online production systems.
	6E-2.2.1.b If a CA is used, examine the CA's HSMs and observe CA process to ensure that HSMs do not remain in the "sensitive" state when connected to online production systems.
6E-2.2.2 Keys no longer needed are destroyed.	**6E-2.2.2** Verify that keys no longer needed are destroyed.
6E-2.2.3 Procedures for monitoring and alerting to the presence of multiple cryptographic synchronization errors, including the following: • 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.	**6E-2.2.3.a** Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.
	6E-2.2.3.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.
6E-2.2.4 Physical and logical controls exist over the access to and use of SCDs used to create cryptograms to prevent misuse	**6E-2.2.4.a** Verify physical controls exist over the access to and use of devices used to create cryptograms.
	6E-2.2.4.b Verify logical controls exist over the access to and use of devices used to create cryptograms.

Domain 6 Requirements	Testing Procedures
6E-2.3 Key-component documents and their packaging that show 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-2.3.a** Verify procedures are documented for the following: • Key-component documents 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. • Key-component packaging 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-2.3.b Interview personnel and observe processes to verify procedures are implemented as follows: • Key-component documents 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. • Key-component packaging showing signs of tampering results in the destruction 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 To limit the magnitude of exposure should any key(s) be compromised, and to significantly strengthen the security of the underlying system, the device must enforce the following practices:	
6E-3.1.1 Cryptographic keys must only be used for the purpose they were intended—for example, key-encryption keys must not be used as data-encryption keys, PIN keys must not be used for account-data encryption, and these keys must not be used to encrypt any arbitrary data (data that is not account data).	**6E-3.1.1.a** Examine key-management documentation and interview key custodians to verify that cryptographic keys are defined for a specific purpose.
	6E-3.1.1.b Observe cryptographic devices and key-management processes to verify that cryptographic keys are used only for the defined purpose for which they were intended.
6E-3.1.2 Master keys (and any variants or keys derived from master keys) used by host processing systems for encipherment of keys for local storage are not used for other purposes—for example, key conveyance between platforms that are not part of the same logical configuration.	**6E-3.1.2** Observe cryptographic devices and key-management processes to verify that master keys—and any variants or keys derived from master keys—used for encipherment of keys for local storage are not used for other purposes.

Domain 6 Requirements	Testing Procedures
6E-3.1.3 Account data keys, key-encipherment keys, and PIN-encryption keys have different values. *Ensuring key purpose is an essential part of key management, and compromise of key purpose can render even strong cryptography invalid. Review of HSM commands used to access keys for decryption of data will often show if keys are being misused; for example, where a key that is designed for account-data encryption is used to decrypt other data as well.*	**6E-3.1.3.a** Examine key-management documentation and interview key custodians to verify that account data keys, key-encipherment keys, and PIN-encryption keys must have different values.
	6E-3.1.3.b Observe key-generation processes and a sample of key check values to verify that account data keys, key-encipherment keys, and PIN-encryption keys must have different values.
6E-3.2 To limit the magnitude of exposure should any key(s) be compromised and to significantly strengthen the security of the underlying system, the following practices must be enforced for private/public keys:	
6E-3.2.1 Private keys must only be 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 (except for transaction-originating SCDs).	**6E-3.2.1** Examine key-management documentation and interview key custodians 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.
6E-3.2.2 Public keys must only be used as follows: • 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 transaction-originating devices).	**6E-3.2.2** Examine key-management documentation and interview key custodians 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.
6E-3.3 Keys must never be shared or substituted between production and test systems. • Production keys must never be present or used in a test system, and • Test keys must never be present or used in a production system.	**6E-3.3.a** Examine key-management documentation and interview key custodians to verify that cryptographic keys are never shared or substituted between production and development systems.
	6E-3.3.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-3.3.c Observe processes for generating and loading keys into in test systems to ensure that they are in no way associated with production keys.
	6E-3.3.d Compare check, hash, cryptogram, or fingerprint values for production and development keys to verify that development and test keys have different key values.

Domain 6 Requirements	Testing Procedures
6E-4 All secret and private keys must be unique (except by chance) to that device.	
6E-4.1 All cryptographic keys that have ever been used in a transaction-originating POI device to encrypt account data or to protect account-data keys through encryption, must be: • Known only to a single POI device, and • Known only to HSMs and Host System(s) in the solution provider's decryption environment for that POI device, 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.* *The requirement for unique private and secret keys includes all keys that are used to secure account data or to provide security to account-data keys. This includes not only the account-data keys themselves, but also any KEKs, master keys, or any secret and private keys used to sign firmware updates or for other device-management operations.*	**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 keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to one or more HSMs and Host System(s) in the solution provider's decryption environment for that POI device, at the minimum number of facilities consistent with effective system operations.
	6E-4.1.b Observe HSM functions and procedures for generating and loading 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, hash, or fingerprint values for a sample of cryptographic keys from different POI devices to verify keys are unique for each POI device.
	6E-4.1.d Compare all POI public keys, if used, across all decryption points as well as for every POI connection, to ensure there are no duplicates across POI devices.
	6E-4.1.e Compare the number of POI devices in use to the number of cryptographic keys in use to verify that an individual key is defined for each device. (Having fewer keys than devices would indicate that the same key is being used for several devices.)
	6E-4.1.f Examine cryptograms of keys used between the POI and its decryption point and compare to cryptograms used in other decryption points to verify that the key exists at the minimum number of facilities consistent with effective system operations.
6E-4.2 These unique keys, or set of keys, must be totally independent and produced using an irreversible process	**6E-4.2.a** Examine documented procedures for generating all types of keys and verify the procedures ensure: • That unique keys, or sets of keys, must be totally independent. • That unique keys, or sets of keys, are produced using an irreversible process.

Domain 6 Requirements	Testing Procedures
	6E-4.2.b Interview personnel and observe key-generation processes to verify that keys are generated independently of other keys of the same type.
	6E-4.2.c Interview personnel and observe key-generation processes to verify that variants of one key are not used across multiple POI devices, or multiple decryption end points.
6E-4.3 Emergency procedures must support requirements for unique device keys and not circumvent uniqueness controls.	**6E-4.3.a** Examine documented emergency procedures and very they: • Support requirements for unique device keys. • Do not circumvent uniqueness controls.
	6E-4.3.b Interview responsible personnel to verify: • Requirements for unique device keys are maintained during emergency situations. • Uniqueness controls are not circumvented during emergency situations.
6E-4.4 Where master keys are generated by a derivation process and derived from the same base derivation key, ensure the following: • Unique data must be used for the derivation process such that all transaction-originating SCDs receive unique secret keys. • Key derivation must be performed prior to a key being loaded/sent to the recipient transaction-originating POI. *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.*	**6E-4.4.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 SCDs receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.
	6E-4.4.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.

Domain 6 Requirements	Testing Procedures
Requirement 6F: Ensure secure administration of cryptographic keys.	
Keys must be administered in a secure manner.	
6F-1 Secret keys used for encrypting 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 a secure cryptographic device, except for the following conditions: • When encrypted or managed using the principles of dual control and split knowledge. • Clear-text data-decryption keys (DDKs) may temporarily be retained by the Host System in volatile memory for the purpose of decrypting account data. (See Requirement 5E-1 for additional requirements for DDKs)	
6F-1.1 All secret or private keys, with the exception of DDKs used on the Host System (see Note), must only exist in one or more of the following forms at all times—including during generation, transmission, storage, and use: • At least two separate key shares or full-length components • Encrypted with a key of equal or greater strength • Contained within a secure cryptographic device ***Note:*** *Clear-text data-decryption keys (DDKs) may temporarily be retained by the Host System in volatile memory whilst being used to decrypt account data.*	**6F-1.1.a** Examine documented key-generation procedures and observe key-generation processes to verify that secret or private keys only exist in one or more approved forms at all times during key generation.
	6F-1.1.b Examine documented procedures for transmission of keys and observe key-transmission processes to verify that secret or private keys only exist in one or more approved forms at all times during transmission.
	6F-1.1.c Examine documented procedures for key storage and observe key stores to verify that all secret or private keys, with the exception of DDKs used on the Host System, only exist in one or more approved forms at all times when stored.
	6F-1.1.d Examine documented key-usage procedures and observe operational processes to verify that all secret or private keys, with the exception of DDKs used on the Host System, only exist in one or more approved forms at all times during use.
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:

Domain 6 Requirements	Testing Procedures
6F-1.2.1 Knowledge of any one key component 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.	**6F-1.2.2** Observe processes for constructing cryptographic keys to verify that at least two key components are required for each key construction.
6F-1.2.3 Each key component has one or more specified custodians.	**6F-1.2.3.a** Examine documented procedures for the use of key components and interview key custodians 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 that component.
6F-1.2.4 Procedures exist to ensure any custodian never has access to sufficient key components to reconstruct a cryptographic key. *For example, in an* m-of-n *scheme, where only two of any three components are required to reconstruct the cryptographic key, a custodian cannot have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian cannot 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 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 (for example, 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 to reconstruct a 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 to reconstruct a cryptographic key.

Domain 6 Requirements	Testing Procedures
6F-1.2.5 Key components must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components. (For example, via XOR'ing.) *Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two eight-hexadecimal character halves to form a sixteen-hexadecimal secret key.* The resulting key must only exist within the SCD.	**6F-1.2.5.a** Examine documented procedures for combining 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.
	6F-1.2.5.b Examine key-component lengths for a key generated with those components to verify that key components are not concatenated to form the 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 follows:
6F-1.3.1 Key components that exist in clear text outside of an SCD must be sealed in opaque, tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging. ***Note:*** *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, 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 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).

Domain 6 Requirements	Testing Procedures
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 are not sufficient to meet this requirement (for example, desk drawers).* *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 a PIN or similar 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 corresponding PIN.	**6F-1.3.3** If a key component is stored on a token, and a PIN or similar mechanism is used to access the token, verify that only that token's owner—or designated backup(s)—has possession of both the token and its corresponding PIN.
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, and include 6F-2.1.1 through 6F-2.1.9 below.
6F-2.1.1 Key components are never reloaded when there is any suspicion that either the originally loaded key, the SCD or 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 the originally loaded key, the SCD or the Host System has been compromised.
6F-2.1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD or 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 Host System has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.

Domain 6 Requirements	Testing Procedures
6F-2.1.3 If compromise of the cryptographic key is suspected, processing with that key is halted, and the key is replaced with a new unique key. This process includes any systems, devices, or processing that involves subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.	**6F-2.1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, 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.
6F-2.1.4 For each key in the solution provider's key suite, including any subordinate keys that are generated, protected, or transported under other keys, the purpose of that key is listed.	**6F-2.1.4** Interview responsible personnel and observe documented key lists to verify the purpose of each key is listed, for all keys used by the solution provider.
6F-2.1.5 The names and/or functions of each staff member assigned to the recovery effort, as well as phone numbers and the place where the team is to assemble, are defined.	**6F-2.1.5** Interview responsible personnel and observe documentation to verify he following are defined: • The names and/or functions of each staff member assigned to the recovery effort • Contact phone numbers for staff members assigned to the recovery effort • A designated place where the recovery team is to assemble
6F-2.1.6 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • A damage assessment • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	**6F-2.1.6.a** Interview responsible personnel and observe implemented processes to verify the escalation process includes notification to organizations that currently share or have previously shared the key(s). **6F-2.1.6.b** Verify notifications include the following: • A damage assessment • Details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.

Domain 6 Requirements	Testing Procedures
6F-2.1.7 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: • Missing SCDs • Host System tamper-detection mechanism has been activated • Tamper-evident seals or package numbers or dates and times not agreeing with log entries • Tamper-evident seals or packages that have been opened without authorization or show signs of attempts to open or penetrate	**6F-2.1.7** Interview responsible personnel and observe implemented processes to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • Host System tamper-detection mechanism has been activated • Tamper-evident seals or package numbers or dates and times not agreeing with log entries • Tamper-evident seals or packages that have been opened without authorization or show signs of attempts to open or penetrate
6F-2.1.8 Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.	**6F-2.1.8** Interview responsible personnel and observe implemented processes to verify procedures address indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.
6F-2.1.9 If attempts to load a secret key or key component into an SCD or the Host System 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 SCD or host system.	**6F-2.1.9** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an SCD or Host System 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 SCD or host system.
6F-3 Keys generated using reversible key-calculation methods, such as key variants, must only be used in devices 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 cannot be used as a working key or as a master file key for local storage. *Key generation that uses a non-reversible process, such as key derivation with a base key using an encipherment process, is 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.	**6F-3.1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.

Domain 6 Requirements	Testing Procedures
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.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-3.1.1 Reversible transformations of a key must not be exposed outside of the secure cryptographic device that generated those transforms.	**6F-3.1.1** Verify that reversible transformations of keys are not exposed outside of the secure cryptographic device that generated those transforms.
6F-3.2 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate data-encryption keys from master keys, or from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or different data-encryption keys from an initial data-encryption key. *Using transforms of keys across different levels of a key hierarchy—for example, generating an account-data 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-3.2** 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: • Master keys must only be generated from or be used to generate other master keys. • Key-encrypting keys must only be generated from or be used to generate other key-encrypting keys. • Data-encryption keys must only be generated from or be used to generate other data-encryption keys. • Any other type of key must only be generated from or be used to generate other keys of the same type.
6F-4 Secret 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, or 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, or key components that are no longer used or that have been replaced by a new key.

Domain 6 Requirements	Testing Procedures
	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-4.2 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.	**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 (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 any keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.
	6F-4.2.1.b Observe key-destruction processes to verify that any keys (including components or shares) maintained on paper is burned, pulped, or shredded in a crosscut shredder.
6F-4.2.2 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-4.2.2.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-4.2.2.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-4.2.3 The key-destruction process must be observed by a third party other than the custodian.	**6F-4.2.3** Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian.
6F-4.2.4 The third-party witness must sign an affidavit of destruction. ***Note:*** *For keys on paper, consider having the affidavit of destruction as a part of the same piece of paper that contains the key-component value itself. To destroy the key, tear off the section of the sheet that contains the value, destroy it, sign and witness the affidavit and log it. Affidavits of destruction can also be digitally signed if considered legally acceptable in the locale.*	**6F-4.2.4** 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.

Domain 6 Requirements	Testing Procedures
6F-4.3 Any residues of key-encryption keys used for the conveyance of working keys (such as components used to create the key) must be destroyed after successful loading and validation as being operational.	**6F-4.3.a** Verify documented procedures exist for destroying any residues of key-encryption keys used for the conveyance of working keys, once the working keys are successfully loaded and validated as operational.
	6F-4.3.b Observe key-conveyance/loading processes to verify that any residues of key-encryption keys used for the conveyance of working keys are destroyed, once the working keys are successfully loaded and validated as operational.
6F-5 Access to material which can be used to construct secret and private keys (such as key components) 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 as follows:	**6F-5.1** Interview key custodians and observe implemented processes to verify the following:
6F-5.1.1 Designate a primary and a backup key custodian for each component, such that the fewest number of key custodians are assigned as necessary to enable effective key management.	**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.
6F-5.1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form in some legally binding way.	**6F-5.1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form in some legally binding way.
	6F-5.1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form in some legally binding way.

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 • 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 • An effective date and time for the custodian's access • Signature of management authorizing the access.
6F-5.1.4 Key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual. For example, for a key managed as three components, at least two custodians report to different individuals. In an *m-of-n* scheme, such as *three of five* key shares, no more than two key custodians can report to the same individual. In all cases, neither the direct reports nor the direct reports in combination with their immediate supervisor (if they are a key custodian) shall possess the necessary threshold of key components sufficient to form any given key.	**6F-5.1.4** 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-6 Logs are kept for any time that keys, key components, or related materials are removed from secure 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.	**6F-6.1** 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-6.2 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-6.2** 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)

Domain 6 Requirements	Testing Procedures
6F-7 Backup copies 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:*** *Clear-text cryptographic keys used on the Host System must not be included in any system backup. (Refer to Requirement 5E-1.14)*	
6F-7.1 The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as operational keys in line with all requirements specified in this document.	**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 Verify that any backup copies of secret and private keys exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible.
	6F-7.1.b Inspect backup storage locations and access controls to verify 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) 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. *It is not a requirement to have backup copies of key components or keys, but it is acceptable to maintain such backup copies for the purposes of business continuity if they are secured and maintained in approved forms.*	**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-7.3 If backup copies of secret and/or private keys exist, confirm that they are maintained in one of the approved forms noted in Requirement 6F-1.1 and are managed under dual control and split knowledge.	**6F-7.3** Interview responsible personnel and observe backup processes to verify the following • Backup copies of secret and/or private keys are maintained in one of the approved forms identified Requirement 6F-1.1 • Backup copies of secret and/or private keys are managed under dual control and split knowledge.

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 be in place and all affected parties must be aware of those procedures, as follows: • All aspects of and activities related to key administration must be documented, including: ○ A defined cryptographic-key change policy for each key layer defined in the key hierarchy (this applies to both symmetric and asymmetric-key types) ○ Security-awareness training ○ Role definition—nominated individual with overall responsibility ○ Background checks for personnel ○ 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: • A defined cryptographic-key change policy for each key layer defined in the key hierarchy • Security-awareness training • Role definition—nominated individual with overall responsibility • Background checks for personnel • 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 personnel to verify background checks are performed.

Domain 6 Requirements	Testing Procedures
Requirement 6G: Implement secure hybrid key management	
6G-1 Data-Decryption Key Usage	
6G-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 (for example 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.	**6G-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 (for example 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.
	6G-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.
6G-1.2 DDKs must be erased from the Host System volatile memory via a mechanism that ensures the key cannot be recovered or reconstructed.	**6G-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.
	6G-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.

Domain 6 Requirements	Testing Procedures
6G-1.3 If the DDK is generated from a master key, then 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.	**6G-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.
	6G-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.
6G-1.4 The DDK must be encrypted between the HSM and the Host System, for example using a fixed transport key or a cryptographic protocol such as TLS/SSL. The method of encryption used must maintain the security policy to which the HSM was approved (either FIPS140-2, Level 3 or higher, or the PCI PTS HSM standard).	**6G-1.4.a** Examine key-management policies and procedures to verify that DDKs must be encrypted between the HSM and the Host System.
	6G-1.4.b Examine HSM and Host System configurations to verify that DDKs are encrypted between the HSM and the Host System.
	6G-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.
6G-1.5 The encryption mechanism used to protect the DDK between the HSM and the Host System must meet the following:	**6G-1.5** Verify the encryption mechanism used to protect the DDK between the HSM and the Host System, includes 6G-1.5.1 through 6G-1.5.2 Perform the following:
6G-1.5.1 The encryption key must be of equal or greater strength than the key it protects.	**6G-1.5.1.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is of equal or greater strength than the key it protects.
	6G-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 of equal or greater strength than the key it protects.

Domain 6 Requirements	Testing Procedures
6G-1.5.2 The encryption key must be unique for each Host System.	**6G-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.
	6G-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.
6G-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.	**6G-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.
	6G-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.
6G-1.5.4 The encryption key must have a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices	**6G-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
	6G-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

Domain 6 Annex A: Cryptographic Key Operations – Symmetric-Key Distribution using Asymmetric Techniques

This annex contains requirements that apply to remote key establishment and distribution.

Asymmetric remote key-distribution schemes should be used for initial key loading only—for example, the establishment of a TDES or AES key hierarchy, such as a terminal master key. Standard symmetric-key-exchange mechanisms should be used for subsequent symmetric-key exchanges, except where a device requires a new key initialization due to unforeseen loss of the existing terminal master key.

These requirements pertain to two distinct areas.

1. Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key-distribution using asymmetric techniques.
2. 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 solution providers and their associated entities 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 to enforce the integrity and authenticity of a block of data through the encryption of a whole or digest 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 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 or CMACs).

Requirements that apply only to entities operating as Certification and/or Registration Authorities are indicated with **CA/RA.** All other requirements in this annex apply to entities involved in symmetric-key distribution using asymmetric techniques.

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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
Compromise must not be possible without collusion.	
RD-1 Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals. *(Reference 6B-2)*	
RD-1.1 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 (for example, secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.	**RD-1.1.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
	RD-1.1.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 (for example, zeroized) immediately after the transfer to the device that will use the key pair.
Cryptographic keys must be conveyed or transmitted securely.	
RD-2 Cryptographic keys must be conveyed or transmitted securely. (*Reference 6C-1)*	
RD-2.1 All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed	**RD-2.1.a** 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.
	RD-2.1.b 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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
Authenticity of keys must be validated.	
RD-3 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. *(Reference 6D)*	
RD-3.1 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.*	**RD-3.1.a** Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: • SCDs 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.
	RD-3.1.b Observe key-loading processes to verify that mutual authentication of the sending and receiving devices is performed, as follows: • SCDs 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.
RD-3.2 Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange or key establishment with POIs. ***Note:*** *An example of this kind of mechanism is through limiting communication between the transaction-originating POI and KDH to only those KDHs contained in a list of valid KDHs managed by the POI.*	**RD-3.2.a** Examine documented procedures to confirm they define mechanisms to prevent an unauthorized KDH from performing key transport, key exchange, or key establishment with POIs.
	RD-3.2.b Observe mechanisms in use to verify they prevent an unauthorized KDH from performing key transport, key exchange, or key establishment with POIs.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-3.3 Key establishment and distribution procedures must be designed such that: • Within an implementation design, there shall be no means available for "man in middle" attacks. • System implementations must be designed and implemented to prevent replay attacks.	**RD-3.3.a** 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 middle" attacks. • System implementations are designed to prevent replay attacks.
	RD-3.3.b Observe key-exchange and establishment operations to verify that system implementations are implemented such that: • There are no means available for "man in middle" attacks. • System implementations prevent replay attacks.
RD-3.4 Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device: that is, the secrecy of private keys and the integrity of public keys must be ensured.	**RD-3.4** If key pairs are generated external to the device that uses the key pair, perform the following:
	RD-3.4.a 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.
	RD-3.4.b Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured.
RD-3.5 Once asymmetric keys are loaded for a specific P2PE solution provider, changing of those keys must not be permitted without the authorization of that solution provider.	**RD-3.5.a** Examine documentation to verify that procedures are defined to ensure that, once asymmetric keys are loaded, changing of those keys is not permitted without authorization of that P2PE solution provider.
	RD-3.5.b Interview responsible personnel and observe records of the authorization process to verify that once asymmetric keys have been loaded, authorization from the P2PE solution provider is obtained before those keys are changed.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
Procedures must prevent or detect unauthorized key substitution.	
RD-4 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. *(Reference 6E-2)*	
RD-4.1 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.	**RD-4.1.a** Examine documented procedures to verify that: • POIs are only required to 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 are only required to communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.
	RD-4.1.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 for key management, normal transaction processing, and certificate (entity) status checking.
RD-4.2 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.	**RD-4.2.a** Examine documented procedures to verify that: • KDHs are only required to communicate with POIs for the purpose of key management and normal transaction processing; • KDHs are only required to communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.
	RD-4.2.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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
Keys must be used only for their intended purpose and may never be shared between systems.	
RD-5 Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems. *(Reference 6E-3)*	
RD-5.1. Only one certificate shall be issued per key pair. Key pairs shall not be reused for certificate renewal or replacement.	**RD-5.1.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 renewal request • Certificate replacement request
	RD-5.1.b Interview responsible personnel and observe certificate issuing, renewal, and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Expired certificates are renewed by generating a new key pair and requesting a new certificate. • Certificates are replaced by generating a new key pair and requesting a new certificate.
RD-5.2 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 (as required in Requirement RD-9.3). See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.	**RD-5.2.a** Examine certificate policy and key-usage procedures and verify that documented key-usage procedures are defined in accordance with the certificate policy.
	RD-5.2.b Verify that mechanisms are defined that preclude the use of a key for other than its designated and intended purpose.
	RD-5.2.c Observe key-usage processes to verify that mechanisms are in use that preclude the use of a key for other than its designated and intended purpose.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-5.2.1 CA/RA: CA certificate signature keys, certificate (entity) status checking (for example, Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorized host lists in encryption devices cannot 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.*	**RD-5.2.1.a** Examine certificate policy and documented procedures to verify that: • Certificate signature keys, • Certificate status checking (for example, 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
	RD-5.2.1.b Interview responsible personnel and observe key-usage processes to verify that: • Certificate signature keys, • Status checking (for example, 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
RD-5.2.2 CAs that issue certificates to other CAs cannot be used to issue certificates to POIs.	**RD-5.2.2** if a CA issues certificates to POIs, examine CA certificate policy and documented procedures to verify that the CA does not issue certificates to other CAs.
RD-5.3 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.*	**RD-5.3.a** 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.
	RD-5.3.b Observe the mechanisms in use to verify that they restrict and control the use of public and private keys.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-5.4 CA/RA: CA private keys cannot be shared between devices except for load balancing and disaster recovery.	**RD-5.4.a** 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.
	RD-5.4.b Examine cryptograms of the private keys on CA systems and/or observe records of key-management operations to verify that CA private keys are not shared between devices, except for load balancing and disaster recovery.
RD-5.5 KDH private keys cannot be shared between devices except for load balancing and disaster recovery.	**RD-5.5.a** Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.
	RD-5.5.b Examine cryptograms of the private keys and/or observe records of key-management operations to verify that KDH private keys are not shared between devices, except for load balancing and disaster recovery.
RD-5.6 POI private keys cannot be shared.	**RD-5.6.a** Examine documented processes to verify that POI private keys are not permitted to be shared between devices.
	RD-5.6.b Inspect public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI.
All secret and private keys must be unique to their devices.	
RD-6 All secret and private keys must be unique (except by chance) to a POI device. *(Reference 6E-4)*	
RD-6.1 Keys in all hosts and POIs must be uniquely identifiable via cryptographically verifiable means (for example, through the use of digital signatures, "fingerprints," or key check values). The method used must not expose any part of the actual key value.	**RD-6.1.a** Examine documented procedures to verify that a cryptographic method is defined which: • Uniquely identifies private keys stored within all hosts and POIs. • Does not expose any part of the actual key value.
	RD-6.1.b Examine a sample of hosts and POIs to verify the method used: • Uniquely identifies the private keys stored within all hosts and POIs. • Does not expose any part of the actual key value.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-6.2 Private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the following forms: • At least two separate key shares or full-length components; • Encrypted using an algorithm and key size of equivalent or greater strength; or • Within an SCD (for example, an HSM or POI) approved to FIPS140-2 Level 3, PCI HSM, or PCI PTS.	**RD-6.2.a** Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the approved forms at all times.
	RD-6.2.b Observe key-management operations and interview key custodians to verify that private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the approved forms at all times.
Keys Known or suspected to be compromised must be replaced.	
RD-7 Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) with a value not feasibly related to the original key. *(Reference 6F-2)*	
RD-7.1 Solution provider must provide for continuity of service in the event of the loss of a root key (for example, through compromise or expiration). *For example, a key-distribution management system and the associated end entities (KDHs, encryption devices) could provide support for more than one root.*	**RD-7.1.a** Examine documented key-management procedures to verify the solution provider provides for continuity of service in the event of the loss of a root key.
	RD-7.1.b Observe key-management operations and interview key custodians to verify the solution provider provides for continuity of service in the event of the loss of a root key.
RD-7.2 CA/RA: Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.	**RD-7.2** Through the examination of documented procedures, interviews and observation confirm that Root CAs provide for segmentation of risk to address key compromise.
RD-7.3 CA/RA: Mechanisms must be in place to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke subordinate certificates and notify affected entities.	**RD-7.3.a** Examine documented procedures to verify that mechanisms are defined to address compromise of a CA. Verify the mechanisms include procedures to: • Revoke subordinate certificates, and • Notify affected entities.
	RD-7.3.b Interview responsible personnel to verify that the defined mechanisms to address compromise of a CA are in place and include: • Revoking subordinate certificates, and • Notifying affected entities.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-7.3.1 CA/RA: If a compromise is known or suspected, the CA must cease issuance of certificates and perform a damage assessment, including a documented analysis of how and why the event occurred. • The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. • The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.	**RD-7.3.1.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. • The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. • The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.
	RD-7.3.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: • The CA ceases issuance of certificates. • The CA performs a damage assessment, including a documented analysis of how and why the event occurred. • The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. • The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.
RD-7.3.2 In the event of the issuance of fraudulent certificates with the compromised key, the CA should determine whether to recall and reissue all signed certificates with a newly generated signing key.	**RD-7.3.2.a** Examine documented procedures to verify that in the event of the issuance of fraudulent certificates with the compromised key, procedures are defined for the CA to determine whether to recall and reissue all signed certificates with a newly generated signing key.
	RD-7.3.2.b Interview responsible personnel to verify procedures are followed for the CA to determine whether to recall and reissue all signed certificates with a newly generated signing key.
RD-7.3.3 Mechanisms (for example, time stamping) must exist to ensure that fraudulent certificates cannot be successfully used.	**RD-7.3.3.a** Examine documented procedures to verify that mechanisms are defined to ensure that fraudulent certificates cannot be successfully used.
	RD-7.3.3.b Interview responsible personnel and observe implemented mechanisms to verify that fraudulent certificates cannot be successfully used.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures

RD-7.4 CA/RA: The compromised CA must notify any superior or subordinate CAs of the compromise. The compromised CA must re-issue and distribute certificates or notify affected parties to apply for new certificates.
Note: *Affected parties may include subordinate CAs or solution providers (KDHs and POIs), depending upon the function of the compromised CA.*
	RD-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 either:
	  ○ Reissue and distribute certificates to affected parties, or
	  ○ Notify the affected parties to apply for new certificates.

	RD-7.4.b Interview responsible personnel to verify that the following procedures are performed in the event of a compromise:
	• The CA notifies any superior CAs.
	• The CA will notify any subordinate CAs.
	• The CA either:
	  ○ Reissues and distributes certificates to affected parties, or
	  ○ Notifies the affected parties to apply for new certificates.

Access to key-construct material must be limited and protected.	
RD-8 Access to material that can be used to construct secret and private keys (such as key components) must be: • Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use, and • Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. *(Reference 6F-5)*	
RD-8.1 CA/RA: 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 (for example, through the use of unique IDs).	**RD-8.1.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.
	RD-8.1.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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.1.1 CA/RA: 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, operating-system, and procedural controls.*	**RD-8.1.1.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.
	RD-8.1.1.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.
RD-8.2 CA/RA: The system enforces an explicit and well-defined certificate security policy and certification practice statement (as required in RD-9.2 and RD-9.3). This must include the following:	
RD-8.2.1 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 (for example, KDHs). ***Note:*** *Requirements for CA systems that issue certificates to POIs are covered at RD-8.6.*	**RD-8.2.1** 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 and/or revocation, or both certificate issuance and revocation. • Outside network access shall exist only for the purposes of "pushing" certificate-status information to relying parties (for example, KDHs).
RD-8.2.2 No CA or Registration Authority (RA) software updates are done over the network (local console access must be used for CA or RA software updates).	**RD-8.2.2** Examine software update processes to verify that local console access is used for all CA or RA software updates.
RD-8.2.3 Non-console access requires two-factor authentication. This also applies to the use of remote console access.	**RD-8.2.3** Examine remote access mechanisms and system configurations to verify that all non-console access, including remote access, requires two-factor authentication.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.2.4 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.*	**RD-8.2.4.a** Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions.
	RD-8.2.4.b Observe an authorized CA personnel attempt non-console access to the host platform without the authenticated encrypted session to verify that non-console access is not permitted.
RD-8.2.5 CA certificate (for SCD/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.*	**RD-8.2.5.a** Examine certificate security policy and certification practice statement to verify that CA certificate-signing keys must only be enabled under at least dual control.
	RD-8.2.5.b Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.
RD-8.3 CA/RA: 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).	**RD-8.3.a** Examine documented procedures to verify they include following: • Critical functions of the CA are defined. • Separation of duties is required to prevent one person from maliciously using a CA system without detection. • At a minimum, multi-person control is required for operational procedures such that no one person can gain control over the CA signing key(s).
	RD-8.3.b Observe CA operations and interview responsible personnel to verify: • Critical functions of the CA are identified. • Separation of duties is required to prevent one person from maliciously using a CA system without detection. • At a minimum, multi-person control is required for operational procedures such that no one person can gain control over the CA signing key(s).
RD-8.4 CA/RA: CA systems must be hardened to include: • Services that are not necessary or that allow non-secure access (for example, 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.	**RD-8.4.a** Examine system documentation to verify the following is required: • Services that are not necessary or that allow non-secure access (for example, 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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
	RD-8.4.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 (for example, rlogin, rshell, etc., commands in Unix) are removed or disabled. • Unnecessary ports are disabled. • There is documentation to support all active services and ports.
RD-8.4.1 CA/RA: Vendor-default IDs that are required only as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason.	**RD-8.4.1.a** Examine documented procedures to verify that vendor-default IDs required as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason.
	RD-8.4.1.b Examine system configurations and interview responsible personnel to verify that vendor-default IDs required as owners of objects or processes, or for installation of patches and upgrades, are disabled from login except as necessary for a documented and specific business reason.
RD-8.4.2 Vendor defaults (for example, passwords, SNMP strings, and IDs such as "Guest") must be changed, removed, or disabled before installing a system on the network.	**RD-8.4.2.a** Examine documented procedures to verify that vendor defaults (for example, passwords, SNMP strings, and IDs such as "Guest") must be changed, removed, or disabled before installing a system on the network.
	RD-8.4.2.b Examine system configurations and interview responsible personnel to verify that vendor defaults (for example, passwords, SNMP strings, and IDs such as "Guest") are changed, removed, or disabled before installing a system on the network.
RD-8.5 CA/RA: 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)	**RD-8.5.a** Examine system configurations and audit trails to verify that all key-management operations are logged.
	RD-8.5.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
RD-8.5.1 Audit logs must be archived for a minimum of two years.	**RD-8.5.1** Examine audit trail files to verify that audit trails are archived for a minimum of two years.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.5.2 Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.	**RD-8.5.2.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.
	RD-8.5.2.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.
RD-8.5.3 Logical events are divided into operating-system and CA application events. For both events 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.	**RD-8.5.3.a** Examine audit trails to verify that logical events are divided into operating-system and CA application events.
	RD-8.5.3.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.
	RD-8.5.3.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.
RD-8.5.4 Mechanisms must be in place to prevent and detect attempted tampering of CA application and operating system logs. *For example: A digital signature or a symmetric MAC (based on TDES) may be used to protect logs from alteration.*	**RD-8.5.4** Examine log security controls to verify that mechanisms are in place to prevent and detect attempted tampering of application and operating system logs.
RD-8.6 CA/RA: Certificate-processing systems may only be operated on-line for the issuance of certificates to POIs.	**RD-8.6.a** Examine certificate security policy and certification practice statement to verify that certificate-processing systems are only operated on-line for the issuance of certificates to POIs.
	RD-8.6.b Examine certificate-processing systems to verify they are only operated on-line for the issuance of certificates to POIs.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.6.1 Online certificate-processing system components 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 and external router. • 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.	**RD-8.6.1.a** Examine network and system configurations to verify that on-line certificate-processing system are protected from unauthorized access by firewall(s).
	RD-8.6.1.b Examine firewall configurations to 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 and external router. • 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.
RD-8.6.2 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.	**RD-8.6.2.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.
	RD-8.6.2.b Verify that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.
RD-8.7 CA/RA: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system-hardening standards.	**RD-8.7.a** Examine system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.
	RD-8.7.b Verify system configuration standards address all known security vulnerabilities.
	RD-8.7.c Examine a sample of system configurations to verify that system configuration standards are applied when new systems are configured.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.8 CA/RA: Implement user-authentication management for all system components as follows:	
RD-8.8.1 Employ at least one of the following methods to authenticate all users: • Something you know, such as a password or pass phrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	**RD-8.8.1.a** Examine documented procedures to verify that at least one of the defined authentication methods is required to authenticate all users to CA processing systems.
	RD-8.8.1.b Examine system configurations and observe authorized personnel authenticate to CA processing systems to verify that at least one of the defined authentication methods is used to authenticate all users to CA processing systems.
RD-8.8.2 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**RD-8.8.2** 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 changed after first use.
RD-8.8.3 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**RD-8.8.3.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 to administer any system components.
	RD-8.8.3.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.
	RD-8.8.3.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.
RD-8.8.4 Change user passwords at least every 30 days.	**RD-8.8.4** 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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.8.5 Require a minimum password length of at least eight characters.	**RD-8.8.5** 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.
RD-8.8.6 Use passwords containing numeric, alphabetic, and special characters.	**RD-8.8.6** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain numeric, alphabetic, and special characters.
RD-8.8.7 Limit repeated access attempts by locking out the user ID after not more than five attempts.	**RD-8.8.7** 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.
RD-8.8.8 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.	**RD-8.8.8** 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.
RD-8.8.9 The embedding of passwords in shell scripts, command files, communication scripts, etc., is strictly prohibited.	**RD-8.8.9** For a sample of system components, obtain and inspect system configuration settings to verify that passwords are not embedded in shell scripts, command files, or communication scripts.
RD-8.8.10 Where log-on security tokens (for example, smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/pass phrase to enable their usage. The PIN/pass phrase must be at least eight decimal digits in length, or equivalent. ***Note:*** *Log-on security tokens (for example, smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.*	**RD-8.8.10.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/pass phrase to enable their usage. **RD-8.8.10.b** Examine token-configuration settings to verify parameters are set to require PINs/passwords be at least eight decimal digits in length, or equivalent.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-8.9 CA/RA: Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations, including any physical access to the CA environment. If the synchronization process is manual, ensure that it occurs at least quarterly.	**RD-8.9.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 • Any physical access to the CA environment
	RD-8.9.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 • Any physical access to the CA environment
	RD-8.9.c If a manual process is defined, verify that the documented procedures require that it occurs at least quarterly.
	RD-8.9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.
Procedures must be in place for all key-administration operations.	
RD-9 Documented procedures must exist and must be demonstrably in use for all key-administration operations. *(Reference 6F-8)*	
RD-9.1 CA/RA: CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.	**RD-9.1.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.
	RD-9.1.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.
	RD-9.1.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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-9.2 CA/RA: 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.*	**RD-9.2.a** Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document.
	RD-9.2.b Examine documented operating procedures to verify they are defined in accordance with the CPS.
	RD-9.2.c Interview personnel and observe CA processes to verify that CA operations are in accordance with its CPS.
RD-9.3 CA/RA: 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.)	**RD-9.3.a** Examine documented certificate policy to verify that the CA has one in place.
	RD-9.3.b Examine documented operating procedures to verify they are defined in accordance with the certificate policy.
	RD-9.3.c Interview personnel and observe CA processes to verify that CA operations are in accordance with its certificate policy.
RD-9.4 CA/RA: 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.	**RD-9.4.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.
	RD-9.4.b Observe certificate issuing processes to verify that the identity of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-9.4.1 For CA and KDH certificate-signing requests, including certificate or key-validity status changes (for example, 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 (for example, 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.	**RD-9.4.1.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 (for example, 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.
	RD-9.4.1.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 (for example, 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.
RD-9.4.2 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.	**RD-9.4.2** 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

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
The certificate-processing operations center must implement a physical security boundary.	
RD-10 Certificate and Registration Authorities must implement physical security to reduce the risk of compromise of their systems. Physical security must be implemented to provide three tiers of physical security, as indicated below.	
RD-10.1 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 serversand cryptographic devices.	**RD-10.1.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
	RD-10.1.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	
RD-10.2 The entrance to the CA facility/building must include the following controls:	
RD-10.2.1 The facility entrance only allows authorized personnel to enter the facility.	**RD-10.2.1.a** Examine physical-security procedures and policies to verify they require that the facility entrance only allows authorized personnel to enter the facility.
	RD-10.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed to enter the facility.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-10.2.2 The facility has a guarded entrance or a foyer with a receptionist.	**RD-10.2.2.a** Examine physical-security procedures and policies to verify they require that the facility have a guarded entrance or a foyer with a receptionist.
	RD-10.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.
RD-10.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.	**RD-10.2.3.a** Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.
	RD-10.2.3.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	
RD-10.3 The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.	**RD-10.3.a** Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the level 2 barrier/entrance.
	RD-10.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.
RD-10.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.	**RD-10.3.1.a** Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.
	RD-10.3.1.b Interview CA personnel and observe visitors entering the environment to verify that visitors are authorized and escorted at all times within the Level 2 environment.
RD-10.3.2 Access logs must record all personnel entering the Level 2 environment. ***Note:*** *The logs may be electronic, manual, or both.*	**RD-10.3.2.a** Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.
	RD-10.3.2.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.
RD-10.4 The Level 2 entrance must be monitored by a video-recording system.	**RD-10.4.a** Observe the Level 2 entrance to verify that a video-recording system is in place.
	RD-10.4.b Review a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
Level 3 Barrier	
RD-10.5 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.*	**RD-10.5.a** Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.
	RD-**10.5.b** Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.
	RD-10.5.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.
RD-10.5.1 Doors to the Level 3 area must have locking mechanisms.	**RD-10.5.1** Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.
RD-10.5.2 The Level 3 environment must have true floor-to-ceiling (slab-to-slab) walls, or use solid materials (such as steel mesh or bars) below floors and above ceilings to protect against intrusions. (For example, the Level 3 environment may be implemented within a "caged" environment.)	**RD-10.5.2.a** Examine physical security documentation for the Level 3 environment to verify that true floor-to-ceiling walls, or enclosure on all sides with solid materials (such as steel mesh or bars), including below floors and above ceilings, is required.
	RD-10.5.2.b Examine the physical boundaries of the Level 3 environment to verify that it has true floor-to-ceiling walls, or is enclosed on all sides with solid materials (such as steel mesh or bars), including below floors and above ceilings.
RD-10.6 Documented procedures must exist for: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical	**RD-10.6.a** Examine documented procedures to verify they include the following: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical
	RD-10.6.b Interview responsible personnel to verify that the documented procedures are followed for: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-10.6.1 The Level 3 entrance requires dual access, as follows: • Personnel with access must be divided into an "A" group and a "B" group, such that access requires at least one member from each group. • The A and B groups must correlate to separate organizational units.	**RD-10.6.1.a** Examine documented access-control procedures to verify they require dual access to the Level 3 environment, as follows: • Personnel with access are divided into an "A" group and a "B" group. • Access requires at least one member from the "A" group and the "B" group. • The "A" and "B" groups must correlate to separate organizational units.
	RD-10.6.1.b Examine Level 3 access controls to verify that: • All personnel with access are included in either the "A" group or the "B" group. • Access requires at least one member from the "A" group and one from the "B" group.
	RD-10.6.1.c Examine organizational charts and interview a sample of personnel from the "A" and "B" groups to verify that the groups correlate to separate organizational units.
RD-10.6.2 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.*	**RD-10.6.2**.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.
	RD-10.6.2.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.
	RD-10.6.2.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.
RD-10.6.3 Other personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) must be accompanied by two (2) authorized and assigned resources at all times.	**RD-10.6.3.a** Examine documented policies and procedures to verify that personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) must be accompanied by two (2) authorized and assigned resources at all times.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
	RD-10.6.3.b Interview a sample of responsible personnel to verify that personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) are accompanied by two (2) authorized and assigned resources at all times.
RD-10.7 The Level 3 environment must require dual-control access and dual-occupancy such that the room is never occupied by a single individual for more than thirty (30) seconds. *For example: The Level 3 room is never occupied by a single individual except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.*	**RD-10.7.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 a single individual for more than thirty (30) seconds.
	RD-10.7.b Observe authorized personnel access the Level 3 environment to verify that dual-control access and dual-occupancy is enforced such that the room is never occupied by a single individual for more than thirty (30) seconds.
RD-10.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated	**RD-10.7.1.a** Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.
	RD-10.7.1.b Observe enforcement mechanism configuration to verify it is automated.
RD-10.7.2 The system must enforce anti-pass-back.	**RD-10.7.2.a** Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.
	RD-10.7.2.b Observe mechanisms in use and authorized personnel within the environment to verify that anti-pass-back is enforced.
RD-10.7.3 Dual occupancy requirements are managed using electronic (for example, badge, and/or biometric) systems.	**RD-10.7.3.a** Examine documented policies and procedures to verify that dual occupancy requirements are defined to be managed using electronic (for example, badge and/or biometric) systems.
	RD-10.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic systems.
RD-10.7.4 Any time a single occupancy exceeds 30 seconds, the system must automatically generate an audit event that is followed up by security personnel.	**RD-10.7.4.a** Examine documented policies and procedures to verify that the system must automatically generate an audit event that is followed up by security personnel, any time a single occupancy exceeds 30 seconds.
	RD-10.7.4.b Observe mechanisms in use to verify that the system automatically generates an audit event when single occupancy exceeds 30 seconds.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
	RD-10.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.
RD-10.8 Access to the Level 3 room must create an audit event, which must be logged.	**RD-10.8** 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.
RD-10.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel.	**RD-10.8.1** Observe authorized personnel perform 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.
RD-10.9 The Level 3 environment must be monitored as follows:	
RD-10.9.1 One or more cameras must provide continuous monitoring (for example, 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.*	**RD-10.9.1.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.
	RD-10.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.
	RD-10.9.1.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.
RD-10.9.2 The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.	**RD-10.9.2** 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.
RD-10.9.3 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 (for example, if intra-red cameras are used).*	**RD-10.9.3.a** Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for the cameras monitoring the environment.
	RD-10.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.
RD-10.9.4 Surveillance cameras must be configured to prevent the monitoring of computer screens, keyboards, PIN pads, or other systems which may expose sensitive data.	**RD-10.9.4.a** Observe 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.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
	RD-10.9.4.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.
RD-10.9.5 Personnel with access to the Level 3 environment must not have access to the media (for example, VCR tapes, digital-recording systems, etc.) with the recorded surveillance data.	**RD-10.9.5.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.
	RD-10.9.5.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.
RD-10.9.6 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.	**RD-10.9.6.a** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.
	RD-10.9.6.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.
RD-10.10 The environment must have continuous (24/7) intrusion-detection systems in place, which protect the secure area by motion detectors when unoccupied.	**RD-10.10.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
	RD-10.10.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
RD-10.10.1 Any windows in the secure area must be locked and protected by alarmed sensors.	**RD-10.10.1.a** Observe all windows in the secure areas to verify they are locked and protected by alarmed sensors.
	RD-10.10.1.b Examine configuration of window sensors to verify that the alarm mechanism is active.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-10.10.2 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**RD-10.10.2** Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.
RD-10.10.3 The intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have exited the secure area.	**RD-10.10.3.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.
	RD-10.10.3.b Observe a system test to verify that the intrusion-detection system(s) activates the alarm if a person is detected in the Level 3 area when the system is activated.
RD-10.10.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.	**RD-10.10.4** Examine security-system configurations to verify that an alarm event is generated for: • Unauthorized entry attempts • Actions that disable the intrusion-detection system
RD-10.11 All personnel (including CA personnel and visitors) must sign an access logbook when entering the Level 3 environment. ***Note:*** *The logs may be electronic, manual, or both.*	**RD-10.11.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.
	RD-10.11.b For a sample of personnel authorized to access the Level 3 environment, examine the access logbook to verify that they signed in when entering the Level 3 environment.
RD-10.11.1 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	**RD-10.11.1** 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
RD-10.11.2 The logbook must be maintained within the Level 3 secure environment.	**RD-10.11.2** Observe the location of the access logbook and verify that it is maintained within the Level 3 secure environment.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-10.12 All access-control and monitoring systems (including intrusion detection systems) are powered through an uninterruptible power source (UPS).	**RD-10.12** 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.
RD-10.13 All alarm events must be documented.	**RD-10.13.a** Examine security policies and procedures to verify they require that all alarm events are logged.
	RD-10.13.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
RD-10.13.1 Under no circumstances shall an individual sign off on an alarm event in which they were involved.	**RD-10.13.1.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.
	RD-10.13.1.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.
RD-10.13.2 The use of any emergency entry or exit mechanism must cause an alarm event.	**RD-10.13.2** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
RD-10.13.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.	**RD-10.13.3.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.
	RD-10.13.3.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.
RD-10.14 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. ***Note:*** *This may be done by either automated or manual mechanisms.*	**RD-10.14.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.
	RD-10.14.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	RD-10.14.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.

Annex A: Requirements for Symmetric-Key Distribution using Asymmetric Techniques	Testing Procedures
RD-10.14.1 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.	**RD-10.14.1.a** If a manual synchronization process is implemented, interview responsible personnel an examine records of synchronization to verify the mechanism is performed at least quarterly.
	RD-10.14.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.

Domain 6 Annex B: Cryptographic Key Operations – Key-Injection Facilities

The term key-injection facility (KIF) describes those entities that perform key injection of POI devices. 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 are in addition to those set out in all other Domains of this document.

For key-injection facilities participating in remote key establishment and distribution, requirements in Annex A also apply.

Keys that a KIF may manage in connection with POI key injection include but are not limited to the following:

- Base derivation keys (BDKs) used in the Derived Unique Key Per Transaction (DUKPT) key-management method
- Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (for example, 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)
- Master derivation keys (MDKs) used to derive unique terminal master keys for devices
- Terminal master keys (TMK) used in the master key/session key key-management method
- Data-encryption keys (DEK) used in the fixed-transaction key method
- Public and private key pairs loaded into encryption devices for supporting remote key-establishment and distribution applications
- Digitally signed public key(s) that are signed by a device manufacture's private key and subsequently loaded into an encryption device for supporting certain key-establishment and distribution applications protocols (if applicable)
- Device manufacturer's authentication key loaded into an encryption device for supporting certain key-establishment and distribution applications protocols (if applicable)
- Digitally signed HSM authentication public key(s) that are 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)

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
Account data must be in equipment resistant to compromise.	
KF-1 Account data must be encrypted in equipment that is resistant to physical and logical compromise. *(Reference 1A-1, 6D-2)*	
KF-1.1 Key-injection facilities must have processes in place to ensure: • Only keys specifically generated for use in a particular P2PE solution are injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution are not injected into any devices other than those designated by the specific P2PE solution provider.	**KF-1.1.a** Examine documented procedures to verify that procedures are defined to ensure: • Only keys specifically generated for use in a particular P2PE solution may be injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution must not be injected into any devices other than those designed by the specific P2PE solution provider.
	KF-1.1.b Interview responsible personnel and observe key-generation and loading processes to verify: • Only keys specifically generated for use in a particular P2PE solution may be injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution must not be injected into any devices other than those designed by the specific P2PE solution provider.
KF-1.2 Key-injection platforms and systems that include hardware devices for managing (for example, generating and storing) cryptographic keys must ensure those hardware devices conform to the requirements for SCDs. ***Note:*** *These devices must be managed in accordance with Domain 5 of this document.*	**KF-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.
	KF-1.2.b Examine key-injection platforms and systems used for managing cryptographic keys to verify they conform to the requirements for SCDs.

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
Keys must be entered using dual control and split knowledge.	
KF-2 Unencrypted secret or private keys must be entered into encryption devices using the principles of dual control and split knowledge. *(Reference 6D-1)*	
KF-2.1 Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (for example, 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.*	**KF-2.1.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. **KF-2.1.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. **KF-2.1.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.
KF-2.2 Controls must be in place to prevent and detect the loading of keys 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.*	**KF-2.2.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. **KF-2.2.b** Interview responsible personnel and observe key-loading processes and controls to verify that controls are implemented to prevent and detect the loading of keys by any one single person.

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
Procedures must prevent or detect unauthorized substitution.	
KF-3 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. *(Reference 6E-2)*	
KF-3.1 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 (for example, serial number) when deriving the key (for example, DUKPT, TMK) injected into it.	**KF-3.1.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.
	KF-3.1.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.
All keys must be unique to their devices.	
KF-4 All secret and private keys must be unique (except by chance) to that device. *(Reference 6E-4)*	
KF-4.1 Key-injection facilities must ensure that unique keys are loaded into each device. The same key(s) must not be loaded into multiple devices.	**KF-4.1.a** Examine documented procedures to verify they include controls to ensure that unique keys are loaded into each device, and that keys are not loaded into multiple devices.
	KF-4.1.b Interview responsible personnel and observe key-loading processes and controls to verify controls are implemented to ensure that only unique keys can be loaded into each device, and that keys cannot be loaded into multiple devices.
KF-4.2 Key-injection facilities that use DUKPT or other key-derivation methodologies on behalf of multiple acquirers must use different BDKs for each acquirer.	**KF-4.2.a** Examine documented procedures for generation and use of BDKs to verify they require separate BDKs be used for different acquirers.
	KF-4.2.b Observe key-loading processes for a sample of POIs to verify that separate BDKs are used for different acquirers.

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
KF-4.2.1 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.	**KF-4.2.1.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.
	KF-4.2.1.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
KF-4.3 Keys that are generated by a derivation process and derived from the same BDK must use unique data for the derivation process so that all POIs receive unique initial secret keys.	**KF-4.3.a** Examine documented key-generation procedures to verify they require that keys derived from the same BDK must use unique data for the derivation process so that all POIs receive unique initial secret keys.
	KF-4.3.b Observe key-loading processes to verify that keys which are derived from the same BDK use unique data for the derivation process so that all POIs receive unique initial secret keys.
KF-4.4 In a master/session key approach, the master key(s) and all session keys must be unique to each POI.	**KF-4.4.a** Examine documented key-generation procedures to verify they require that, in a master/session key approach, the master key(s) and all session keys must be unique to each POI.
	KF-4.4.b Observe key-loading processes to verify that in a master/session key approach, the master key(s) and all session keys must be unique to each POI.
KF-4.5 If injecting keys onto a single POI for more than one acquirer, the POI must have a completely different and unique key, or set of keys, for each acquirer. These different keys, or set of keys, must be totally independent and not variants of one another.	**KF-4.5.a** Examine documented key-generation and injection procedures to verify that the following is required when injecting keys onto a single POI for more than one acquirer: • The POI must have a completely different and unique key, or set of keys, for each acquirer. • These different keys, or set of keys, must be totally independent and not variants of one another.
	KF-4.5.b Observe processes for generation and injection of keys onto a single POI for more than one acquirer, to verify: • The POI has a completely different and unique key, or set of keys, for each acquirer. • These different keys, or set of keys, are totally independent and not variants of one another.

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
Physical protection of Key-Injection Facilities.	
KF-5 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.	
KF-5.1 The KIF must implement a physically secure area (secure room) for key injection. The secure room for key injection must include the following.	**KF-5.1** Observe the physical facility to verify that a secure room is designated for key injection and that all SCDs and other devices used in the key-injection platform are physically located in this room.
KF-5.1.1 The secure area must have extended walls from the real floor to the real ceiling using sheetrock or wire mesh.	**KF-5.1.1** 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.
KF-5.1.2 Any windows into the secure room must be locked and protected by alarmed sensors.	**KF-5.1.2.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	KF-5.1.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.
KF-5.1.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**KF-5.1.3** Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
KF-5.1.4 A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.	**KF-5.1.4** 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.
KF-5.1.5 A badge-control system must be in place that enforces: • Dual-access requirements for entry into the secure area, and • Anti-pass-back requirements.	**KF-5.1.5** 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
KF-5.1.6 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.*	**KF-5.1.6** 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.

Annex B: Requirements for Key-Injection Facilities	Testing Procedures
KF-5.1.7 A CCTV system must be in place that monitors on a continuous (24/7) basis.	**KF-5.1.7** Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a24/7 basis.
KF-5.1.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	**KF-5.1.8** 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.
KF-5.1.9 The CCTV server and digital storage must be secured in a separate secure area that is not accessible to personnel that have access to the key-injection area.	**KF-5.1.9.a** Inspect location of the CCTV server and digital-storage area to verify that the CCTV server and digital storage are located in a secure area that is separate to the key-injection area.
	KF-5.1.9.b Inspect access-control configurations for the CCTV server/storage area and the key-injection area to identify all personnel that 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.
KF-5.1.10 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.	**KF-5.1.10** 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.
KF-5.1.11 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.	**KF-5.1.11** 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.

Appendix A: Minimum Key Sizes and Equivalent Key Strengths

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	TDEA	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	112	1024	160	1024/160	128

A key-encipherment key shall be at least of equal or greater strength than any key that it is protecting. This applies to any key-encipherment key 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 purposes of this requirement, the following algorithms and key sizes by row are considered equivalent.

Algorithm	TDEA	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	112	1024	160	1024/160	-
Minimum key size in number of bits:	168	2048	224	2048/224	-
Minimum key size in number of bits:	-	3072	256	3072/256	128
Minimum key size in number of bits:	-	7680	384	7680/384	192
Minimum key size in number of bits:	-	15360	512	15360/512	256

TDEA refers to TDES keys with non-parity bits. The RSA key size 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.

The strength of the key should be appropriate for the number of enciphered blocks that the key is expected to process. For example, double-length TDES (112-bit) keys should not be used for more than one million enciphered blocks. In cases where the number of transactions potentially processed through the system using a “single” 112-bit TDES key greatly exceeds one million, triple-length TDES (168-bit) keys or AES should be used. Note that key-management schemes that greatly limit the number of transaction processed by a single key, such as Derived Unique Key Per Transaction (DUKPT), can be used to ensure that any individual key is used only a limited number of times

For Diffie-Hellman 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*,). Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
- Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES—see *ISO 16609 – Banking –Requirements for message authentication using symmetric techniques;* Method 3 should be used).