Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)®

Security Requirements and Testing Procedures

Version 3.2

June 2025

Document Changes

Date	Version	Revision	Description
September 2011	1.0		Initial release of *PCI Point-to-Point Encryption: Solution Requirements – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware).*
April 2012	1.1		Updated release of PCI P2PE Solution Requirements to incorporate Testing Procedures and additional guidance and content. For complete information, see *PCI P2PE Solution Requirements and Testing Procedures: Summary of Changes from PCI P2PE Initial Release.*
June 2015	2.0		Update from P2PE v1.1: For complete information, see the *Point-to-Point Encryption Standard – Summary of Changes from P2PE v.1.1 to v2.0.*
July 2015	2.0	1.1	Update from P2PE v2.0 to P2PE v2.0 Revision 1.1 to replace erroneous footnote in Annex C and to correct numbering for 1C-1.2.3.
December 2019	3.0		Updated from P2PE v2.0 r1.1 For complete information, see the *Point-to-Point Encryption Security Requirements and Testing Procedures – Summary of Significant Changes from P2PE v.2.0 to v3.0*
September 2021	3.1		Alignment with PCI PIN v3.1, updates based on a Request For Comment (RFC), and errata. For complete information, see the *Point-to-Point Encryption Security Requirements and Testing Procedures – Summary of Significant Changes from v3.0 to v3.1*
June 2025	3.2		Updated based on stakeholder feedback. For complete information, see the *Point-to-Point Encryption Standard – Summary of Significant Changes from v3.1 to v3.2.*

Contents

Introduction: Security Requirements for Point-to-Point Encryption

Purpose of this Document

This document, the *PCI Point-to-Point Encryption (P2PE)®: Security Requirements and Testing Procedures (P2PE Standard),* defines both security requirements and testing procedures for Point-to-Point Encryption (P2PE) Solutions, Components, and software (P2PE Applications and Non-payment Software). The objective of this P2PE Standard is to facilitate the development, validation, acceptance, listing, and subsequent deployment of P2PE Solutions that will increase the protection of account data by encrypting that data from the point of interaction (POI) within the merchant encryption environment where account data is captured through to the point of decrypting that data inside a decryption environment, effectively removing cleartext account data between these two points.

The requirements contained within this standard are intended for P2PE Solution Providers and other entities that provide P2PE Components or P2PE Applications for use in P2PE Solutions, as well as P2PE Assessors evaluating these entities. Additionally, merchants benefit from using P2PE Solutions due to increased protection of account data and subsequent reduction in the presence of cleartext account data within their environments.

Types of Solution Providers

P2PE Solution Provider

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

Merchant as a Solution Provider / Merchant-managed Solution

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

Note: *For merchant-managed solutions, where the term “merchant” is used in Domains 1, 3, 4, and 5 of this document, those requirements refer to the merchant’s encryption environments and represent requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.*

P2PE at a Glance – Overview of Domains and Requirements

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

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

Domain	Overview	P2PE Validation Requirements
Domain 1: **Encryption Device Management**	The secure management of the PCI-approved PTS POI devices with SRED used for account data acceptance, encryption, and subsequent transmission to the secure decryption environment.	**1A** Account data must be accepted by, processed, and encrypted in PCI-approved PTS POI devices with SRED **1B** Logically secure PTS POI devices **1C** Managing whitelists and Non-payment software **1D** Implement secure application-management processes **1E** Component providers *ONLY*: report status to solution providers
Domain 2: **Application Security**	The secure development of payment applications designed to have access to cleartext account data intended solely for installation on PCI-approved PTS POI devices.	**2A** Protect account data **2B** Develop and maintain secure applications **2C** Implement secure application-management processes
Domain 3: **P2PE Solution Management**	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the *P2PE Instruction Manual* (PIM).	**3A** P2PE solution management **3B** Third-party management **3C** Creation and maintenance of *P2PE Instruction Manual* for merchants **3D** Management of P2PE Applications
Domain 4: **Decryption Environment**	The secure management of the environment that receives encrypted account data and decrypts it.	**4A** Use approved decryption devices **4B** Secure the decryption environment **4C** Monitor the decryption environment and respond to incidents **4D** Implement secure, hybrid decryption processes **4E** Component providers *ONLY*: report status to solution providers

Domain	Overview	P2PE Validation Requirements
Domain 5: **P2PE Cryptographic Key Operations and Device Management**	Establish and administer key-management operations for account-data encryption PTS POI devices and decryption HSMs.	**Control Objective 1** Account data is processed using equipment and methodologies that ensure they are kept secure. **Control Objective 2** Account data keys and key-management methodologies are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys. **Control Objective 3** Keys are conveyed or transmitted in a secure manner. **Control Objective 4** Key loading is handled in a secure manner. **Control Objective 5** Keys are used in a manner that prevents or detects their unauthorized usage. **Control Objective 6** Keys are administered in a secure manner. **Control Objective 7** Equipment used to process account data and keys is managed in a secure manner. **5A** Account data is processed using algorithms and methodologies that ensure they are kept secure. **5H** For hybrid decryption solutions: Implement secure hybrid-key management. **5I** Component providers *ONLY*: report status to solution providers.
Appendix A: **Merchant-managed Solutions** *Note that this appendix is not applicable to third-party solution providers.*	Separate duties and functions between merchant encryption and decryption environments.	**MM-A** Restrict access between the merchant decryption environment and all other networks/systems. **MM-B** Restrict traffic between the encryption environment and any other CDE. **MM-C** Restrict personnel access between the encryption environment and the merchant decryption environment.

Merchant Encryption Environment

The P2PE Standard and Program are not intended to require an assessment of a merchant's encryption environment (excluding merchant-managed solutions where the merchant is both the merchant customer and the solution provider). P2PE Components, P2PE Applications, and P2PE Solutions may exist initially in the absence of any merchant customers or merchant-specific implementation. Where applicable, the entity being assessed must be able to demonstrate the capability to meet the security objectives as they apply to the intended implementation.

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

Secure cryptographic devices (SCDs) are used for the encryption and decryption of account data, signing P2PE Applications, Non-payment Software, and whitelists, as well as for the storage and management of cryptographic keys. SCDs include but are not limited to key-loading devices (KLDs), point-of-interaction (POI) encryption devices, and hardware security modules (HSMs).

An SCD used for the acceptance and encryption of account data at the point of sale is required to be a PCI-approved PTS POI device, which is a device evaluated and approved via the PCI PTS program and includes SRED (secure reading and exchange of data) as part of its evaluation and approval.

HSMs used within the decryption environment for decryption of account data and related cryptographic key operations must be approved to either *FIPS PUB 140-2* / *140-3* (overall level 3 or 4) or the PCI PTS HSM Standard.

***Note**: For P2PE Solutions using hybrid decryption, SCDs are used for encryption of account data as well as for storage and management of cryptographic keys; however, they are not required for decryption of account data.*

P2PE Solutions: Hardware Decryption or Hybrid Decryption

For P2PE Solutions, the merchant encryption environment at the point of payment acceptance consists exclusively of hardware-based encryption performed within PCI-approved PTS POI devices with SRED.

P2PE decryption environments require HSMs for *all* management of cryptographic keys, and that HSMs be used for decryption of account data (hardware decryption); or optionally account-data decryption can occur outside an HSM in non-SCD "Host Systems" (hybrid decryption) meeting additional hybrid decryption requirements specified in Domains 4 and 5, in Sections **4D** and **5H,** respectively.

***Note:** Hybrid decryption is NOT an option for merchant-managed solutions (MMS).*

SCD Domain Applicability

P2PE Solutions require the use of various types of SCDs. To assist in evaluating these device types, the following matrix indicates the domains each SCD type must be assessed to. The P2PE Standard does not require an evaluation of the physical and logical controls (i.e., the hardware and firmware of an SCD), which must have already been evaluated and approved as part of PCI HSM, *FIPS 140-2* or *140-3*, or PCI PTS POI, as applicable.

	SCD Type and Usage		
Domain	**PCI-Approved PTS POI Device for Account-Data Encryption**	***FIPS 140-2* or *140-3* Level 3 or 4, or PCI Approved HSM for Account-Data Decryption**	**SCD for Cryptographic Key Injection, Key Operations, or Software/Whitelist Signing**
Domain 1: Encryption Device and Application Management	Applicable	N/A	N/A
Domain 2: Application Security	Applicable	N/A	N/A
Domain 3: P2PE Solution Management	N/A	N/A	N/A
Domain 4: Decryption Environment[1]	N/A	Applicable	N/A
Domain 5: P2PE Cryptographic Key Operations and Device Management[1]	Applicable	Applicable	Applicable

[1] For hybrid decryption environments, note that while account-data decryption is performed in a Host System that meets requirements specified in Domain 4 (Section 4D) and Domain 5 (Section 5H), cryptographic key injection and key management must still be performed in a *FIPS 140-2* / *140-3* Level 3 or 4 HSM or a PCI-approved HSM.

Signing Devices

Keys used for signing software (P2PE Applications and Non-payment Software) must be stored and managed securely, either in an SCD (Secure Cryptographic Device) or an HMD (Hardware Management Device). Examples of an HMD include a smartcard or physical token approved to FIPS140-2/3 level 3 or Common Criteria EAL4+. Examples of an SCD include a HSM or (modified) PTS POI device. In all cases, the SCD or HMD must be configured or programmed to ensure the signing keys are not exposed outside of the protected memory and processing elements of the device.

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

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

A "**P2PE Component Provider**" is an entity that provides a service assessed to a defined set of P2PE requirements and has the potential to result in a P2PE Component Provider listing on the PCI SSC website. P2PE Component Providers' services are performed on behalf of other P2PE solution providers for use in P2PE Solutions. Refer to the PCI P2PE Program Guide for details.

P2PE *Solution Providers (or merchants as solution providers) must manage the overall P2PE Solution and any third parties used to perform P2PE functions on their behalf, whether those third parties are separately listed by PCI SSC as P2PE Component Providers or are assessed as part of the solution provider's P2PE assessment. Refer to the PCI P2PE Program Guide for additional information regarding the use of third parties and P2PE Component Providers.*

P2PE Applications and P2PE Non-payment Software

Note: *P2PE Applications and P2PE Non-payment Software do not meet the PCI PTS definition of "firmware" and are not reviewed as part of the PTS POI assessment. Therefore, both P2PE Applications and P2PE Non-payment Software must be assessed as part of this Standard. Additionally, software meeting the PTS definition of "firmware" is not reassessed during a P2PE assessment (PTS firmware is not considered a P2PE Application, nor is it P2PE Non-payment Software).*

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

A **"P2PE Application"** is any software or other files *with access to cleartext account data* that is intended to be loaded onto a PCI-approved PTS POI device and used as part of a P2PE Solution. All P2PE Applications and P2PE Non-payment Software intended for use on a PCI-approved PTS POI device as part of a P2PE Solution must be assessed either to Domain 2 or applicable requirements in Domain 1, respectively. P2PE Applications may be assessed and listed on PCI SSC's list of *Validated P2PE Applications*, for example, if that application is intended for use in more than one P2PE Solution. Alternatively, it can be assessed as part of a P2PE Solution and listed only as part of, and for exclusive use in, the P2PE Solution (known as a Solution-specific P2PE Application).

"P2PE Non-payment Software" is any software or other files with *no access to cleartext account data* that is intended to be loaded onto a PCI-approved PTS POI device and used as part of a P2PE Solution. P2PE Non-payment Software is assessed only per designated P2PE Domain 1 Requirements. *Note that this software is not subject to P2PE Domain 2 Requirements.*

Scope of Assessment for P2PE Products

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

The P2PE Program Guide contains a section denoting the P2PE Security Requirements that apply to P2PE Solutions (including Merchant-Managed Solutions), P2PE Applications, and P2PE Components.

Note: 'Not Applicable' (N/A) cannot be used by entities that provide only partial aspects of a defined P2PE Product. I.e., partial assessments are not permitted.

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

Domain 1 – Security requirements for the account data encryption devices and their management within the merchant environment	▪ All PCI-approved PTS POI devices included in the P2PE Solution (for the merchant to use for payment acceptance) ▪ Integration of all software/files onto PTS POI devices – P2PE payment applications (subject to a Domain 2 assessment) – P2PE Non-payment software (no access to clear-text account data—e.g., a loyalty or advertising application) – Whitelists
Domain 2 – Security requirements for P2PE Applications	▪ For software with access to cleartext account data intended for use on PTS-approved PTS POI devices
Domain 3 – Security requirements for management of the P2PE Solution	***Note:*** *This domain cannot be outsourced to a third party or to a P2PE Component Provider and MUST be satisfied by the P2PE Solution Provider (or merchant as a solution provider for MMS).* ▪ The solution provider's overall management of the P2PE Solution, including any third-party relationships, communications between various P2PE entities, and/or use of P2PE Component Providers ▪ Management of all software residing on the PTS POI devices, including: – P2PE Applications (subject to a Domain 2 assessment) ▪ The merchant-focused *P2PE Instruction Manual (PIM)* that the solution provider prepares for and distributes to merchants (for their encryption environments), including completion of the *PCI PIM Template*

Domain 4 – Security requirements for the decryption environment	▪ Management of all system components located within or connected to the decryption environment, including those used for decryption of account data, and ▪ Maintenance of PCI DSS compliance for the decryption environment
Domain 5 – Security requirements for P2PE key-management operations	▪ Secure key management—including all HSMs, key-loading devices, etc.—used by the solution provider or third party for cryptographic-key operations performed in support of account-data encryption PTS POI devices and decryption HSMs

Relationship between the PCI P2PE Standard and other PCI Standards

The relationship with other PCI standards is as follows:

- PTS POI devices (for account-data encryption) are approved per the PCI PIN Transaction Security (PTS) Point of Interaction (POI) Standard and Program
- HSMs used in the decryption environment for account-data decryption, as well as HSMs used for cryptographic-key operations, are approved per the PCI PTS HSM Standard and Program, or, via NIST *FIPS 140-2* or *140-3* (Level 3 or 4)
- The P2PE decryption environment is required to be PCI DSS compliant

Note: *This standard does not supersede the PCI Data Security Standard, PCI PIN Security Requirements, or any other PCI Standards, nor do these requirements constitute a recommendation from the PCI SSC or obligate merchants, service providers, or financial institutions to purchase or deploy such solutions. As with all other PCI standards, any mandates, regulations, or rules regarding these requirements are provided by the participating payment brands.*

For Assessors: Sampling for P2PE Solutions

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

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

Sampling of system components for assessment purposes does not reduce the scope of the applicability of P2PE requirements. Whether or not sampling is to be used, P2PE requirements apply to the entire P2PE Product under assessment as indicated in the P2PE Applicability of

Requirements section in the PCI P2PE Program Guide. If sampling is used, each sample must be assessed against all applicable P2PE requirements. Sampling of the P2PE requirements themselves is not permitted.

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

Samples of keys / key components must include all key types and/or functions.

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

- With respect to the PTS POI device HW/FW combinations, at least one unique combination of PTS POI device HW and FW supported by the P2PE Product must be validated and functionally tested (as determined by the P2PE requirements and associated testing procedures) **from each** PTS approval that is being associated with the P2PE Product assessment.
- Where the FW is not monolithic, i.e., it is split into separate FW functionality (e.g., OS, SRED, OP), every FW required for the device to function as intended must be validated and functionally tested (as determined by the P2PE requirements and associated testing procedures).

Note: *In the PCI PTS POI Program, firmware can also be denoted as an 'Application' (not to be confused with a P2PE Application or Non-payment Software) and listed as such on the PTS POI approval via the 'Applic:' label. This usually occurs if the firmware is modular, and it is at the PTS POI device vendor's discretion in terms of how they prefer the firmware to be listed on the PTS approval of their PTS POI device.*

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

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

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

Multiple Acquirers

The P2PE Standard outlines the technology and processes needed to ensure the security of a solution that protects account data from the point of interaction to the point of initial decryption. In some instances, multiple acquirers or multiple solution providers may manage one or more P2PE solutions on the same merchant PTS POI device. P2PE does not preclude these scenarios, as the business processes governing this shared environment are outside the responsibility of the PCI SSC. Vendors and merchants should be aware that in order for a P2PE Solution to be listed

on the PCI SSC website, each solution must be evaluated and tested, either independently or collectively. Once listed, merchants can then work with their acquirers to select a PTS POI device and validated solution provider(s) that meet their multiple-acquirer needs.

P2PE Program Guide

Refer to the PCI P2PE Program Guide for information about the PCI P2PE program, including, but not limited to, the following topics:

- Applicability matrix denoting the applicability of P2PE security requirements for each P2PE Product
- P2PE Component Provider types
- P2PE Report on Validation submission and acceptance processes
- Annual renewal process for validated P2PE products
- Vendor Release Agreements for vendors and providers of P2PE Solutions, P2PE Applications, and P2PE Components
- The Administrative and Delta Change processes
- Notification responsibilities in the event a listed P2PE solution is determined to be at fault in a compromise

Note: *The PCI SSC does* ***not*** *approve or list merchant-managed solutions (MMS) on its website. Refer to the P2PE Program Guide for more information on MMS.*

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

Technical FAQs

The PCI P2PE Technical FAQs is a separate document from this PCI P2PE Standard that provides answers to questions regarding the PCI P2PE Standard and Program.

Technical FAQs are normative and are an integral and mandatory part of the PCI P2PE Standard and Program. P2PE Technical FAQs must be fully considered during a PCI P2PE security assessment.

The PCI P2PE Technical FAQs document can be found in the PCI Council's Document Library for P2PE at https://www.pcisecuritystandards.org/document_library

Requirements Structure

The security requirements defined within this standard are presented in the following format:

- **Security Objectives**: The top-level requirements that identify the high-level security objectives.
- **Security Requirements**: Specific security controls or activities that must be satisfied to support the overarching security objectives.
- **Testing Procedures**: The expected testing activities to validate the security requirements have been satisfied.

Testing Procedure Methods

Entities are expected to produce evidence that the security requirements defined in this document have been satisfied. The Testing Procedures typically include the following activities:

- **Examine:** The tester critically evaluates evidence. Common examples include, ***but are not limited to***, reviewing policies, procedures, software design and architecture documents (electronic or physical), source code, configurations, log files, and security-testing results.
- **Interview:** The tester converses with relevant individual personnel. The purpose of interviews includes determining how an activity is performed, whether an activity is performed as defined, and whether personnel have particular knowledge or understanding of applicable policies, processes, responsibilities, and concepts.
- **Observe:** The tester watches a particular process or action. Common examples include, ***but are not limited to***, observation of personnel performing tasks or processes, software or system components performing a function or responding to input, system configurations/settings, environmental conditions, and physical controls. Observation may include the performance of "tests," so that the output of those tests may be observed, potentially under changing conditions as the input is manipulated by the tester or other systems.
- **Test:** The tester generally performs a process, action, or otherwise invokes functionality to confirm a requirement is satisfied.

At-a-glance P2PE Implementation Diagram

Diagram 1 illustrates a generic P2PE implementation. The remainder of this document details the P2PE security requirements and testing procedures on a domain-by-domain basis.

Note: *This diagram is for illustrative purposes.*

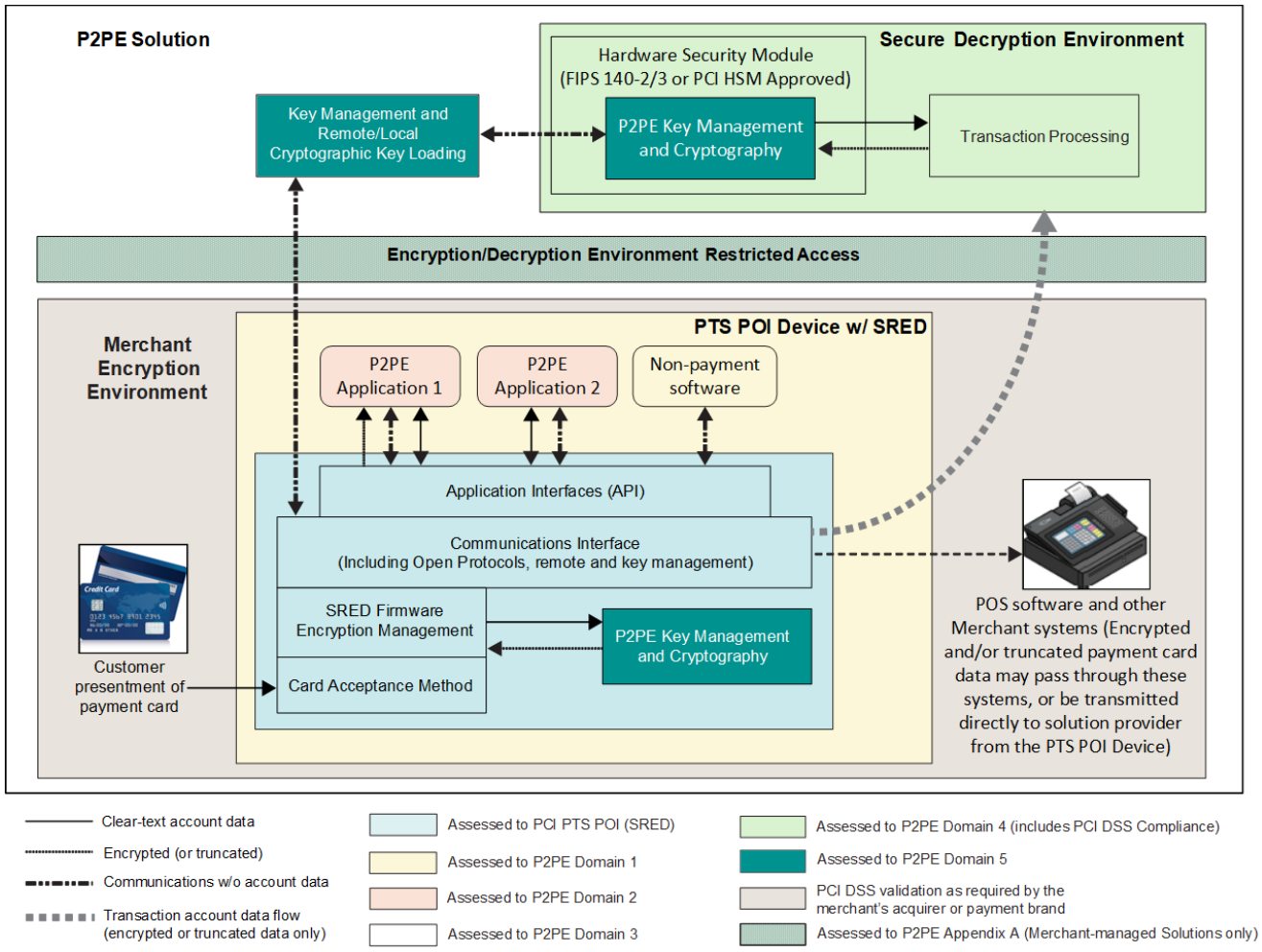


Diagram 1: Example P2PE Implementation at a Glance

Technical References

This list contains the specific standards referenced in the security requirements. As the standards referenced may change in order to more completely reflect the state of both technology and the threat environment at a particular point in time, it is necessary to ensure that the current version is used of a particular reference when evaluating whether a process, technique, piece of equipment, or policy is compliant with a specific requirement.

ANSI, FIPS, ISO, NIST, and PCI Standards

Source	Publication
ANSI	*ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques*
	ANSI X9.24 (Part 2): Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
	ANSI X9.24 (Part 3): Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
	ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
	ANSI X9.44: Key Establishment Using Integer Factorization Cryptography
	ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
	ANSI X9.102: Symmetric Key Cryptography For the Financial Services Industry—Wrapping of Keys and Associated Data
	ASC X9 TR 34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport
	ANSI X9.119 Part 1: Retail Financial Services - Requirements for Protection of Sensitive Payment Card Data - Part 1: Using Encryption Method
	ANSI X9.142: Public Key Cryptography For The Financial Services Industry - The Elliptic Curve Digital Signature Algorithm - ECDSA

Source	Publication
FIPS	*FIPS PUB 140–2: Security Requirements for Cryptographic Modules* *FIPS PUB 140–3: Security Requirements for Cryptographic Modules* *FIPS PUB 186-4: Digital Signature Standard (DSS)*
ISO	*ISO 9564: Financial services - Personal Identification Number Management and Security* *ISO 11568: Banking – Key Management (Retail)* *ISO 13491: Banking – Secure Cryptographic Devices (Retail)* *ISO TR 14742: Financial services - Recommendations on cryptographic algorithms and their use* *ISO 16609: Banking – Requirements for message authentication using symmetric techniques*
NIST	*NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* *NIST Special Publication 800-57: Recommendation for Key Management* *NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management* *NIST Special Publication 800-131: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*
PCI SSC	*PCI P2PE Program Guide* *PCI P2PE Glossary* *PCI P2PE Technical FAQs* *PCI P2PE PIM Template* *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements* *PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements* *PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Derived Test Requirements*

Domain 1: Encryption Device Management

Domain	Overview	P2PE Validation Requirements
Domain 1: **Encryption Device Management**	The secure management of the PCI-approved PTS POI devices with SRED used for account data acceptance, encryption, and subsequent transmission to the secure decryption environment.	**1A** Account data must be accepted by, processed, and encrypted in PCI-approved PTS POI devices with SRED **1B** Logically secure PTS POI devices **1C** Managing whitelists and Non-payment software **1D** Implement secure application-management processes. **1E** Component providers *ONLY*: report status to solution providers

Target audience: *P2PE Solution Providers or those who, on behalf of P2PE Solution Providers (a Component Provider or a Third Party), manage the PTS POI devices used in the P2PE Solution.*

Overview

Domain 1 requirements encompass the use of secure PTS POI devices and their management. The POI device must be a PCI-approved PTS POI device with SRED.

Domain 1 requirements also include the confirmation that all P2PE Applications, P2PE Non-payment software, and whitelists are properly reviewed and installed on the device.

Note: *Within this domain, the term "solution provider" refers to whichever entity is undergoing the P2PE assessment. This may be a P2PE Solution Provider, a P2PE Component Provider, or a merchant as a solution provider (MMS). Refer to "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" for more information about validating this Domain.*

Note: *For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 4, and 5 of this document refers to the merchant's encryption environments and represents requirements the merchant as a solution provider is responsible for meeting, for or on behalf of, those merchant encryption environments.*

Requirement 1A: Account data must be accepted by, processed, and encrypted in PCI-approved PTS POI devices with SRED	
Domain 1 Requirements	**Testing Procedures**
***1A-1** PCI-approved PTS POI devices with SRED are used for payment acceptance in the merchant environment.*	
1A-1.1 Account-data encryption operations must be performed using a PTS POI device (including the individual hardware and firmware) approved per the PCI PTS program with SRED (secure reading and exchange of data). The PTS approval listing must match the deployed PTS POI devices in the following characteristics: • Model name and number • Hardware (HW) version number(s) • Firmware (FW) version number(s) • Application (Applic) version number(s) • SRED listed as a function provided ***Note:*** *The PCI PTS POI approval listing must not be expired.* *The PCI PTS POI firmware must not be expired.* *Individual PTS POI hardware and firmware must also be assessed and approved to the PTS POI SRED requirements.*	**1A-1.1** For each PTS POI device type intended for use in the solution, examine the PCI SSC list of Approved PTS Devices to verify that all of the following PTS POI device type characteristics match the associated PTS listing: • Model name/number • Hardware (HW) version number(s) • Firmware (FW) version number(s) • Application (Applic) version number(s) (*This refers to PTS POI applications*) • SRED listed as a function provided ***Note**:* *Refer to the P2PE Technical FAQs and P2PE Program Guide for relevant information regarding PTS POI devices.* *This requirement CANNOT be sampled. Every PTS POI device type intended for use in the P2PE solution, including its hardware, firmware, and [PTS] applications, must be validated to this requirement.*
1A-1.1.1 The PTS POI device's SRED capabilities must be enabled and active prior to being placed into service.	**1A-1.1.1.a** Examine documented procedures to verify that SRED capabilities are enabled and active on all PTS POI devices prior to the devices being placed into service for payment acceptance in merchant encryption environments.
	1A-1.1.1.b [Removed]
1A-1.2 PTS POI devices must be configured to use only SRED-validated account-data capture mechanisms of its approved hardware/firmware.	**1A-1.2.a** Examine documented procedures to verify that PTS POI devices must be configured to use only SRED-validated account-data capture mechanisms of the approved hardware/firmware.
	1A-1.2.b [Removed]

Requirement 1A: Account data must be accepted by, processed, and encrypted in PCI-approved PTS POI devices with SRED	
Domain 1 Requirements	**Testing Procedures**
1A-1.2.1 [Requirement removed]	
1A-1.3 If the PTS POI device implements Open Protocols (as defined in the PCI PTS POI Standard) , the PTS POI device, including the specific HW and FW, must also be validated to the PCI PTS POI Open Protocols (OP) module. Open protocols include the following: • Link Layer Protocols • IP Protocols • Security Protocols • IP Services ***Note:*** *The PTS approval of a PTS POI device (including its specific hardware and firmware) using a communication method that uses a wireless, local, or wide area network to transport data is subject to a PCI PTS POI 'open protocols' evaluation. This includes, but is not limited to, Bluetooth, Wi-Fi, Cellular (GPRS, CDMA), or Ethernet. A serial point-to-point connection would not need to be assessed unless that connection is wireless or through a hub, switch, or other multiport device. In addition, any communication that uses a public domain protocol or security protocol would also be assessed with the applicable Open Protocols requirements.*	**1A-1.3.a** For each PTS POI device type that implements Open Protocols (as defined in the PCI PTS POI Standard) intended for use in the solution, examine the PCI SSC list of Approved PTS Devices to verify the PTS POI device, including the individual HW and FW, has been validated to the PCI PTS POI Open Protocols (OP) module.
	1A-1.3.b ***[This testing procedure is only applicable for PTS POI devices where its PTS approval listing denotes that a HW and/or FW version excludes the use of a specific Open Protocol]*** For all PTS POI device types where the PTS approval denotes the HW and/or FW excludes specific Open Protocols from being used, examine documented procedures to verify that these PTS POI devices must be configured to use only the validated Open Protocols of the approved hardware/firmware through appropriate examination, testing, and/or observation.
1A-1.4 Clear-text account data must not be disclosed to any component or device outside of the PCI-approved POI device.	**1A-1.4.a** Examine documented transaction processes and data flows to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.
	1A-1.4.b Using forensic tools and/or other data tracing methods, inspect a sample of test transactions to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI device.

Requirement 1A: Account data must be accepted by, processed, and encrypted in PCI-approved PTS POI devices with SRED	
Domain 1 Requirements	**Testing Procedures**
1A-2 [Moved to 3D-1]	
1A-2.1 [*Moved to Domain 3, Requirement 3D-1.1*]	
1A-2.2 [*Moved to Domain 3, Requirement 3D-1.2*]	

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
***1B-1** Solution provider ensures that logical access to PTS POI devices deployed at merchant encryption environment(s) is restricted to authorized personnel.*	
1B-1.1 Solution provider must ensure merchant logical access (by any means/method) to PTS POI devices, if needed, is restricted as follows: • Cannot view or access device configuration settings that could impact the security controls of the device or allow access to cryptographic keys or cleartext account data. • Cannot [re]enable device interfaces or data-capture mechanisms that are required to be disabled. • Does not use the PTS POI vendor's default passwords. • Cannot access PTS POI devices remotely	**1B-1.1.a** Examine documented PTS POI device configuration procedures and documented account privilege assignment rules to verify that merchant logical access (by any means/method) to PTS POI devices is restricted as follows: • Cannot view or access device configuration settings that could impact the security controls of the device or allow access to cryptographic keys or cleartext account data. • Cannot [re]enable device interfaces or data-capture mechanisms that are required to be disabled. • Does not use the PTS POI vendor's default passwords. • Cannot access PTS POI devices remotely

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
	1B-1.1.b Interview personnel and observe processes to verify that merchant logical access meets the following: • Cannot view or access device configuration settings that could impact the security controls of the device or allow access to cryptographic keys or cleartext account data. • Cannot [re]enable device interfaces or data-capture mechanisms that are required to be disabled. • Does not use the PTS POI vendor's default passwords. • Cannot access PTS POI devices remotely
1B-1.1.1 [Requirement removed]	
1B-1.2 All solution-provider personnel with logical access to PTS POI devices deployed in merchant encryption environments must be: • Documented in a formal list that is reviewed annually • Authorized by solution provider management. • Based on least privilege and need to know	**1B-1.2.a** Examine documented access-control policies and procedures for logical access to PTS POI devices by solution provider personnel to verify that all personnel with access: • Are documented in a formal list that is reviewed annually. • Are authorized by solution provider management. • Are granted access based on least privilege and need to know.
	1B-1.2.b Interview personnel and observe the process to logically access PTS POI devices and verify the requirement is satisfied.
1B-1.2.1 [Combined into 1B-1.2]	
***1B-2** Solution provider secures any remote access to PTS POI devices deployed at merchant encryption environments.*	
1B-2.1 Solution provider's authorized personnel must use multi-factor or cryptographic authentication for all remote access to merchant PTS POI devices. *[continued on next page]*	**1B-2.1.a** Examine documented procedures to verify that either multi-factor or cryptographic authentication must be used for all remote access to PTS POI devices.
	1B-2.1.b Interview personnel and observe remote-access mechanisms and controls to verify that either multi-factor or cryptographic authentication is used for all remote access to PTS POI devices.

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
Note: *Authorized solution provider personnel must use multi-factor or cryptographic authentication for all remote access to a terminal management system (TMS), or similar system used to either directly access or to manage merchant PTS POI devices.*	**1B-2.1.c [Removed]**
1B-2.2 PTS POI devices must be configured to ensure that remote access is only permitted from the solution provider's authorized systems (which might include a terminal management system (TMS) or similar system).	**1B-2.2.a** Examine documented PTS POI device-configuration procedures to verify that PTS POI devices must be configured to permit remote access only from the solution provider's authorized systems.
	1B-2.2.b Interview personnel and observe the remote access process to verify that remote access is permitted only from the solution provider's authorized systems.
1B-2.3 [Combined into 1B-1.1]	
1B-2.4 Solution provider must implement secure identification and authentication procedures for remote access to PTS POI devices deployed at merchant encryption environments.	**1B-2.4** Examine documentation to verify secure identification and authentication procedures are defined for remote access to PTS POI devices deployed at merchant encryption environments.
1B-2.5 Solution Provider must maintain individual authentication credentials for all authorized solution-provider personnel that are unique for each merchant, including: ***Note:*** *If a centralized terminal-management system (TMS) is utilized to manage multiple merchant accounts, it is acceptable for the TMS system to only require unique access for each authorized solution-provider employee accessing the TMS instead of requiring unique access per merchant.*	**1B-2.5** Examine documentation to verify that all authorized solution-provider personnel are required to have individual authentication credentials that are unique for each merchant (or if applicable, per centralized TMS).
1B-2.5.1 Tracing all logical access to PTS POI devices by solution-provider personnel to an individual user.	**1B-2.5.1.a** Examine documentation to verify that all logical access to PTS POI devices by solution-provider personnel can be traced to an individual user.

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
	1B-2.5.1.b Observe a sample of authorized logical accesses and examine access records/logs to verify that all logical access is traced to an individual user.
1B-2.5.2 Maintaining audit logs of all logical access to PTS POI devices by solution-provider personnel and retaining access logs for at least one year.	**1B-2.5.2** Examine documentation to verify that access records/logs of all logical access to PTS POI devices by solution-provider personnel are required to be retained for at least one year.
1B-3 *The solution provider implements procedures to protect PTS POI devices and applications from known vulnerabilities and securely update devices.*	
1B-3.1 [Requirement removed]	
1B-3.2 An up-to-date inventory of PTS POI device system builds must be maintained and confirmed at least annually and upon any changes to the build. ***Note:*** *A PTS POI system build includes at least the following information:* • *Model name and number* • *Hardware version number(s)* • *Firmware version number(s)* • *PTS Application version number(s)* • *P2PE Applications* • *Non-payment Software*	**1B-3.2.a** Examine documented procedures to verify they include: • Procedures for maintaining an up-to-date inventory of PTS POI device system builds • Procedures for confirming all builds at least annually and upon any changes to the build
	1B-3.2.b Examine documented inventory of PTS POI devices and their system builds to verify: • The inventory includes all PTS POI device system builds. • The inventory of PTS POI device system builds is up to date.

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
1B-3.3 Critical software security updates must be deployed to PTS POI devices in the merchant environment within 30 days of receipt from PTS POI device vendors and application/software vendors.	**1B-3.3.a** Examine documented procedures to verify they include defined procedures for deploying critical software security updates to PTS POI devices in the merchant environment within 30 days of receipt from PTS POI device vendors and application/software vendors.
Note: *A "critical software security update" is one that addresses an imminent risk to account data, either directly or indirectly.* *These security patches can be deployed via "push" from the solution provider or vendor, or via "pull" from the PTS POI device or merchant. In all cases, the solution provider is ultimately responsible to ensure security patches are installed in a timely manner.* Aligns with 2C-1.2	**1B-3.3.b** Examine security update deployment records and device logs, and interview responsible solution provider personnel to verify that critical security updates are deployed to PTS POI devices in the merchant environment within 30 days of receipt from PTS POI device vendors and application/software vendors.
1B-3.4 The integrity of software updates must be maintained during delivery and deployment, as defined by the relevant vendor—e.g., in the PTS POI device vendor's security guidance or in the P2PE Application's *Implementation Guide*.	**1B-3.4.a** Examine documented procedures for PTS POI device software updates to verify they follow guidance from the PTS POI device or application/software vendor to maintain the integrity of all patch and update code during delivery and deployment.
	1B-3.4.b Observe processes for delivering updates and interview responsible personnel to verify that the integrity of software is maintained during delivery and deployment, and according to guidance from the PTS POI device or application/software vendor. This must include attempts to load/run invalid software to verify the update is rejected.
	1B-3.4.c [Combined into 1B-3.4.b]

Requirement 1B: Secure logical access to PTS POI devices	
Domain 1 Requirements	**Testing Procedures**
1B-4 *Solution provider implements procedures to secure account data when troubleshooting.*	
1B-4.1 Any account data used for debugging or troubleshooting purposes must be securely deleted. These data sources must be collected in limited amounts and collected only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.	**1B-4.1.a** Examine documented procedures for troubleshooting customer problems and verify the procedures include the following for account data: • Never output to merchant environments • Collection only when needed to solve a specific problem • Storage in a specific, known location with limited access • Collection of only a limited amount of data needed to solve a specific problem • Encryption while stored • Secure deletion immediately after use
	1B-4.1.b For a sample of recent troubleshooting requests, observe data collection and storage locations, and interview responsible personnel to verify the procedures identified at **1B-4.1.a** were followed.
1B-5 *The P2PE solution provider maintains auditable logs of any changes to critical functions of the PTS POI device(s).*	
1B-5.1 Any changes to critical functions of PTS POI devices must be logged—either on the PTS POI device or within the remote-management systems of the P2PE solution provider. ***Note:*** *Critical functions include application and firmware updates as well as changes to security-sensitive configuration options, such as whitelists or debug modes.*	**1B-5.1.a** Examine documented procedures to verify that any changes to the critical functions of the PTS POI devices are logged, including: • Changes to the applications/software within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)
	1B-5.1.b Observe authorized personnel perform authorized changes on PTS POI devices and examine the log files to verify all activities in 1B-5.1.a.
	1B-5.1.c [Moved to new requirement 1B-5.1.1]
1B-5.1.1 The logs must be limited to need-to-know personnel, and the integrity of the logs is maintained and verified.	**1B-5.1.1.a** Examine documented procedures and sample logs to ensure access to logs is limited to need-to-know personnel and the integrity of logs is maintained and verified.

Requirement 1C: Managing whitelists and Non-payment software	
Domain 1 Requirements	**Testing Procedures**
***1C-1** Whitelists are managed securely.*	
1C-1.1 Processes for managing whitelisting functionality must exist and include, at a minimum: a) Implementing whitelisting functionality in accordance with the (as applicable): – PTS POI device vendor's security guidance – P2PE Application's *Implementation Guide* b) Signing in accordance with the PCI PTS POI Standard requirements that apply to the PTS POI device and its PTS approval prior to installation on the PTS POI device. c) Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data d) Documentation for all new installations and updates to whitelist functionality that includes the following (at a minimum): – Description and justification for the functionality – The identity of the authorized person who approved the new installation or updated functionality prior to release. ***Note:** The entity being assessed, which includes either the Component Provider or the Solution Provider, is expected to have documented processes to securely manage whitelists should they be utilized in the solution.*	**1C-1.1** Examine documented policies and procedures and interview personnel (as needed) to verify that processes for managing whitelisting functionality includes items a through d.
1C-1.1.1 [Superseded by revised 1C-1.1]	
1C-1.1.2 [Superseded by revised 1C-1.1]	
1C-1.1.3 [Superseded by revised 1C-1.1]	

Requirement 1C: Managing whitelists and Non-payment software	
Domain 1 Requirements	**Testing Procedures**
***1C-2** All software without a business need does not have access to cleartext account data.*	
***Note:** Requirements at 1C-2 are the only requirements applicable to software (Non-payment software) on PCI-approved POI devices with no access to clear-text account data (e.g., a loyalty or advertising application).*	
1C-2.1 Processes must be documented and implemented to ensure that, prior to new installations and updates, all Non-payment software: a) Is confirmed to not have any logical interfaces (e.g., application programming interfaces [APIs]) that allow for receiving, storing, processing, or transmitting of cleartext account data. b) Is signed in accordance with the PCI PTS POI Standard requirements that apply to the PTS POI device and its PTS approval prior to installation on the PTS POI device. c) Documentation for all new installations and updates to Non-payment software that includes the following (at a minimum): – The identity of the authorized person who approved the new installation or updated functionality prior to release. ***Note:** The entity being assessed, which includes either the Component Provider or the Solution Provider, is expected to have documented processes to securely manage Non-payment should it be utilized in the solution.*	**1C-2.1** Examine documented processes and interview responsible personnel (as needed) to confirm the stated processes are documented and established.
1C-2.1.1 [Requirement superseded by 1C-2.1]	
1C-2.1.2 [Requirement superseded by 1C-2.1]	
1C-2.1.3 [Requirement superseded by 1C-2.1]	

Requirement 1D: Implement secure application-management processes	
Domain 1 Requirements	**Testing Procedures**
***1D-1** Installation, updates, and changes to P2PE Applications is managed securely.*	
1D-1.1 Processes must be documented and implemented to ensure that, prior to new installations and updates, all P2PE Applications being installed must be: a) Implemented in accordance with the following, as applicable: – PTS POI device vendor's security guidance – P2PE Application's *Implementation Guide* b) Signed in accordance with the PCI PTS POI Standard requirements that apply to the PTS POI device and its PTS approval. c) Documented to include the identity of the authorized person(s) who approved the installation. **Note:** The entity being assessed, which includes either the Component Provider or the Solution Provider, is expected to have documented processes to securely manage P2PE Applications used in the solution.	**1D-1.1.a** Examine documented processes for installing P2PE Applications to verify the defined processes are in place.
1D-1.2 Processes must be documented and implemented to manage all changes to applications, including: • Documented approval for all changes by appropriate personnel • Documented reason and impact for all changes • Documented back-out procedures for application installations/updates ***Note:** Adding P2PE Applications to a Validated P2PE Solution, or defined changes to a Validated P2PE Application, requires a "Delta Change" process. See the PCI P2PE Program Guide for more information.*	**1D-1.2.a** Examine documented processes for implementing changes to applications, and interview solution-provider personnel, and confirm the following processes are in place: • All changes to applications include documented approval by appropriate authorized solution-provider personnel. • All changes to applications are documented as to reason and impact of the change. • Documentation includes back-out procedures for application installations/updates.
1D-1.2.1 [Requirement removed]	

Requirement 1D: Implement secure application-management processes	
Domain 1 Requirements	**Testing Procedures**
1D-1.3 [Requirement removed]	
***1D-2** Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	
1D-2.1 Upon receipt from the application vendor, a current copy of the application vendor's *Implementation Guide* must be retained and distributed to any outsourced integrators/resellers used for the P2PE solution. Aligns with 2C-3.1.3	**1D-2.1** Interview solution-provider personnel and examine documentation (including a current copy of the *Implementation Guide* from the application vendor) to confirm the following: • The solution provider retains a current copy of the *Implementation Guide*. The solution provider distributes the *Implementation Guide* to any outsourced integrators/resellers the solution provider uses for the P2PE solution upon obtaining updates from the application vendor.

Requirement 1E: Component providers ONLY: report status to solution providers	
Domain 1 Requirements	**Testing Procedures**
1E-1 For component providers of encryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain for subsequent PCI listing of the validated component provider's encryption management services. This section is not applicable to, and does not need to be completed by, P2PE solution providers (or merchants as solution providers) that include encryption management functions in their P2PE solution assessment (whether those functions are performed by the solution provider or are outsourced to non-PCI listed third parties).*	
1E-1.1 Track status of the encryption-management services and provide reports to solution provider annually and upon significant changes, including at least the following (per merchant location): • Types/models of PTS POI devices • Number of PTS POI devices deployed and any change in numbers since last report • Date of last inventory of PTS POI device system builds • Date when list of personnel with logical remote access to deployed merchant PTS POI devices was last reviewed/updated	**1E-1.1.a** Examine component provider's documented procedures for providing required reporting to applicable solution providers and interview responsible component-provider personnel to confirm that the following processes are documented and implemented (per merchant location): • Types/models of PTS POI devices • Number of devices deployed and change since last report • Date of last inventory of PTS POI device system builds • Date list of personnel with logical remote access to deployed merchant PTS POI devices was last reviewed/updated
	1E-1.1.b Examine reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of PTS POI devices • Number of PTS POI devices deployed and any change in numbers since last report • Date of last inventory of PTS POI device system builds • Date when list of personnel with logical remote access to deployed merchant PTS POI devices was last reviewed/updated

Requirement 1E: Component providers ONLY: report status to solution providers	
Domain 1 Requirements	**Testing Procedures**
1E-1.2 Manage and monitor changes to encryption-management services and notify the solution provider upon occurrence of any of the following: • Critical software security updates deployed to PTS POI devices • Addition and/or removal of PTS POI device types • Adding, changing, and/or removing P2PE Applications on PTS POI devices including description of change • Adding, changing, and/or removing P2PE Non-payment Software on PTS POI devices, including description of change • Updated list of PTS POI devices, P2PE Applications, and/or P2PE Non-payment Software ***Note:*** *Adding, changing, or removing PTS POI device types, P2PE Applications, and/or P2PE Non-payment Software may require adherence to PCI SSC's process for making changes. Please refer to the PCI P2PE Program Guide for details about obligations when adding, changing, or removing elements of a P2PE Solution.*	**1E-1.2.a** Examine component provider's documented procedures and interview responsible component-provider personnel, and confirm that processes include notifying the solution provider upon occurrence of the following: • Critical software security updates deployed to PTS POI devices • Addition and/or removal of PTS POI device types • Adding, changing, and/or removing P2PE Applications on PTS POI devices, (including description of change • Adding, changing, and/or removing P2PE Non-payment Software on PTS POI devices, including description of change • Updated list of PTS POI devices, P2PE Applications, and/or P2PE Non-payment Software
	1E-1.2.b Examine reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical software security updates deployed to PTS POI devices • Addition and/or removal of PTS POI device types • Adding, changing, and/or removing P2PE Applications on PTS POI devices, including description of change • Adding, changing, and/or removing P2PE Non-payment Software, including description of change • Updated list of PTS POI devices, P2PE Applications, and/or P2PE Non-payment Software

Domain 2: Application Security

Domain	Overview	P2PE Validation Requirements
Domain 2: **Application Security**	The secure development of payment applications designed to have access to cleartext account data intended solely for installation on PCI-approved PTS POI devices (with SRED) as part of a P2PE Solution.	**2A** Protect account data **2B** Develop and maintain secure applications **2C** Implement secure application-management processes

Target audience: *Application vendors designing applications (that have access to cleartext account data) for use within PCI-approved PTS POI devices (with SRED) as part of a P2PE Solution.*

Overview

Additional software is often added to PTS POI devices after the PTS evaluation and approval. It is vital to the security of these devices and their use in a P2PE solution that any such software is assessed to confirm its secure operation and protection of account data. This domain accounts for the assessment of all P2PE Applications (software with access to cleartext account data) that are intended for use within the PTS POI devices as part of a P2PE Solution.

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

Note: *The P2PE Standard does not require P2PE Applications used in a P2PE Solution to be validated to any other PCI Standard.*

See "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" for more information about P2PE Applications and software, and about validating P2PE Applications per this domain.

Use of a "Test Platform"

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

Domain 2 Informative Annex – Application's Implementation Guide

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

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
***2A-1** The application executes on a PCI-approved PTS POI device with SRED enabled and active.*	
2A-1.1 The application must be intended for use on a PTS POI device approved per the PCI PTS program, with SRED (secure reading and exchange of data). The PTS approval listing must match the following characteristics: • Model name and number • Hardware (HW) version number(s) • Firmware (FW) version number(s) • Application (Applic) version number(s) • SRED listed as a function provided ***Note:*** *Refer to the PCI P2PE Technical FAQs - Domain 2, Q4 regarding PTS POI device expiry.* *Individual PTS POI hardware and firmware must also be assessed and approved to the PTS POI SRED requirements.*	**2A-1.1** For each PTS POI device type the application is intended to support, examine the PCI SSC list of Approved PTS Devices to verify that all of the following PTS POI device type characteristics match the associated PTS approval listing: • Model name/number • Hardware (HW) version number(s) • Firmware (FW) version number(s) • Application version number(s) (*This refers to PTS POI applications*) • SRED listed as a function provided ***Note:*** *Refer to the P2PE Technical FAQs and P2PE Program Guide for additional information regarding PTS POI devices.* *This requirement CANNOT be sampled. Every PTS POI device type the application is intended to be used with in a P2PE solution, including its hardware, firmware, and [PTS] applications, must be validated to this requirement.*
2A-1.2 The application must only use the SRED-validated account-data capture mechanisms of the underlying PTS POI device for accepting and processing P2PE-related transactions.	**2A-1.2.a** Examine documentation to verify the application is designed to use only SRED-validated account-data capture mechanisms on the PTS POI device.
	2A-1.2.b *[This testing procedure is only applicable for PTS POI devices where its PTS approval listing denotes that a HW and/or FW version excludes the use of a specific account-data capture interface]* For all PTS POI device types where the PTS approval denotes the HW and/or FW the application is intended to support has an account-data capture interface excluded from being used, verify the application does not use that interface(s) through appropriate examination, testing, and/or observation.

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
***2A-2** The application does not store account data for any longer than business processes require.*	
2A-2.1 The application vendor must maintain current documentation for all data flows of account data (encrypted and cleartext) and provide a business justification for all uses of account data input into, processed by, and output from the application. ***Note:** It is prohibited for the application to output cleartext account data anywhere other than to the PTS POI firmware per 2A-3.1.*	**2A-2.1.a** Examine the application's design documentation to verify it documents all data flows (encrypted and cleartext) of account data and justifies all uses of account data input into, processed by, and output from the application.
	2A-2.1.b Examine the application source code and verify that account data is only utilized by the application according to the documentation.
2A-2.2 The application must not store account data (even if encrypted) as follows: • Application must not store PAN data after the payment transaction is complete. • Application must not store SAD after authorization is complete. ***Note:** Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (e.g., offline transactions). However, at all times, SAD is not stored after authorization is complete.*	**2A-2.2.a** Examine the application's design documentation and verify it includes a description of the following: • How it ensures the application does not store PAN after the payment transaction is complete • How it ensures the application does not store SAD after authorization is complete
	2A-2.2.b Examine source code to verify that the application is designed such that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.
	2A-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
2A-2.3 The application must not retain account data in working memory any longer than strictly necessary. ***Note:*** *If there are technical constraints of the architecture/language, they must be clearly documented, including:* • *The extent the account data can be considered to be securely deleted or otherwise inaccessible from working memory.* • *The technical limitation of the implementation and why the limitation cannot be resolved or otherwise remediated.* • *The residual risk that exists due to the technical limitation.* • *Any additional mechanisms employed to reduce the residual risk incurred by the technical limitation.*	**2A-2.3.a** Examine the application's design documentation and verify it contains a detailed description of how the application is designed to not retain account data in working memory any longer than strictly necessary.
	2A-2.3.b Examine the application source code and verify that account data is cleared from all working memory locations after use.
	2A-2.3.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application clears all working memory locations utilized for the temporal retention of account data during processing.
2A-2.4 The application must securely delete account data that was stored during application processing using industry-accepted methods for secure deletion of data. ***Note:*** *If there are technical constraints of the architecture/language, they must be clearly documented, including:* • *The extent the account data can be considered to be securely deleted or otherwise inaccessible from working memory.* • *The technical limitation of the implementation and why the limitation cannot be resolved or otherwise remediated.* • *The residual risk that exists due to the technical limitation.* • *Any additional mechanisms employed to reduce the residual risk incurred by the technical limitation.*	**2A-2.4.a** Examine the application's design documentation and verify it describes the process used by the application to securely delete account data that was stored during application processing industry-accepted methods for secure deletion of data.
	2A-2.4.b Examine the application source code and verify that all stored account data is irrecoverable once application processing is completed, in accordance with industry-accepted methods for secure deletion of data.
	2A-2.4.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide.* Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the application renders all account data irrecoverable, in accordance with industry-accepted standards for secure deletion of data, once the business process of the application is completed.

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
***2A-3** The application does not transmit cleartext account data outside of the PTS POI device or to any other co-resident software other than to the PTS POI device firmware and only uses communication methods included in the scope of the PCI-approved PTS POI device evaluation.*	
2A-3.1 The application must not: • Output cleartext account data outside the PTS POI device • Make cleartext account data externally available (e.g., to a printer, screen, etc.), except as allowed for requirement 2A-3.1.2 ***Note:** Output or sharing of cleartext data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process is assessed at Requirement **2A-3.4**.*	**2A-3.1.a** Examine the application's design documentation and verify the application is designed such that it does not: • Output cleartext account data outside of the PTS POI device • Make cleartext account data externally available (e.g., to a printer, screen, etc.), except as allowed for requirement 2A-3.1.2.
	2A-3.1.b Examine the application source code and verify the application satisfies this requirement.
	2A-3.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), test all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application satisfies this requirement.
2A-3.1.1 If the application outputs truncated PANs, the truncation must adhere to the allowable number of digits. ***Note:** Refer to the PCI P2PE Technical FAQs - Domain 2, Q3 regarding the allowable number of digits.* ***Note:** This requirement does not supersede stricter requirements in place for displays of PAN—e.g., legal or payment card brand requirements for point-of-sale (POS) receipts*	**2A-3.1.1.a** Examine the application's design documentation and verify that any truncation of PANs adheres to the allowable number of digits.
	2A-3.1.1.b Examine the application source code and verify that truncation of PANs adheres to the allowable number of digits.
	2A-3.1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that truncation of PANs adheres to the allowable number of digits.

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
2A-3.1.2 If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, this is ONLY allowable if the application includes the following: • The application only transmits cleartext PAN internally within the PTS POI device to an integrated printer that is part of the PTS POI device that is not attached via cabling or other networking mechanisms. • The P2PE Application securely deletes the cleartext PAN after completion of printing using industry-accepted methods for secure deletion of data.	**2A-3.1.2.a** Examine the application's design documentation and verify: • The application only transmits cleartext PAN internally within the PTS POI device to an integrated printer that is part of the PTS POI device that is not attached via cabling or other networking mechanisms. • The P2PE Application securely deletes the cleartext PAN after completion of printing using industry-accepted methods for secure deletion of data. • It contains a description of the legal/regulatory obligation necessitating supporting the printing of full PANs on merchant receipts.
	2A-3.1.2.b Examine the application source code and verify it satisfies the requirement.
	2A-3.1.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the application design/functionality satisfies the requirement.

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
2A-3.2 The application must not facilitate, via its own logical interface(s), sharing of (or allowing access to) cleartext account data directly with other applications/software (including other P2PE Applications and Non-payment Software). ***Note:*** *The application is allowed to share cleartext account data directly with the PTS POI device's SRED-approved firmware.*	**2A-3.2.a** Examine the application's *Implementation Guide* required at **2C-3** of this document and determine that it includes the following: • A list of all logical interfaces for the application, and the function/purpose of each. • The logical interfaces intended for sharing of cleartext account data (e.g., those used to pass cleartext data back to the approved firmware of the PTS POI device). • The logical interfaces *not* intended for sharing of cleartext account data (e.g., those for communication with other applications/software). Examine the logical interfaces used to communicate with other applications and confirm that the application cannot share cleartext account data with other applications/software via these logical interfaces. ***Note:*** *While an application is generally assessed in isolation, it may be deployed to a PTS POI device within a P2PE Solution that contains other co-resident software, or additional software might be added later. The assessor must validate this requirement with this point in mind.*
	2A-3.2.b Examine the application source code and verify it satisfies this requirement.
	2A-3.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the application satisfies this requirement.

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

Requirement 2A: Protect Account Data	
Domain 2 Requirements	**Testing Procedures**
2A-3.4 If whitelisting functionality is implemented in the application, the *Implementation Guide* must include the following: • How to configure the whitelisting functionality to ensure the output of cleartext account data is prohibited, except for non-PCI payment brand account/card data • How to perform cryptographic signing (or similar) prior to installation on the PTS POI device by authorized personnel using dual control • That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data • That such functionality must be approved by authorized personnel prior to implementation • That all new installations or updates to whitelist functionality must include the following: – Description and justification for the functionality – Who approved the new installation or updated functionality prior to release – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data	**2A-3.4** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify it contains details to describe whitelisting functionality and that it provides instructions as denoted in the requirement.

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

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

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
2B-1.3 All changes to the application must follow change-control procedures. The procedures must include the following:	**2B-1.3.a** Obtain and examine the developer's change-control procedures for software modifications, and verify that the procedures require the following: • Documentation of customer impact • Documented approval of change by appropriate authorized parties • Functionality testing to verify that the change does not adversely impact the security of the device • Back-out or application de-installation procedures
	2B-1.3.b Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it includes the following: • Documentation detailing the impact of all changes included in the relevant application release • Instructions detailing back-out or de-installation procedures for the application
	2B-1.3.c Examine recent application changes and trace those changes back to related change-control documentation. Verify that, for each change examined, the following was documented according to the change-control procedures:
2B-1.3.1 Documentation of impact.	**2B-1.3.1** Examine documentation to verify that the customer impact is included in the change-control documentation for each change.
2B-1.3.2 Documented approval of the change by appropriate authorized parties.	**2B-1.3.2** Examine documentation to verify documented approval by appropriate authorized parties is present for each change
2B-1.3.3 Functionality testing to verify that the change does not adversely impact the security of the device.	**2B-1.3.3.a** For each sampled change, examine evidence to verify that functionality testing was performed to verify that the change does not adversely impact the security of the device.
	2B-1.3.3.b Examine evidence to verify that all changes (including patches) are tested per secure coding guidance before being released.
2B-1.3.4 Back-out, rollback, or application de-installation procedures.	**2B-1.3.4** Examine evidence to verify that back-out, rollback, or application de-installation procedures are prepared for each change.

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
2B-1.4 Applications must be developed according to industry best practices for secure coding techniques, including (but not limited to): • Developing with least privilege. • Developing with fail-safe exception handling. • Developing with defensive (protective) techniques regarding the logical input interfaces of the application.	**2B-1.4** Examine software development processes and interview software developers to verify that secure coding techniques are defined and include: • Developing with least privilege • Developing with fail-safe defaults • Developing with defensive (protective) techniques regarding the logical input interfaces of the application
2B-1.4.1 Application development processes must include prevention of common coding vulnerabilities.	**2B-1.4.1.a** Examine software development processes for applications. Verify the process includes prevention of common coding vulnerabilities relevant to the programming languages and platforms in use.
	2B-1.4.1.b Test to verify that application is 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).

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

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

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

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

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

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

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

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
2B-2.1.1 The application must not circumvent, bypass, or add additional services or protocols to the Open Protocols of the PTS POI device firmware as approved and documented in the PTS POI device vendor's security guidance. This includes the use of: • Link Layer protocols • IP protocols • Security protocols • IP services ***Note:*** *The PCI PTS POI Open Protocol requirements ensures that open protocols and services in POI devices do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device. The POI device vendor defines what protocols and services are supported by the device and provides guidance to their use.* *Adding or enabling additional services or protocols or failing to follow the issued PTS POI device vendor's security guidance, will invalidate the approval status of that device for that implementation.*	**2B-2.1.1** Examine the application source-code and verify that the application: • Was developed according to the PTS POI device vendor's security guidance with respect to the documented Open Protocols • Does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the PTS POI device firmware as approved and documented in the POI device's vendor security guidance. This includes the use of: – Link Layer protocols – IP protocols – Security protocols – IP services
2B-2.2 The application-development process must include secure integration with any resources shared with or between applications. *(continued on next page)*	**2B-2.2.a** Examine the PTS POI device vendor's security guidance and the application's *Implementation Guide*. Confirm that the application's *Implementation Guide* required at **2C-3** of this document is in accordance with any applicable information in the PTS 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

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
2B-2.2 *(continued)*	**2B-2.2.b** Examine the application source-code and verify that any connection to, or use of, shared resources is done securely and in accordance with the POI device vendor's security guidance.
	2B-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that any connections to, or use of, shared resources are handled securely and in accordance with the POI device vendor's security guidance.
2B-2.3 Applications do not bypass or render ineffective any application segregation that is enforced by the POI device.	**2B-2.3** Examine the application source-code and verify that applications do not bypass or render ineffective any application segregation that is enforced by the POI device, in accordance with the POI device vendor's security guidance.
2B-2.4 Applications do not bypass or render ineffective any OS hardening implemented by the POI device.	**2B-2.4** Examine the application source-code and verify that applications do not bypass or render ineffective any OS hardening which is implemented by the POI device, in accordance with the device vendor's security guidance.
2B-2.5 Applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI device.	**2B-2.5** Examine the application source-code and verify that applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI device, in accordance with the device vendor's security guidance.
2B-2.6 If the application provides configuration/update functionality at-the-terminal (e.g., using an on-screen menu system), the application must not bypass or render ineffective any applicable controls contained within this standard. ***Note:*** *Some applications may provide administrative or other privileged functions at the terminal, such as the ability to load whitelists or change other application configurations. Any such functions provided in this way must meet all applicable P2PE requirements.*	**2B-2.6** Test the application loaded on each applicable PTS POI device type and verify that the application does not bypass or render ineffective any applicable controls contained within this standard.

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
***2B-3** The application vendor uses secure protocols, provides guidance on their use, and performs integration testing on the final application.*	
2B-3.1 The application developer's process must include full documentation, and integration testing of the application and intended platforms, including the following:	**2B-3.1** Examine/observe the application developer's system development documentation to verify the application developer's process includes full documentation and integration testing of the application and intended platforms, including the following:
2B-3.1.1 The application developer must provide security guidance describing how cryptographic keys and/or certificates have to be used. ***Note:** Examples of guidance include which cryptographic certificates to load, how to load account-data keys (through the firmware of the device), when to roll keys, etc.*	**2B-3.1.1** Examine the application's *Implementation Guide* required at 2C-3 of this document, and confirm it includes security guidance for solution providers, describing how cryptographic keys and/or certificates have to be used and managed.
2B-3.1.2 The application developer must perform final integration testing on the device, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform.	**2B-3.1.2** Interview application developers to confirm that final integration testing, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform, was performed.

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

Requirement 2B: Develop and maintain secure applications	
Domain 2 Requirements	**Testing Procedures**
2B-4.2 The application must not be able to decrypt SRED-encrypted account data—i.e., the application must not be able to recover the original cleartext account data from the encrypted account data.	**2B-4.2.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 is not capable of decrypting any cleartext account data encrypted by the SRED functions of the underlying POI firmware.
	2B-4.2.b Examine the application source code to verify that the application is not capable of decrypting cleartext account data encrypted by the SRED functions of the underlying PTS POI firmware.
	2B-4.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application is not capable of decrypting any cleartext account data encrypted by the SRED functions of the underlying POI firmware.

Requirement 2C: Implement secure application-management processes	
Domain 2 Requirements	**Testing Procedures**
***2C-1** New vulnerabilities are discovered, and applications are tested for those vulnerabilities on an ongoing basis.*	
2C-1.1 Software developers must establish and implement a process to identify and test their applications for security vulnerabilities and implementation errors prior to every release (including updates or patches) using manual or automated vulnerability assessment processes.	**2C-1.1.a** Examine processes to identify new vulnerabilities and test applications for vulnerabilities that may affect the application. Verify the processes include the following: • Using outside sources for security vulnerability information • Periodic testing of applications for new vulnerabilities
	2C-1.1.b Interview responsible software vendor personnel to confirm the following: • New vulnerabilities are identified using outside sources of security vulnerability information • All applications are tested for vulnerabilities
2C-1.2 Software vendors must establish and implement a process to develop and deploy critical security updates to address discovered security vulnerabilities in a timely manner. ***Note:** A "critical security update" is one that addresses an imminent risk to account data.*	**2C-1.2.a** Examine processes to develop and deploy application security upgrades. Verify that processes include the timely development and deployment of critical security updates to customers.
	2C-1.2.b Interview responsible software-vendor personnel to confirm that application security updates are developed and critical security updates are deployed in a timely manner.

Requirement 2C: Implement secure application-management processes	
Domain 2 Requirements	**Testing Procedures**
2C-2 *Applications are installed, and updates are implemented on the PTS POI devices only via trusted and cryptographically authenticated processes using an approved security mechanism evaluated for the PTS POI devices.*	
2C-2.1 Ensure that all application installations and updates are cryptographically authenticated as follows:	**2C-2.1** To confirm that all application installations and updates are cryptographically authenticated, verify the following:
2C-2.1.1 All application installations and updates on a POI device are cryptographically authenticated using the approved security mechanisms of the POI device's firmware.	**2C-2.1.1.a** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify that it includes the following: • A description of how the application is cryptographically authenticated using the approved security mechanisms of the POI device's firmware for any application installations and updates • Instructions for how to use the approved security mechanisms to perform application installations and updates • A statement that application installations and updates cannot occur except by using the approved security mechanisms of the POI device's firmware
	2C-2.1.1.b Examine the application source-code to verify that the application only allows installations and updates using the approved security mechanisms of the POI device's firmware.
	2C-2.1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that, by following the *Implementation Guide,* the application only allows installations and updates using the approved security mechanisms of the POI device's firmware.
	2C-2.1.1.d After the application is installed and configured in accordance with the *Implementation Guide,* test in order to perform an installation and an update using non-approved security mechanisms and verify that the PTS POI device will not allow the installation or update to occur.

Requirement 2C: Implement secure application-management processes	
Domain 2 Requirements	**Testing Procedures**
2C-2.1.2 The application developer includes guidance for whoever signs the application, including requirements for using an SCD or an HMD with dual control for the application-signing process.	**2C-2.1.2** Examine the application's *Implementation Guide* required at **2C-3** of this document and verify that it includes the following: • Instructions for how to sign the application • Instructions how to use an SCD or HMD with dual control for the application-signing process • A statement that all applications must be signed via the instructions provided in the *Implementation Guide*
***2C-3** Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	
2C-3.1 The process to develop, maintain, and disseminate an *Implementation Guide* for the application's installation, maintenance, upgrades, and general use must include the following:	**2C-3.1 [Removed]**
2C-3.1.1 Addresses all requirements in P2PE Domain 2 wherever the *Implementation Guide* is referenced.	**2C-3.1.1** Examine the *Implementation Guide* to verify it covers all related requirements in P2PE Domain 2.
2C-3.1.2 Review of the *Implementation Guide* at least annually and upon changes to the application or the P2PE Domain 2 requirements, and update as needed to keep the documentation current with: • Any changes to the application (e.g., device changes/upgrades, and major and minor software changes) • Any changes to the *Implementation Guide* requirements in this document	**2C-3.1.2.a** Examine documented procedures to verify the *Implementation Guide* is reviewed at least annually and upon changes to the application or the P2PE Domain 2 requirements
	2C-3.1.2.b Examine documented procedures to verify the *Implementation Guide* is updated as needed to keep the documentation current with: • Any changes to the application (e.g., device changes/upgrades and major and minor software changes) • Any changes to the *Implementation Guide* requirements in this document
2C-3.1.3 Distribution to all new application installers (e.g., solution providers, integrator/resellers, etc.), and re-distribution to all existing application installers every time the guide is updated.	**2C-3.1.3** Examine documented procedures to verify the *Implementation Guide* is distributed to new application installers and re-distributed to all application installers every time the guide is updated.

Requirement 2C: Implement secure application-management processes	
Domain 2 Requirements	**Testing Procedures**
2C-3.2 Develop and implement training and communication programs to ensure application installers (e.g., solution providers or integrators/resellers) know how to implement the application according to the *Implementation Guide*.	**2C-3.2** Examine the training materials and communication program, and confirm the materials cover all items noted for the *Implementation Guide* throughout P2PE Domain 2.
2C-3.2.1 Review the training materials for application installers on an annual basis and whenever new application versions are released. Update as needed to ensure materials are current with the *Implementation Guide*.	**2C-3.2.1** Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new application versions are released and updated as needed.

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

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

Domain 2 Requirement	Required Content for the *Implementation Guide*
2A-3.2	▪ A list of all logical interfaces for the application, and the function/purpose of each. ▪ The logical interfaces intended for sharing of cleartext account data (e.g., those used to pass cleartext data back to the approved firmware of the PTS POI device) ▪ The logical interfaces not intended for sharing of cleartext account data (e.g., those for communication with other applications)
2A-3.3	Guidance that use of any other methods for external communications is not allowed.
2A-3.4	If applicable, details to describe the whitelisting functionality implemented by the application as follows: • How to configure the application functionality to ensure the output of cleartext account data is prohibited, except for non-PCI payment brand account/card data • How to perform cryptographic signing (or similar) prior to installation on the PTS POI device by authorized personnel using dual control. • That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data. • That such functionality must be approved by authorized personnel prior to implementation • That documentation for all new installations or updates to whitelist functionality includes the following: • Description and justification for the functionality • Who approved the new installation or updated functionality prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data
2B-1.1	Information from the PTS POI device vendor's security guidance applicable to the application (e.g., application configuration settings which are necessary for the application to function with the device).
2B-1.3	• Documentation detailing the impact of all changes included in the relevant application release • Instructions detailing back out or de-installation procedures for the application

Domain 2 Requirement	Required Content for the *Implementation Guide*
2B-1.10	A description of the vendor's published versioning methodology, including the following: • Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.) • Details of how security-impacting changes will be indicated by the version scheme • Details of how other types of changes will affect the version • Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change
2B-2.1	• Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing. • Any guidance that the PTS POI device vendor intended for integrators/ resellers, solution providers, and/or end-users.
2B-2.2	Includes the following, in accordance with the PTS 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	Security guidance for solution providers, describing how cryptographic keys and/or certificates have to be used and managed.
2B-4.1	The description of the application's function that includes the following: • Confirmation that the application does not perform its own encryption of cleartext account data, nor does it replace the PTS POI device's SRED encryption. • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption.
2C-2.1.1	• A description of how the application uses the approved security protocol of the PTS POI device's firmware for any application installations and updates • Instructions for how to use the approved security protocol to perform application installations and updates • A statement that application installations and updates cannot occur except by using the approved security protocol of the POI device's firmware

Domain 2 Requirement	Required Content for the *Implementation Guide*
2C-2.1.2	• Instructions for how to sign the application • Instructions how to implement the dual control for the application-signing process • A statement that all applications must be signed via the instructions provided in the *Implementation Guide*

Domain 3: P2PE Solution Management

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

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

Overview

The effective management and integration of the essential elements comprising the P2PE Solution ultimately results in the absence of cleartext account data within the merchant's encryption environment—e.g., merchant stores, shops, retail premises, etc. Domain 3 is critical to the P2PE Solution due to the fact that P2PE Solutions consist of numerous devices/products (PTS POI devices, P2PE Applications, HSMs, management of Component Providers, etc.) operating in various environments (e.g., encryption, decryption, and key-injection), and all of these devices, products, and environments must be successfully integrated together and managed. In all cases, the P2PE Solution Provider remains responsible for the compliance and security of their entire P2PE Solution.

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

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

For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 4, and 5 of this document refers to the merchant's encryption environments and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
***3A-1** The solution provider maintains documentation detailing the P2PE solution architecture and data flows.*	
3A-1.1 Current documentation must be maintained to describe or illustrate the architecture of the overall P2PE solution and include the following: • Identification of all parts of the overall solution managed by the solution provider • Identification of any parts of the overall solution outsourced to third-party service providers • Identification of P2PE controls covered by each third-party service provider.	**3A-1.1.a** Interview relevant personnel and examine documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the overall P2PE solution.
	3A-1.1.b Interview relevant personnel and examine documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document is current.
	3A-1.1.c Interview relevant personnel and examine documentation that describes and/or illustrates the architecture of the overall P2PE solution to verify that the document: • Identifies all components of the overall solution managed by the solution provider. • Identifies all components of the overall solution that have been outsourced to third-party solution providers. • Identifies all P2PE controls covered by each third-party service provider.
3A-1.2 Current documentation (including a data-flow diagram) must include details of the account-data flow from the PTS POI devices (the point the card data is captured and encrypted) through to the point the encrypted card data is decrypted and the cleartext data exits the decryption environment.	**3A-1.2** Examine documentation and interview personnel (as needed) to verify (for each intended solution implementation, if they differ, e.g., across different merchant environments): • All account-data flows across systems and networks from the point the card data is captured by the PTS POI devices through to the point the card data exits the decryption environment. • All documentation is kept current and updated as needed upon changes to the environment and/or solution.
3A-1.2.1 Cleartext account data must not be disclosed to any component or device outside of the PCI-approved PTS POI devices within the merchant environment until it is securely decrypted in the decryption environment.	**3A-1.2.a** Examine documentation (for each intended solution implementation, if they differ, e.g., across different merchant environments) to verify that cleartext account data is not disclosed to any component or device outside of the PCI-approved PTS POI devices within the merchant environment(s) until it is securely decrypted in the decryption environment(s).

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-1.3 If there is a legal or regulatory obligation in a region for merchants to print full PAN on merchant receipts, it is allowable for the merchant to have access to full PAN for this purpose, but the solution provider must document specifics about the legal or regulatory obligation including at least the following: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies **Note:** *Domain 2 (at 2A-3.1.2) also includes requirements that must be met for any PTS POI device and any P2PE Application, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*	**3A-1.3.a** Examine solution provider's documentation about the legal/regulatory obligation that requires merchants to have access to full PANs for receipt printing purposes to verify that the documentation includes at least the following details about the legal/regulatory obligation: • What specifically is required • Which legal/regulatory entity requires it • To which region/country it applies **3A-1.3.b [Removed]**

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
***3A-2** The solution provider manages and monitors status reporting from P2PE component providers.*	
3A-2.1 If P2PE component providers are used, a methodology must be implemented to manage and monitor status reporting from P2PE component providers, including: • Ensuring reports are received from all P2PE component providers as specified in the "*Component providers ONLY: report status to solution providers*" sections of this Standard (as applicable to the component provider) • Confirming reports include at least the details specified in the "*Component providers ONLY: report status to solution providers*" sections of this Standard (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider • Following up with the component provider to resolve any questions or changes in expected performance of the component provider	**3A-2.1** Interview responsible personnel, examine documentation, and observe processes to verify the solution provider has implemented a methodology for managing and monitoring status reporting from P2PE component providers, including processes for: • Ensuring reports are received from all P2PE component providers as specified in the "*Component providers ONLY: report status to solution providers*" sections of this Standard (as applicable to the component provider) • Confirming reports include at least the details specified in the "*Component providers ONLY: report status to solution providers*" sections of this Standard (as applicable to the component provider), and any additional details as agreed between a component provider and the solution provider • Following up with the component provider to resolve any questions or changes in expected performance of the component provider
3A-2.2 Processes must be implemented to ensure P2PE controls are maintained when changes to the P2PE solution occur, including but not limited to: • Changes in third-party service providers • Changes in overall solution architecture	**3A-2.2.a** Interview responsible personnel and examine documentation to verify the solution provider has a formal process for ensuring P2PE controls are maintained when changes to the P2PE solution occur, including procedures for addressing the following: • Changes in third-party service providers • Changes in overall solution architecture
	3A-2.2.b For a sample of changes, examine the changes to verify they were documented and the solution updated accordingly.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-3 *Solution provider implements processes to respond to notifications from merchants, component providers, and/or other third parties, and provide notifications about any suspicious activity involving the P2PE solution.*	
3A-3.1 Processes must be implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity, and provide immediate notification to all applicable parties of suspicious activity including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures ***Note:*** *"immediate" means promptly or as soon as possible.*	**3A-3.1** Examine documented procedures and interview personnel to verify processes are implemented to respond to notifications from merchants, component providers, and other third parties about any suspicious activity and provide immediate notification to all applicable parties, including but not limited to: • Physical device breaches • Tampered, missing, or substituted devices • Unauthorized logical alterations to devices (e.g., configuration, access controls, whitelists) • Failure of any device security control • Unauthorized use of sensitive functions (e.g., key-management functions) • Encryption/decryption failures
3A-3.2 Upon detection of any suspicious activity defined at **3A-3.1**, the PTS POI device must be immediately removed, shut down, or taken offline until the integrity of the device is verified and the P2PE encryption mechanism is restored.	**3A-3.2** Examine documented procedures and interview responsible personnel to verify that upon detection of any suspicious activity defined at **3A-3.1**, PTS POI devices are immediately removed, shut down, or taken offline.
3A-3.2.1 The PTS POI device must not be re-enabled until it is confirmed that the issue has been resolved and P2PE encryption functionality is restored and re-enabled.	**3A-3.2.1** Examine documented procedures and interview personnel to verify the PTS POI devices must not be re-enabled until it is confirmed that the issue has been resolved and P2PE encryption functionality is restored and re-enabled.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-3.3 The solution provider must maintain a record, at minimum of one year, of all suspicious activity, to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that the issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled	**3A-3.3** Examine documented procedures and related records, and interview personnel to verify they maintain records of all suspicious activity, including the following details: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time that issue was resolved • Details of whether any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled
3A-3.4 Procedures must incorporate any applicable incident response procedures defined by the PCI payment brands, including timeframes for reporting incidents.	**3A-3.4.a** Examine documented incident-response plans to verify they incorporate procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.
	3A-3.4.b Interview responsible personnel to verify that any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents, are known and implemented.

Requirement 3A: P2PE solution management	
Domain 3 Requirements	**Testing Procedures**
3A-3.5 Processes must be implemented to ensure any P2PE control failures are addressed including, but not limited to: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Updating the solution and/or controls to prevent cause from recurring	**3A-3.5.a** Interview responsible personnel and examine documentation to verify the solution provider has a formal process for any P2PE control failures, including procedures for addressing the following: • Identification that a failure has occurred • Identifying the root cause • Determining remediation needed to address root cause • Identifying and addressing any security issues that occurred during the failure • Implementing controls to prevent cause from recurring
	3A-3.5.b For a sample of P2PE control failures, interview personnel and examine supporting document to verify that: • Identification occurred. • Corrective actions were implemented and documented. • The solution and/or control was updated accordingly.

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

Requirement 3B: Third-party management	
Domain 3 Requirements	**Testing Procedures**
3B-1.2 If the Solution Provider uses third parties to manage any of the SCD types used in the P2PE solution, the solution provider must establish formal agreements with the third parties to ensure those third parties provide the Solution Provider with the following: • Notification of any changes that require a Delta Change per the P2PE Program Guide • Details of the change, including the reason for the change • Updated list of any dependencies included in the Delta Change (e.g., PTS POI devices, P2PE Applications, and/or HSMs) used in the solution	**3B-1.2** Examine documentation for all third parties managing SCDs on behalf of the solution provider and verify the following is required: • Notification of any changes that require a Delta Change per the P2PE Program Guide • Details of the change, including the reason for the change • Updated list of any dependencies included in the Delta Change (e.g., PTS POI devices, P2PE Applications, and/or HSMs) used in the solution

Requirement 3C: Creation and maintenance of the P2PE Instruction Manual *for merchants*	
Domain 3 Requirements	**Testing Procedures**
***3C-1** Solution provider develops, maintains, and disseminates a P2PE Instruction Manual (PIM) to merchants.*	
3C-1.1 The PIM must be developed, maintained, distributed to merchants, and provided to merchants upon request. Content for the PIM must be in accordance with the mandatory *PIM Template*. ***Note:** It is imperative that the PIM accurately contains all required information. This is critical for the PTS POI devices and instructions on how to access the PTS POI device HW/FW/Application version information such that it can be verified in the merchant environment against the Validated P2PE Solution details. The PIM must accurately reflect the information required for the merchant, which may warrant separate PIMs for differing merchant environments if the PTS POI devices, instructions, and/or required information differ between merchants.*	**3C-1.1.a** Examine the *P2PE Instruction Manual* (PIM) to verify it covers all related instructions, guidance and requirements as specified in the *PIM Template*.
	3C-1.1.b Examine documented procedures to verify mechanisms are defined to distribute the PIM to all merchants using the P2PE solution, and to provide the PIM to merchants upon request.
	3C-1.1.c Interview responsible personnel and observe processes to verify PIM is distributed to all merchants using the P2PE solution and that the PIM is provided to merchants upon request.
	3C-1.1.d Examine the PIM to verify that all devices specified in the PIM are eligible PCI-approved PTS POI devices that were assessed as part of this P2PE solution assessment.
	3C-1.1.e Examine the PIM to verify the following: • All P2PE Applications specified in the PIM are assessed for this solution. • All P2PE Applications specified in the PIM are *either* PCI-listed P2PE Applications or assessed to Domain 2 as part of this P2PE solution assessment (Solution-specific P2PE Applications).
	3C-1.1.f Examine the PIM to verify that all P2PE Non-payment software specified in the PIM has been assessed as part of this P2PE solution assessment (per Requirement **1C-2**).
	3C-1.1.g [Removed]

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

Requirement 3D: Management of P2PE Applications	
Domain 3 Requirements	**Testing Procedures**
3D-1 *All software with access to cleartext account data (P2PE Applications) is validated to P2PE Domain 2 and is only deployed on/to eligible PCI-approved PTS POI devices with SRED.* ***Note:*** *Refer to the P2PE Technical FAQs and P2PE Program Guide for information regarding PTS POI devices.*	
3D-1.1 All software on PTS POI devices with access to cleartext account data must be validated according to Domain 2 as a P2PE Application.	**3D-1.1.a** For P2PE Applications on the PCI SSC list of *Validated P2PE Applications*, examine the list and compare with the applications/software intended for use in the solution to verify that the applications match the P2PE Application listing in the following characteristics: • Application name • Version number(s)
	3D-1.1.b For applications/software intended for use in the solution that are not on the PCI SSC list of *Validated P2PE Applications*, the application/software must be assessed to P2PE Domain 2. ***Note:*** *The validated P2PE Application can be submitted independently to be listed as a Validated P2PE Application, or it can be submitted with the P2PE Solution to be listed as part of, and for use only in, the P2PE Solution as a Solution-specific P2PE Application. Refer to the P2PE Program Guide for details.*
3D-1.2 P2PE Applications must only be deployed on eligible PTS POI device types that are: • Confirmed per **1A-1.1** as a PTS approved device(s) and associated with the P2PE Solution, either as part of P2PE Solution assessment, or as part of a Validated P2PE Component being used by the P2PE Solution • Explicitly included in the Domain 2 assessment for that P2PE application *[continued on next page]*	**3D-1.2.a** For P2PE Applications on the PCI SSC list of *Validated P2PE Applications*, review the list and verify all PTS POI device types the P2PE Application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) and associated with the P2PE Solution, either by satisfying the applicable requirements as part of this P2PE Solution assessment, or the requirements already being satisfied as part of a Validated P2PE Component being used by the P2PE Solution • Explicitly included in the Validated P2PE Application's listing ***Note:*** *If the P2PE Application is not separately Validated and Listed, and is intended to be, it must be done prior to submitting the P2PE Solution. Refer to the PCI P2PE Program Guide for details.*

Requirement 3D: Management of P2PE Applications	
Domain 3 Requirements	**Testing Procedures**
3D-1.2 *(continued)*	**3D-1.2.b** For applications not on the PCI SSC list of *Validated P2PE Applications* and intended for use only in this P2PE Solution (Solution-specific P2PE Application), verify all PTS POI device types the P2PE Application is used on are: • Confirmed per **1A-1.1** as a PTS-approved device(s) and associated with the P2PE Solution, either by satisfying the applicable requirements as part of this P2PE Solution assessment, or the requirements already being satisfied as part of a Validated P2PE Component being used by the P2PE Solution • Explicitly included in the P2PE Application assessment and denoted in the applicable P2PE Application P-ROV

Domain 4: Decryption Environment

Domain	Overview	P2PE Validation Requirements
Domain 4: **Decryption Environment**	The secure management of the environment that receives encrypted account data and decrypts it.	**4A** Use approved decryption devices. **4B** Secure the decryption environment. **4C** Monitor the decryption environment and respond to incidents. **4D** Implement secure, hybrid decryption processes. **4E** Component providers *ONLY*: report status to solution providers

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

Within a P2PE Solution, the decryption environment is where incoming encrypted account data is decrypted back to its original cleartext. This environment therefore consists of the secure cryptographic devices (and a Host System for hybrid environments) and cryptographic keys involved in the account-data decryption process. Requirements in Domain 4 entail securing all decryption systems and associated cryptographic keys, along with implementing monitoring and response procedures.

Within this domain, the term "solution provider" refers to whichever entity is undergoing the P2PE assessment. This may be a solution provider, a component provider, or a merchant as a solution provider (MMS). See "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" for more information about validating this Domain as a solution provider, a decryption-environment component provider, or as a merchant as a solution provider.

Note for hybrid decryption environments:

Hybrid decryption environments require HSMs for cryptographic key-management functions but allow for non-SCD Host Systems to be used for account-data decryption. Unlike a P2PE solution with a hardware decryption environment (in which cryptographic key management and account-data decryption are performed entirely within a hardware security module, or HSM), a hybrid decryption environment (which requires HSMs for cryptographic key-management functions) allows for the decryption of account data

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

Note: *All decryption devices, including HSMs and related key-management SCDs, must additionally meet all requirements specified in Domain 5.*

Note: *For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 4, and 5 of this document refers to merchant personnel in the encryption environments and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.*

outside of an HSM in non-SCDs on a Host System. These environments must meet all requirements specified in Domains 4 and 5, including the additional requirements specified in Section **4D** (as well as those specified in Domain 5 in section **5H**).

A Host System is defined as a combination of software and hardware components used to decrypt account data. May also be used for transaction processing using non-SCD host systems.

Requirement 4A: Use approved decryption devices	
Domain 4 Requirements	**Testing Procedures**
***4A-1** Use approved decryption devices*	
4A-1.1 All account-data decryption operations must be performed only by the FIPS-approved and/or PTS-approved HSMs identified in requirement 1-3.	**4A-1.1** Examine documented procedures and interview personnel to verify that all account-data decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified in **1-3.**
4A-1.1.1 [**Removed due to duplication with Requirement 1-4 in Domain 5**]	

Requirement 4A: Use approved decryption devices	
Domain 4 Requirements	**Testing Procedures**
4A-1.1.2 If FIPS-approved HSMs are used for account-data decryption and related processes, the HSM must use the FIPS-approved cryptographic primitives, data-protection mechanisms, and key-management processes for account-data decryption and related processes. ***Note:*** *Solution providers operating HSMs in non-FIPS mode or adding non-FIPS validated software must complete a written confirmation that includes the following:* • *Description of why the HSM is operated in non-FIPS mode* • *Purpose and description of any non-FIPS validated software added to the HSM* • *A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements* • *Note that adding any software may invalidate the FIPS approval.*	**4A-1.1.2.a** Examine FIPS approval documentation and HSM operational procedures to verify that the FIPS approval covers the cryptographic primitives, data-protection mechanisms, and key-management used for account-data decryption and related processes. **4A-1.1.2.b** If the HSM is operated in non-FIPS mode or non-FIPS validated software has been added to the HSM, review the solution provider's written confirmation and confirm that it includes the following: • Description of why the HSM is operated in non-FIPS mode • Purpose and description of any non-FIPs validated software added to the HSM • A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements
4A-1.1.3 If PCI PTS-approved HSMs are used for account-data decryption and related processes, the HSM must be configured to operate in accordance with the security policy that was included in the PTS HSM approval, for all P2PE operations (including algorithms, data protection, key management, etc.). ***Note:*** *PCI HSMs require that the decryption-device manufacturer make available a security policy document to end users, providing information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.*	**4A-1.1.3** Examine HSM configurations for all account-data decryption and related processes to verify that HSMs are configured to operate according to the security policy that was included as part of the PTS approval. In addition, examine the PCI approval listing(s) for any implementation-specific notes and if present, verify they are accounted for.

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
***4B-1** Maintain processes for securely managing the decryption environment.*	
4B-1.1 Current documentation must be maintained that describes or illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from PTS POI devices, all systems within the decryption environment, and any outbound connections.	**4B-1.1.a** Examine documentation to verify that a procedure exists to maintain a document that describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.
	4B-1.1.b Interview responsible personnel and examine documentation to verify that it describes/illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from PTS POI devices, all systems within the decryption environment, and any outbound connections.
4B-1.2 Procedures must be implemented to provide secure administration of decryption devices by authorized personnel, including but not limited to: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of the user interface • Password/smart card management • Console and non-console administration • Access to physical keys • Use of HSM commands *(continued on next page)*	**4B-1.2.a** Examine documented procedures to verify secure administration by authorized personnel is defined for decryption devices including: • Assigning administrative roles and responsibilities only to specific, authorized personnel • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands
	4B-1.2.b Observe authorized personnel performing device-administration operations to verify secure administration procedures are implemented for the following: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
4B-1.2 *(continued)*	**4B-1.2.c** Observe personnel performing decryption-device administration and examine files/records that assign administrative roles and responsibilities to verify that only authorized and assigned personnel perform decryption-device administration operations.
4B-1.3 Only authorized users/processes have the ability to make function calls to the HSM—e.g., via the HSM's application program interfaces (APIs). ***Note:*** *For example, require authentication for use of the HSMs APIs and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate use of the API, limit the exposure of the HSM to a trusted host via a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (e.g., high-speed serial or dedicated Ethernet).*	**4B-1.3.a** Examine documented procedures and processes to verify that only authorized users/processes have the ability to make functions calls to the HSM—e.g., via the HSM's application program interfaces (APIs). **4B-1.3.b** Interview responsible personnel and observe HSM system configurations and processes to verify that only authorized users/processes have the ability to make function calls to the HSM (e.g., via the HSM's application program interfaces [APIs]).
4B-1.4 PTS POI devices used in the merchant environment for account data acceptance and encryption must be authenticated by the decryption environment and upon request by the solution provider. ***Note:*** *The intent is to ensure the decryption environment can authenticate each unique PTS POI device within a P2PE solution with which it is communicating.* This authentication may occur via use of cryptographic keys or certificates, uniquely associated with each PTS POI device and decryption system.	**4B-1.4.a** Examine documented policies and procedures to verify they require PTS POI devices be authenticated upon connection to the decryption environment and upon request by the solution provider. **4B-1.4.b** Examine documented procedures are defined for the following: • Procedures and/or mechanisms for authenticating PTS POI devices by the decryption environment • Procedures and/or mechanisms for authenticating PTS POI devices upon request by the solution provider **4B-1.4.c** Interview responsible personnel and observe a sample of device authentications to verify the following: • PTS POI devices are authenticated by the decryption environment. • PTS POI devices are authenticated upon request by the solution provider.

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
4B-1.5 Processes for inspections of HSMs used for decryption operations and related processes must be: • Capable of detecting tampering or modification • Conducted by authorized personnel • Conducted at least quarterly	**4B-1.5.a** Examine documented procedures, interview personnel, and observe inspections (as needed) to verify: • Inspections performed are capable of detecting tampering or modification of HSMs used for decryption operations and related processes • Inspections are performed by authorized personnel • Inspections are performed at least quarterly
	4B-1.5.b [Removed]
	4B-1.5.c [Removed]
4B-1.6 Decryption environment must be secured according to PCI DSS. ***Note:*** *For merchant-managed solutions, PCI DSS validation of the decryption environment is managed by the merchant in accordance with their acquirer and/or payment brand. This requirement is therefore not applicable to P2PE assessments where merchants are the P2PE solution provider.* ***Note:*** *The P2PE Assessor should NOT challenge or re-evaluate the PCI DSS environment (or its compliance) where a completed and current ROC exists.*	**4B-1.6.a** Examine the current PCI DSS Report on Compliance (ROC) to verify the PCI DSS assessment scope fully covers the P2PE decryption environment.
	4B-1.6.b Examine the PCI DSS ROC and/or AOC to verify that all applicable PCI DSS requirements are "in place" for the P2PE decryption environment.
	4B-1.6.c Examine the PCI DSS ROC and/or AOC to verify that the PCI DSS assessment of the P2PE decryption environment was: • Performed by a QSA • Performed within the previous 12 months

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
4B-1.7 Processes must be implemented to ensure that cleartext account data is never sent back to the encryption environment. ***Note:*** *Output of cleartext data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process when it occurs from the decryption environment is assessed at Requirement* ***4B-1.9.***	**4B-1.7.a** Examine documented processes and interview personnel to confirm that cleartext account data is never sent back to the encryption environment. **4B-1.7.b** Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends cleartext account data back into the encryption environment.
4B-1.8 If the decryption environment allows for truncated PANs to be sent back to the encryption environment, they must adhere to the allowable number of digits. ***Note:*** *Refer to the PCI P2PE Technical FAQs - Domain 2, Q3 regarding the allowable number of digits.*	**4B-1.8.a** Examine documented processes and interview personnel to confirm that any truncated PANs sent back to the encryption environment adhere to the allowable number of digits. **4B-1.8.b** Observe process flows and data flows to verify that there is no process, application, or other mechanism that sends more digits of truncated PANs back to the encryption environment than is permitted.

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
4B-1.9 If whitelisting functionality is implemented in the decryption environment *that transmits data to the encryption environment, it* must be ensured that the *ONLY* allowed output of cleartext account data is for non-PCI payment brand account/card data, and includes the following: • Cryptographic signing (or similar) prior to installation by authorized personnel using dual control • Cryptographic authentication by the HSM • Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data • Approval of functionality by authorized personnel prior to implementation • Documentation for all new installations or updates to whitelist functionality that includes the following: – Description and justification for the functionality – Who approved the new installation or updated functionality prior to release – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data	**4B-1.9.a** Examine documented policies and procedures to verify that that any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* ensures that the *ONLY* allowed output of cleartext account data is for non-PCI payment brand account/card data, and includes the following: • Cryptographic signing (or similar) prior to installation by authorized personnel using dual control. • Cryptographic authentication by the HSM • Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data. • Approval of functionality by authorized personnel prior to implementation • Documentation for all new installations or updates to whitelist functionality that includes the following: – Description and justification for the functionality – Who approved the new installation or updated functionality prior to release – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data
	4B-1.9.b Observe application and system configurations and interview personnel to verify that whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* only allows the output of cleartext account data for non-PCI payment brand account/card data.
	4B-1.9.c Perform test transactions to verify that any whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* only allows output cleartext account for non-PCI payment brand account/card data.
4B-1.9.1 [Accounted for via 4B-1.9]	

Requirement 4B: Secure the decryption environment	
Domain 4 Requirements	**Testing Procedures**
4B-1.9.2 If whitelisting is supported, new installations of, or updates to, whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must be: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM	**4B-1.9.2** Observe the process for new installations or updates to whitelisting functionality and interview personnel to verify that additions or updates to whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* are performed as follows: • Cryptographically signed (or similar) prior to installation only by authorized personnel using dual control • Cryptographically authenticated by the HSM
4B-1.9.3 If whitelisting is supported, new installations of, or updates to, whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment* must follow change-control procedures that include: • Coverage for both new installations and updates to such functionality • Description and justification for the functionality • Who approved the new installation or update prior to release • Confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.	**4B-1.9.3** Examine records of both new and updated whitelisting functionality implemented in the decryption environment *that transmits data to the encryption environment*, and confirm the following: • Both new installations and updates to whitelisting functionality are documented. • The documentation includes description and justification. • The documentation includes who approved it prior to implementation. • The documentation includes confirmation that it was reviewed prior to release to only output non-PCI payment account/card data.

Requirement 4C: Monitor the decryption environment and respond to incidents	
Domain 4 Requirements	**Testing Procedures**
4C-1 *Perform logging and monitor the decryption environment for suspicious activity and implement notification processes.*	
4C-1.1 Changes to the critical functions of the decryption devices must be logged. Logs must be kept for one year, at a minimum. ***Note:*** *Critical functions include* ***but are not limited to*** *application and firmware updates, cryptographic-related functions, as well as changes to security-sensitive configurations/settings.*	**4C-1.1** Examine system configurations and correlating log files to verify that any changes to the critical functions of decryption devices are logged, including (but limited to): • Changes to the applications • Changes to the firmware • Changes to cryptographic-related functions • Changes to any security-sensitive configurations/settings
4C-1.2 Mechanisms must be implemented to detect and respond to suspicious activity, including but not limited to: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices	**4C-1.2.a** Examine documented procedures to verify mechanisms are defined to detect and respond to potential security incidents, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (e.g., configurations, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API

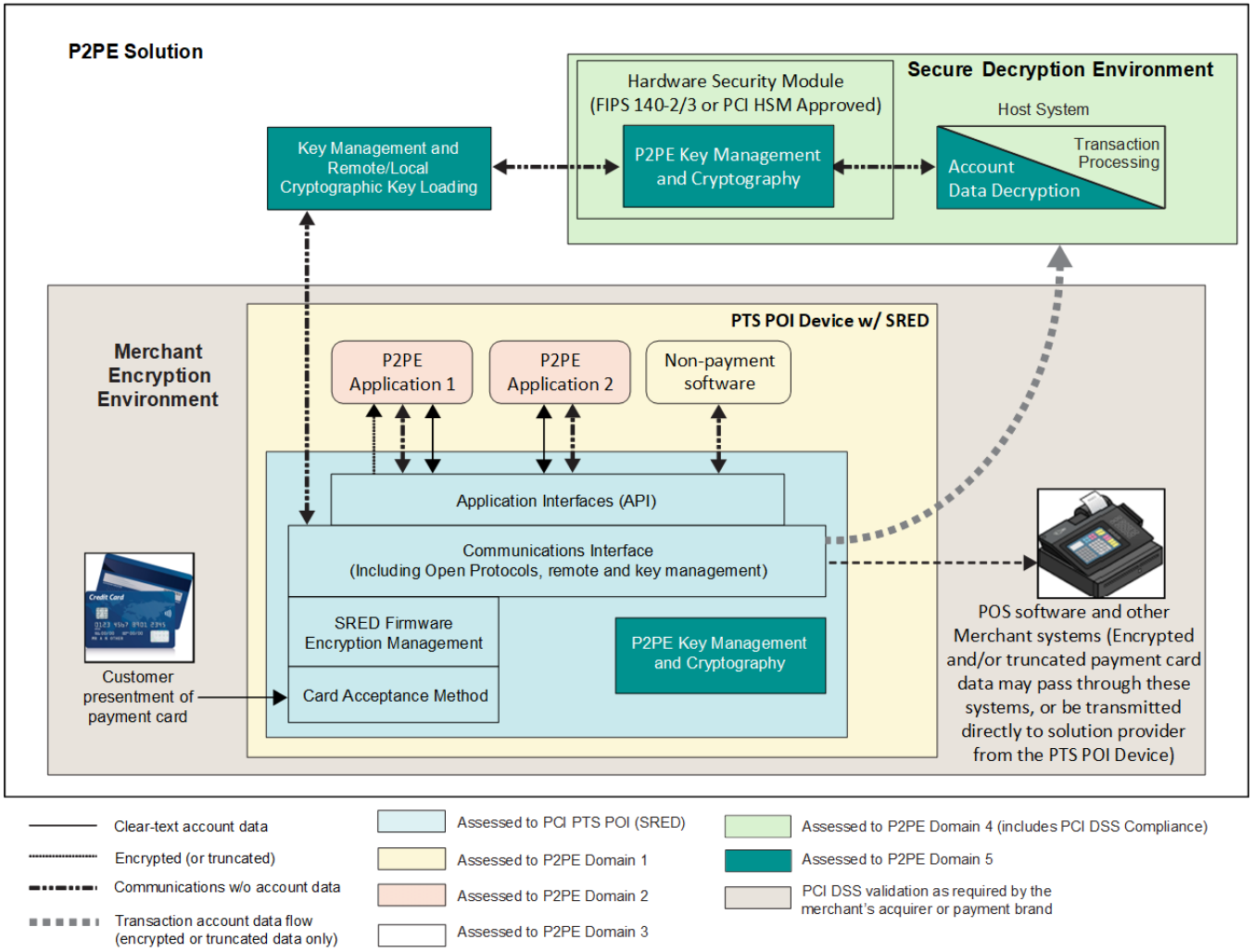
Requirement 4C: Monitor the decryption environment and respond to incidents	
Domain 4 Requirements	**Testing Procedures**
• Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API	**4C-1.2.b** Interview personnel and observe implemented mechanisms to verify mechanisms are implemented to detect and respond to suspicious activity, including: • Physical breach • Tampered, missing, or substituted devices • Unauthorized logical alterations (configuration, access controls) • Unauthorized use of sensitive functions (e.g., key-management functions) • Disconnect/reconnect of devices • Failure of any device security control • Encryption/decryption failures • Unauthorized use of the HSM API
4C-1.3 Mechanisms must be implemented to detect encryption failures, including at least the following: ***Note:*** *Although Domain 4 is concerned with the decryption environment, not the encryption environment, all traffic received into the decryption environment must be actively monitored to confirm that the POI devices in the merchant's encryption environment is not outputting cleartext account data through some error or misconfiguration.*	**4C-1.3** Examine documented procedures to verify controls are defined for the following: • Procedures are defined to detect encryption failures and include **4C-1.3.1** through **4C-1.3.3** below. • Procedures include immediate notification upon detection of a cryptographic failure, for each **4C-1.3.1** through **4C-1.3.3** below.
4C-1.3.1 Checking for incoming cleartext account data.	**4C-1.3.1.a** Observe implemented processes to verify controls are in place to check for incoming cleartext account data.
	4C-1.3.1.b Observe implemented controls and notification mechanisms to verify mechanisms detect and provide immediate notification upon detection of incoming cleartext account data.
	4C-1.3.1.c Interview personnel to verify that designated personnel are immediately notified upon detection of incoming cleartext account data.
4C-1.3.2 Detecting and reviewing any cryptographic errors reported by the HSM.	**4C-1.3.2.a** Observe implemented processes to verify controls are in place to detect and review any cryptographic errors reported by the HSM.

Requirement 4C: Monitor the decryption environment and respond to incidents	
Domain 4 Requirements	**Testing Procedures**
4C-1.3.2 *(continued)*	**4C-1.3.2.b** Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification of cryptographic errors reported by the HSM.
	4C-1.3.2.c Interview personnel to verify that designated personnel are immediately notified upon detection of cryptographic errors reported by the HSM.
4C-1.3.3 Detecting and reviewing any unexpected transaction data received. ***Note:*** *For example, transaction data received without an expected authentication data block (such as a MAC or signature, or a malformed message).*	**4C-1.3.3.a** Observe implemented processes to verify controls are in place to detect and review any unexpected transaction data received.
	4C-1.3.3.b Observe implemented controls and notification mechanisms to verify that mechanisms detect and provide immediate notification for any unexpected transaction data received.
	4C-1.3.3.c Interview personnel to verify that designated personnel are immediately notified upon detection of any unexpected transaction data received.
4C-1.3.4 [Requirement removed]	

Requirement 4C: Monitor the decryption environment and respond to incidents	
Domain 4 Requirements	**Testing Procedures**
4C-1.4 All suspicious activity must be identified and a record maintained for one year, at a minimum, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during any identified time that encryption was malfunctioning or disabled	**4C-1.4.a** Examine documented procedures to verify they include procedures for identifying the source and maintaining a record of all suspicious activity, to include at least the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled
	4C-1.4.b Observe implemented controls and interview responsible personnel to verify that the source of any suspicious activity is identified, and records are maintained to include the following: • Identification of affected device(s), including make, model, and serial number • Identification of affected merchant and specific sites/locations if applicable • Date/time of incident • Duration of device downtime • Date/time the issue was resolved • Details of whether any account data was transmitted from the POI device during the time that encryption was malfunctioning or disabled
4C-1.5 Implement mechanisms to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).	**4C-1.5.a** Examine documented procedures to verify mechanisms are defined to provide immediate notification of suspicious activity to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).
	4C-1.5.b Interview personnel and observe implemented mechanisms to verify that immediate notification of suspicious activity is provided to applicable parties, including merchants, processors, acquirers, and any P2PE solution providers (if decryption services are being performed on behalf of other P2PE solution providers).

At a Glance – Example P2PE Hybrid Decryption Implementation

Note: This diagram is for illustrative purposes only. Requirements 4D-x are ONLY for hybrid decryption environments.



Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
***4D-1** Configure the Host System securely.*	
4D-1.1 The solution provider must maintain current documentation that describes, or illustrates, the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.	**4D-1.1.a** Interview responsible personnel and examine 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.
	4D-1.1.b Interview responsible personnel and examine solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems within that environment, to verify that the document is current.
	4D-1.1.c Examine the solution provider documentation that describes/illustrates the configuration of the Host System, including the flow of data and interconnectivity between all systems, to verify that it accurately represents the decryption environment.
4D-1.2 The Host System must be isolated, or dedicated, to processing payment transactions with only necessary services, protocols, daemons, etc. enabled: • The necessary services, protocols, daemons, etc. must be documented and justified, including description of the enabled security features for these services etc. • Functions not related to transaction processing must be disabled, or isolated (e.g., using logical partitions), from transaction processing ***Note:** "Isolated" means that the Host System must not be accessed, modified or intercepted by other processes.*	**4D-1.2.a** Examine network and system configuration settings to verify the host processing system is isolated, or dedicated, to processing payment transactions, with only necessary services, protocols, daemons, etc. enabled.
	4D-1.2.b Examine 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.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-1.3 The Host System and HSM must, at a minimum: • Utilize a secure connection between them • Reside within the same CDE as defined in PCI DSS • Be dedicated to decryption operations and transaction processing in support of a P2PE Solution	**4D-1.3.a** Examine documentation / network diagrams to verify the Host System(s) and HSM(s), at a minimum, • Utilize a secure connection between them • Reside within the same CDE as defined in PCI DSS • Are dedicated to decryption operations and transaction processing in support of a P2PE Solution
	4D-1.3.b Examine and/or observe network and system configurations to verify 4D-1.3.a.
4D-1.4 All application software installed on the Host System must be authorized and have a business justification.	**4D-1.4.a** Examine documented policies and procedures to verify that all application software installed on the Host System must have a business justification and be duly authorized.
	4D-1.4.b Examine change-control and system-configuration records to verify that all application software installed on the Host System is authorized.
	4D-1.4.c Examine Host System and compare with system configuration standards to verify that all software installed on the Host System has a defined business justification.
4D-1.5 A process, either automated or manual, must be in place to prevent and/or detect and alert, any unauthorized changes to applications/software on the Host System.	**4D-1.5.a** Examine documented policies and procedures to verify that a process is defined to prevent and/or detect and alert of any unauthorized changes to applications/software.
	4D-1.5.b Interview personnel and observe system configurations to verify that controls are implemented to prevent and/or detect and alert personnel upon any unauthorized changes to applications/software.
	4D-1.5.c Examine output from the implemented process to verify that any unauthorized changes to applications/software are either prevented or detected with an alert generated that is immediately investigated.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-1.6 The Host System must perform a self-test when it is powered up to ensure its integrity before use. The self-test must include: • Testing integrity of cryptographic functions • Testing integrity of firmware • Testing integrity of any security functions critical to the secure operation of the Host System	**4D-1.6.a** Examine Host System configuration settings, and vendor/solution provider documentation to verify that the Host System performs a self-test when it is powered up to ensure its integrity before use. Verify the self-test includes the following: • Testing integrity of cryptographic functions • Testing integrity of software/firmware • Testing integrity of any security functions critical to the secure operation of the Host System
	4D-1.6.b Review logs/audit trails from when the Host System has previously been powered-up and interview personnel, to verify that the Host System performs a self-test to ensure its integrity before use. Verify the self-tests included the tests described in **4D-1.6.a**.
4D-1.7 The Host System must perform a self-test when a security-impacting function or operation is modified (e.g., an integrity check of the software/firmware must be performed upon loading of a software/firmware update).	**4D-1.7.a** Examine Host System configuration settings and vendor/solution provider documentation to verify that the Host System performs a self-test when a security-impacting function or operation is modified.
	4D-1.7.b Interview personnel and examine logs/records for when a security-impacting function, or operation, has been modified to verify that the Host System performs a self-test.
4D-1.8 The Host System must enter an error state and generate an alert upon any of the following events: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **4D-1.6** and **4D-1.7** • Failure of a security function or mechanism ***Note:*** *An "error state" identifies the Host System has encountered an issue that requires a response action. To prevent potential damage or compromise, the system must cease cryptographic operations until the issue is resolved, and the host is returned to a normal processing state.*	**4D-1.8.a** Examine Host System configuration settings and documentation to verify that the host enters an error state and generates an alert in the event of the following: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **4D-1.6** and **4D-1.7** • Failure of a security function or mechanism
	4D-1.8.b Interview personnel and examine logs/records of actual or test alerts to verify that alerts are generated and received when the Host System enters an error state under one of the following conditions: • Failure of a cryptographic operation • Failure of a system self-test, as described in Requirements **4D-1.6** and **4D-1.7** • Failure of a security function or mechanism

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-1.9 Alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.	**4D-1.9.a** Examine documented procedures to verify alerts generated from the Host System are documented and result in notification to authorized personnel and initiate a response procedure.
	4D-1.9.b Examine system configurations and records of documented alert events to verify alerts generated from the Host System are documented.
	4D-1.9.c Examine a sample of documented alert events and interview personnel assigned with security-response duties to verify alerts initiate a response procedure.
4D-1.10 The Host System must not perform any cryptographic operations under any of the following conditions: • While in an error state, as described in Requirement **4D-1.8** • During self-tests, as described in Requirements **4D-1.6** and **4D-1.7** • During diagnostics of cryptographic operations	**4D-1.10.a** Examine documented procedures to verify that controls/processes are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement **4D-1.8** • During self-tests, as described in Requirements **4D-1.6** and **4D-1.7** • During diagnostics of cryptographic operations
	4D-1.10.b Examine Host System configuration settings and interview personnel to verify that controls and/or procedures are in place to ensure that the Host System does not perform any cryptographic operations: • While in an error state, as described in Requirement **4D-1.8** • During self-tests, as described in Requirements **4D-1.6** and **4D-1.7** • During diagnostics of cryptographic operations
4D-1.11 All source code and executable code for cryptographic software and firmware on the Host System must be protected from unauthorized disclosure and unauthorized modification.	**4D-1.11.a** Examine 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.
	4D-1.11.b Observe access controls for cryptographic software and firmware to verify that all source code and executable code is protected from unauthorized disclosure and unauthorized modification.
4D-1.12 The cleartext data-decryption keys must not be accessible to any processes or functions not directly required for decryption operations.	**4D-1.12.a** Examine documentation, including data-flow diagrams, to verify that cleartext decryption keys are not accessible to any processes or functions not directly required for decryption operations.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-1.12 (*continued*)	**4D-1.12.b** Examine Host System configurations and access controls and to verify that cleartext decryption keys are not accessible to any processes or functions not directly required for decryption operations.
4D-1.13 The cleartext data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys.	**4D-1.13.a** Examine documented key-management policies and procedures to verify cleartext data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys.
	4D-1.13.b Examine Host System configuration settings and verify that cleartext data-decryption keys are only accessible to authorized personnel with a defined job-related need to access the keys.
4D-1.14 The Host System must not write cleartext cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory "swap/page" file purposes • "Core dumps" of memory required for troubleshooting In the above circumstances, the following conditions apply:	**4D-1.14.a** Examine documented configuration procedures to verify that the Host System must not write cleartext cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following: • Memory swap/page file purposes • Core dumps of memory required for troubleshooting
	4D-1.14.b Examine Host System configuration settings and interview personnel to verify that cleartext cryptographic keys are not written to persistent storage except in the following circumstances: • Memory swap/page file purposes • Core dumps of memory required for troubleshooting
	4D-1.14.c Examine documented procedures to verify they include Requirements **4D-1.14.1** through **4D-1.14.5** below.
4D-1.14.1 The locations must be predefined and documented.	**4D-1.14.1.a** Examine Host System configuration standards to verify that storage locations of any swap/page files and core dumps are defined.
	4D-1.14.1.b Examine Host System configuration settings to verify that the Host System only outputs swap/page files and core dumps to the documented storage locations.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-1.14.2 Storage must only be made to a dedicated hard drive (on its own bus) within the host.	**4D-1.14.2** Examine Host System configuration settings and storage locations to verify that swap/page files and core dumps are written to a dedicated hard drive on its own bus on the Host System.
4D-1.14.3 The swap/page files and/or core dumps must never be backed up or copied.	**4D-1.14.3.a** Examine backup configuration settings for the Host System and storage locations to verify that swap/page files and core dumps are not backed up.
	4D-1.14.3.b Examine the configurations of storage locations to verify that swap/page files and core dumps cannot be copied off the storage locations.
4D-1.14.4 Access to, and the use of, any tools used for troubleshooting or forensics must be controlled and authorized by management.	**4D-1.14.4.a** Examine documented procedures to verify that controls are defined to ensure that the access to, and use of, any tools used for troubleshooting or forensics, are controlled and authorized by management.
	4D-1.14.4.b Observe the process for accessing the tools used for troubleshooting or forensics and verify that they are controlled and authorized by management in accordance with the documented procedure.
	4D-1.14.4.c Observe the process for using the tools used for troubleshooting or forensics and verify that they are controlled and authorized by management in accordance with the documented procedure.
4D-1.14.5 All files must be securely deleted in accordance with industry-accepted standards for secure deletion of data: • Core dumps must be securely deleted immediately after analysis. • Memory swap/page files must be securely deleted upon system shut down or reset.	**4D-1.14.5.a** Examine 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.
	4D-1.14.5.b Test, 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.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
***4D-2** Access controls for the Host System are configured securely.*	
4D-2.1 Host user passwords must be changed at least every 30 days. ***Note:** This requirement applies to all user roles associated to persons with access to the Host System.*	**4D-2.1.a** Examine documented policies and procedures to verify that the Host System (s) user passwords must be changed at least every 30 days. **4D-2.1.b** Examine Host System configuration settings to verify that user password parameters are set to require users to change passwords at least every 30 days.
4D-2.2 User passwords must meet the following: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity. ***Note:** For information on variability and equivalency of password strength/complexity (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.).*	**4D-2.2.a** Examine documented policies and procedures to verify that user passwords must: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity. **4D-2.2.b** Examine Host System (s) configuration settings to verify that user passwords: • Consist of eight characters in length, • Consist of a combination of numeric, alphabetic, and special characters, or • Have equivalent strength/complexity.
4D-2.3 If log-on security tokens (e.g., smart cards) are used to access the Host System, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage. The PIN or password/passphrase must be at least ten alphanumeric characters in length, or equivalent.	**4D-2.3.a** If log-on security tokens are used, observe the security tokens in use to verify that they have an associated usage-authentication mechanism, such as a biometric or associated PIN or password/passphrase to enable their usage. **4D-2.3.b** Examine token-configuration settings to verify parameters are set to require that PINs or password/passphrases be at least ten alphanumeric characters in length, or equivalent.
4D-2.4 User accounts must be locked out of the Host System after not more than five failed attempts.	**4D-2.4.a** Examine documented policies and procedures to verify that authentication parameters on the Host System must be set to require that a user's account be locked out after not more than five invalid logon attempts. **4D-2.4.b** Examine Host System configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon attempts.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-2.5 The Host System must enforce role-based access control to include, at a minimum, the following roles: • Host System operator role – for day-to-day non-sensitive operations of the Host System • Host System administrator role – configuration of host OS, security controls, software and user accounts • Cryptographic administrator role – configuration of cryptographic management functions • Host System security role – auditing of host functions	**4D-2.5.a** Examine documented access-control procedures to verify they define, 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
	4D-2.5.b Examine the Host System configuration settings to verify that role-based access control is enforced and the following roles, at a minimum, 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
	4D-2.5.c Interview a sample of users for each role to verify the assigned role is appropriate for their job function.
4D-2.6 The segregation of duties must be enforced between roles, through automated or manual processes, to ensure that no one person is able to control end-to-end processes; or be in a position to compromise the security of the Host System. The following conditions must be applied:	
4D-2.6.1 A Host System user must not be permitted to audit their own activity on the Host System.	**4D-2.6.1.a** Examine documented procedures to verify that a Host System user is not permitted to audit their own activity on the Host System.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-2.6.1 *(continued)*	**4D-2.6.1.b** Interview audit personnel to verify that a Host System user is not permitted to audit their own activity on the Host System.
4D-2.6.2 A Host System administrator must use their operator-level account when performing non-administrative functions.	**4D-2.6.2.a** Examine documented policies and procedures to verify a Host System administrator is not permitted to use their administrative-level account when performing non-administrative functions.
	4D-2.6.2.b Interview and observe a Host System administrator to verify they use their operator-level account when performing non-administrative functions.
4D-2.7 Changes to a Host System user's account access privileges must be managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.	**4D-2.7.a** Examine documented policies and procedures to verify that changes to a user's access privileges are managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.
	4D-2.7.b Observe the process required to change a user's access privileges and verify that it is managed: • Using a formal change-control procedure. • Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own. • Ensuring all changes to access privileges result in an audit log.
	4D-2.7.c Examine 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.
4D-2.8 All physical and logical access privileges must be reviewed at least quarterly to ensure that personnel with access to the decryption environment, the Host System and Host System software require that access for their position and job function.	**4D-2.8.a** Examine documented policies and procedures to verify that access privileges are reviewed, 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.
	4D-2.8.b Examine records and interview personnel to verify that access privileges are reviewed, as a minimum, on a quarterly basis.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-2.9 Tamper detection mechanisms must be implemented on the host, to include an alert generation upon opening of the Host System case, covers and/or doors.	**4D-2.9.a** Examine Host System documentation to verify that tamper detection mechanisms are defined for the Host System, including the generation of an alert upon opening of the Host System case, covers and/or doors.
	4D-2.9.b Observe tamper-detection mechanisms on the Host System to verify that a tamper detection mechanism is implemented and includes the generation of an alert upon opening of the Host System case, covers and/or doors.
	4D-2.9.c Examine records of alerts and interview personnel to verify an alert is generated upon opening of the Host System, covers and/or doors.
4D-3 *Non-console access to the Host System is configured securely.*	
Note: *The term "non-console access" refers to any authorized access to the Host System that is performed by a person who is not physically present at the host processing system located within the secure room.*	
4D-3.1 All non-console access to the Host System must use strong cryptography and security protocols	**4D-3.1.a** For a sample of systems that are authorized to connect to the Host System via a non-console connection, examine configuration settings to verify that access to the Host System is provided through the use of strong cryptography and security protocols.
	4D-3.1.b Examine the configuration settings of system components to verify that all traffic transmitted over the secure channel uses strong cryptography.
4D-3.2 Non-console access to the Host System must not provide access to any other service, or channel, outside of that used to connect to the Host, e.g., "split tunneling."	**4D-3.2.a** Examine the configuration settings of the secure channel, to verify that split tunneling is prohibited.
	4D-3.2.b Observe a Host System administrator log on to the device which provides non-console access to the Host System to verify that split tunneling is prohibited.
4D-3.3 All non-console access to the Host System must use multi-factor authentication.	**4D-3.3.a** Inspect the configuration settings of the Host System and/or the device permitted to connect to the Host System to verify that multi-factor authentication is required for non-console access to the Host System.
	4D-3.3.b Observe a Host System administrator log on to the device that provides non-console access to the Host System to verify that multi-factor authentication is required.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-3.4 Non-console connections to the Host System must only be permitted from authorized systems.	**4D-3.4.a** Examine documented policies and procedures to verify that a process is defined to authorize systems for non-console access and not permit access until such times that authorization has been granted.
	4D-3.4.b For a sample of systems, examine device configurations to verify that non-console access is permitted only from the authorized systems.
4D-3.5 Non-console access to the Host System must only be permitted directly from within a PCI DSS compliant environment.	**4D-3.5** Examine, Interview, Observe, and/or test as needed to verify that non-console access to the Host System is only permitted from a PCI DSS compliant environment, including **4D-3.5.1** through **4D-3.5.2**
4D-3.5.1 The authorized system (e.g., workstation) from which non-console access originates must meet all applicable PCI DSS requirements. For example, system hardening, patching, anti-virus protection, a local firewall etc.	**4D-3.5.1** Examine 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.
4D-3.5.2 The network/system that facilitates non-console access to the Host System must: • Originate from and be managed by the solution provider • Meet all applicable PCI DSS requirements	**4D-3.5.2** Examine 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.
4D-3.6 Users with access to non-console connections to the Host System must be authorized to use non-console connections.	**4D-3.6.a** Examine documented policies and procedures to verify that non-console access to the Host System must only be provided to authorized users.
	4D-3.6.b Examine a sample of access-control records and compare them to Host System settings to verify that non-console access to the Host System is only provided to authorized users.
4D-3.7 Non-console sessions to the Host System must be terminated by the Host after 15 minutes of inactivity.	**4D-3.7.a** Examine documented policies and procedures to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.
	4D-3.7.b Examine the system configuration settings to verify that the system parameters are set to terminate non-console sessions after 15 minutes of inactivity.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4 *The physical environment of the Host System is secured.*	
Note: *Where "secure room" is referred to in this section, these controls can be met at* ***room level, rack level, or a combination of both****. Whichever way the requirements are applied, they should ensure that access the Host System is appropriately secured, whether in a secure room or a secure rack. For example, access to systems in a rack should be limited to those with a direct need to access that rack.*	
4D-4.1 The Host System must be located within a physically secure room that is dedicated to decryption operations and transaction processing.	**4D-4.1** Observe the physically secure room where the Host System is located and interview personnel to verify that all systems therein are designated to decryption operations and transaction processing.
4D-4.2 All individuals must be identified and authenticated before being granted access to the secure room—e.g., badge-control system, biometrics.	**4D-4.2.a** Examine documented policies and procedures to verify that all individuals must be identified and authenticated before being granted access to the secure room.
	4D-4.2.b Examine physical access controls to verify that all individuals are identified and authenticated before being granted access to the secure room.
	4D-4.2.c Observe authorized personnel entering the secure room to verify that all individuals are identified and authenticated before being granted access.
4D-4.3 All physical access to the secure room must be monitored and logs must be maintained as follows: • Logs must be retained for a minimum of three years. • Logs must be regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein. • Log reviews must be documented. • Logs must include but not be limited to: – Logs of access to the room from a badge access system – Logs of access to the room from a manual sign-in sheet *(continued on next page)*	**4D-4.3.a** Examine documented policies and procedures to verify all physical access to the secure room must be monitored and logs must be maintained. Policies and procedures must require the following: • Logs are retained for a minimum of three years. • Logs are regularly reviewed by an authorized person who does not have access to the secure room or to the systems therein. • Log reviews are documented. • Logs include at a minimum: – Access to the room from a badge access system – Access to the room from a manual sign-in sheet

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4.3 *(continued)*	**4D-4.3.b** Examine a sample of logs used to record physical access to the secure room to verify the following: • Logs are being retained for a minimum of three years. • Logs include at a minimum: – Access to the room from a badge access system – Access to the room from a manual sign-in sheet
	4D-4.3.c Interview personnel responsible for reviewing logs used to record physical access to the secure room to verify the following: • Logs are regularly reviewed. • Log reviews are documented. • The person performing the review does not have access to the secure room or to the systems therein.
4D-4.4 Dual access must be required for the secure room housing the Host System.	**4D-4.4.a** Examine physical access controls to verify that dual access is enforced.
	4D-4.4.b Observe authorized personnel entering the secure room to verify that dual access is enforced.
4D-4.5 Physical access must be only permitted to designated personnel with defined business needs and duties.	**4D-4.5.a** Examine documented policies and procedures to verify that physical access to the secure room is only permitted to designated personnel with defined business needs and duties.
	4D-4.5.b Examine the list of designated personnel and interview responsible personnel to verify that only personnel with defined business needs and duties are permitted access to the secure room.
	4D-4.5.c Examine physical access controls to verify that physical access to the secure room is only permitted to pre-designated personnel with defined business needs and duties.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4.6 The secure room must be monitored via CCTV on a 24-hour basis. This must include, as a minimum, the following areas: • All entrances and exits • Access to the Host System and HSM(s)	**4D-4.6.a** Examine 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)
Note: *Motion-activated systems that are separate from the intrusion-detection system may be used.*	**4D-4.6.b** If CCTV is motion-activated, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.
4D-4.7 Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.	**4D-4.7** Observe CCTV camera positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any computer screens, PIN pads, keyboards, or other systems that may expose sensitive data.
4D-4.8 CCTV recorded images must be securely archived for at least 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**4D-4.8.a** Examine a sample of recordings to verify that at least the most recent 45 days of images are securely archived.
	4D-4.8.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.
4D-4.9 Personnel with access to the secure room must not have access to the media (e.g., VCR tapes, digital recording systems, etc.) with the recorded surveillance data.	**4D-4.9.a** Examine documented access policies and procedures to verify that personnel with access to the secure room are not permitted to have access to the media containing recorded surveillance data for that environment.
	4D-4.9.b Examine access lists for the secure room as well as access controls to the media containing surveillance data, to verify that personnel with access to the secure room do not have access to the media containing recorded surveillance data.
4D-4.10 Continuous or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (e.g., when infrared cameras are used).*	**4D-4.10.a** Observe the secure room to verify that continuous or motion-activated lighting is provided for the cameras monitoring the secure room.
	4D-4.10.b Examine a sample of recorded CCTV images to verify that appropriate lighting is provided when persons are present in the secure room.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4.11 A 24/7 physical intrusion-detection system must be in place for the secure room (e.g., motion detectors when unoccupied). This must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.	**4D-4.11.a** Examine security policies and procedures to verify they require: • Continuous (24/7) physical intrusion-detection monitoring of the secure room • The physical intrusion-detection must be connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.
	4D-4.11.b Observe the physical intrusion-detection system to verify that it: • Provides continuous (24/7) monitoring of the secure room • It is connected to the alarm system and automatically activated whenever all authorized personnel have exited the secure room.
4D-4.12 Any windows in the secure room must be locked, protected by alarmed sensors, or otherwise similarly secured.	**4D-4.12.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	4D-4.12.b Examine the configuration of window sensors to verify that the alarm mechanism is active.
4D-4.13 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**4D-4.13** Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
4D-4.14 Access-control and monitoring systems must be connected to an uninterruptible power source (UPS) to prevent outages.	**4D-4.14** Examine uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems are powered through the UPS.
4D-4.15 All alarm events must be logged.	**4D-4.15.a** Examine security policies and procedures to verify they require that all alarm events are logged.
	4D-4.15.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
4D-4.16 Documented alarm events must be signed off by an authorized person who was not involved in the event.	**4D-4.16.a** Examine security policies and procedures to verify alarm events must be signed off by an authorized person other than the individual who was involved in the event.
	4D-4.16.b For a sample of documented alarm events, interview personnel who signed off on the event to verify that person was not involved in the event.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4.17 Use of an emergency entry or exit mechanism must cause an alarm event.	**4D-4.17** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
4D-4.18 Authorized personnel must respond to all physical intrusion alarms within 30 minutes.	**4D-4.18.a** Examine documented policies and procedures to verify they define that all alarm events are responded to by authorized personnel within 30 minutes.
	4D-4.18.b Examine documented alarm events and interview personnel to verify alarm events were responded by authorized personnel within 30 minutes.
4D-4.19 A process for synchronizing the time and date stamps of the access-control, intrusion-detection and monitoring (camera) systems must be implemented. ***Note:*** *This may be done by either automated or manual mechanisms.*	**4D-4.19.a** Examine documented procedures to verify that mechanisms are defined for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems.
	4D-4.19.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	4D-4.19.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
4D-4.19.1 If a manual synchronization process is used, synchronization must occur at least quarterly, and documentation of the synchronization must be retained for at least a one-year period.	**4D-4.19.1.a** If a manual synchronization process is implemented, interview responsible personnel and examine records of synchronization to verify the mechanism is performed at least quarterly.
	4D-4.19.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.
4D-4.20 The entrance to the secure room must include a mechanism to ensure the door is not left open. ***Note:*** *For example:* *- A door that is contact monitored and fitted with automatic closing or locking devices.* *- An airlock entrance system.*	**4D-4.20** Observe authorized personnel entering the secure room to verify that a mechanism is in place to ensure the door is not left open.

Requirement 4D: Implement secure hybrid decryption process – Applicable for hybrid decryption environments only	
Domain 4 Requirements	**Testing Procedures**
4D-4.21 An audible alarm must sound if the entrance to the secure room remains open for more than 30 seconds.	**4D-4.21.a** Examine secure room entry mechanisms to verify that an audible alarm is configured to sound if the entrance remains open for more than 30 seconds.
	4D-4.21.b Observe authorized personnel entering the secure room and request the door is held open. Verify that an audible alarm sounds if the entrance remains open for more than 30 seconds.

Requirement 4E: Component providers ONLY: report status to solution providers	
Domain 4 Requirements	**Testing Procedures**
4E-1 For component providers of decryption-management services, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment for subsequent PCI listing of the component provider's decryption-management services. This section is not applicable to, and does not need to be completed by, P2PE solution providers (or merchants as solution providers) that include decryption-management functions in their P2PE solution assessment (whether those functions are performed by the solution provider or are outsourced to non-PCI listed third parties).*	
4E-1.1 Component Providers must track the status of the decryption-management service and provide reports to solution providers annually and upon significant changes, including at least the following: • Types/models of HSMs • Number of HSMs deployed and any change in numbers since the last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment (*continued on next page*)	**4E-1.1.a** Examine component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel to confirm that the following processes are documented and implemented: • Providing reports annually and upon significant changes • Types/models of HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per **4C-1.2**

Requirement 4E: Component providers ONLY: report status to solution providers	
Domain 4 Requirements	**Testing Procedures**
• Details of any suspicious activity that occurred, per **4C-1.2**	**4E-1.1.b** Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of HSMs • Number of HSMs deployed and description of any changes since last report • Date of last physical inspection of HSMs • Date/status of last PCI DSS assessment • Details of any suspicious activity that occurred, per **4C-1.2**
4E-1.2 Component Providers must manage and monitor changes to decryption-management services and notify solution providers upon occurrence of any of the following: • Addition and/or removal of HSM types • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status ***Note:*** *Adding or removing HSM types may require adherence to PCI SSC's process for P2PE Delta Changes. Please refer to the P2PE Program Guide for details about obligations when adding, changing, or removing elements of a P2PE solution.*	**4E-1.2.a** Examine component provider's documented procedures and interview responsible component-provider personnel, and confirm that processes include notifying the solution provider upon occurrence of the following: • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types
	4E-1.2.b Observe reports provided to applicable solution providers, and confirm at least the following are reported upon occurrence: • Critical infrastructure changes, including to the PCI DSS environment • Changes to PCI DSS compliance status • Additions and/or removal of HSM types

Domain 5: P2PE Cryptographic Key Operations and Device Management

Domain	Overview	P2PE Validation Requirements
Domain 5: **P2PE Cryptographic Key Operations and Device Management**	Establish and administer key-management operations for account-data encryption PTS POI devices and decryption HSMs.	**Control Objective 1** Account data is processed using equipment and methodologies that ensure they are kept secure. **Control Objective 2** Account-data keys and key-management methodologies are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys. **Control Objective 3** Keys are conveyed or transmitted in a secure manner. **Control Objective 4** Key loading is handled in a secure manner. **Control Objective 5** Keys are used in a manner that prevents or detects their unauthorized usage. **Control Objective 6** Keys are administered in a secure manner. **Control Objective 7** Equipment used to process account data and keys is managed in a secure manner. **5A** Account data is processed using algorithms and methodologies that ensure they are kept secure. **5H** For hybrid decryption solutions: Implement secure hybrid-key management. **5I** Component providers *ONLY*: report status to solution providers.

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

Overview

Domain 5 covers the requirements for the use of strong cryptographic keys and secure key-management functions for all account-data encryption PTS POI devices and decryption HSMs, including related key-management SCDs. Examples include PTS POI devices, HSMs, key-injection/loading devices (KLDs) and signing devices. Implementation of these procedures is fundamental to the security of a P2PE solution. Domain 5 includes detailed key-management procedures including encryption methodologies, key generation, key distribution, key loading, key usage, key administration, equipment management, and hybrid decryption-key management (for hybrid decryption solutions only).

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

Domain 5 requirements address secure cryptographic key-management operations for the encryption environment and the decryption environment, as well as environments performing symmetric-key distribution using asymmetric keys (remote key distribution), certification authority/registration authority and key-injection or key-generation.

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

Vendor-controlled secret and private keys used in connection with the following activities are also in scope:

- When used in connection with vendor-operated PKIs used for remote key loading using asymmetric techniques. This applies specifically to the distribution of acquirer keys to PTS POI devices for use of account-data encryption, whether the actual distribution of acquirer keys occurs from the transaction-processing host or is distributed directly by the vendor. This includes:
  - Root and Subordinate Certification Authority keys and keys used in connection with associated Registration Authority activities
  - Device-specific key pairs used for that purpose
  - Keys associated with protection of the aforementioned keys during storing, loading, and usage
  - The generation of the aforementioned keys
- When used in connection with KIF activities for loading and/or distribution of acquirer keys to PTS POI devices for use of account-data encryption.
- When used for the protection of account data when conveyed between non-integrated PCI-listed PTS POI devices—e.g., an SCR and a PIN pad.

Additionally, acquirer keys generated on behalf of the acquirer are in scope.

Symmetric-Key Distribution using Asymmetric Techniques

Domain 5 also contains requirements that apply to remote key-establishment and distribution applications. Remote key-distribution schemes can be used for initial key loading only—i.e., establishment of a TDEA key hierarchy, such as a terminal master key. Standard symmetric-key-exchange mechanisms should be used for subsequent TMK, DEK, or other symmetric-key exchanges, except where a device requires a new key initialization due to unforeseen loss of the existing TMK. Using asymmetric techniques for routine key exchange can result in unnecessary exposure to man-in-the-middle attacks and should not be used. These requirements pertain to two distinct areas:

Remote Key-Distribution Using Asymmetric Techniques Operations:

Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key-distribution using asymmetric techniques for the distribution of keys to PTS POI devices for use of account-data encryption. If the key loading is not performed remotely and authentication is provided by another method—such as properly implemented dual control and key-loading device(s)—even if these systems involve the use of certificates, the remote key-establishment and distribution applications requirements will not apply. "Remotely" means whenever the key-loading device and the PTS POI device are neither co-located nor connected via a direct mechanism, such as a cable. This includes:

- The distribution of symmetric keys using asymmetric techniques from a key-distribution host (KDH) to many key-receiving devices (KRDs—i.e., PTS POI devices); or
- The exchange of keys between peers, where one is administratively designated as the KDH and one as the KRD (e.g., the transaction processing host).

ANSI TR-34 presents a methodology that is compliant with these requirements. TR34 describes a method for transporting a symmetric key from one SCD to another over an uncontrolled channel. A typical example usage of TR34 would be to load individual initial symmetric transport keys from a Key Distribution Host (KDH) to a population of PEDs. TR34 makes use of asymmetric cryptography to protect this key transport, which means that both the Key-Distribution Host, and the Key-Receiving Devices (e.g., PEDs), must have appropriate credentials in the form of certificates, public and private keys, and must have a common relationship with a Certificate Authority (CA). The CA can be an independent party from both the Key-Receiving Device (KRD) vendor and the KDH, or the KRD vendor can be the CA.

Certification and Registration Authority Operations:

Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.

Certification Authority requirements apply to all entities (P2PE solution providers, P2PE component providers, and entities performing these functions on behalf of solution providers or component providers) signing public keys to be used for remote distribution of cryptographic keys, whether in X.509 certificate-based schemes or other designs, to allow for the required authentication of these signed public keys. For purposes of these requirements, a certificate is any digitally signed value containing a public key, where the term "digitally signed" refers to any cryptographic method used that enforces the integrity and authenticity of a block of data through the cryptographic processing of that block of data with a private key. The CA requirements apply only to methods that allow for the distribution and use of

such signed public keys to multiple systems, and as such do not apply to systems that apply symmetric cryptography to keys for authentication (such as through the use of MACs).

The Certification Authority requirements are not intended to be applied to devices that sign their own keys, nor to key-loading systems where the key loading is not performed remotely and authentication is provided by another method—such as properly implemented dual control and key-loading device(s)—even if these systems involve the use of certificates.

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

Key-Injection Facilities

The term key-injection facility (KIF) describes those entities that perform key injection of PTS POI devices used for account-data encryption and key injection of HSMs used for decryption. Key injection may be performed by the solution provider or by a third party such as a PTS POI terminal manufacturer or vendor. Domain 5 contains requirements that apply to key-injection facilities, or other entities that are performing KIF-related services for others, such as key generation or key loading.

Key-injection systems that allow cleartext secret and/or private keys and/or their components to appear in unprotected memory (e.g., within a computer and outside of the secure boundary of a secure cryptographic device) are inherently less secure. Any such systems are subject to additional controls as delineated in the criteria in this domain.

Note for hybrid decryption environments:

Hybrid decryption environments require HSMs for cryptographic key-management functions but allow for non-SCD Host Systems to be used for account-data decryption. Unlike a P2PE solution with a hardware decryption environment (in which cryptographic key management and account-data decryption are performed entirely within a hardware security module, or HSM), a hybrid decryption environment (which requires HSMs for cryptographic key-management functions) allows for the decryption of account data outside of an HSM in non-SCDs on a Host System. These environments must meet all requirements in Domains 4 and 5, including the additional requirements specified in section **5I** (as well as those specified in Domain 4 in section **4D**). See "P2PE Solutions and use of Third Parties and/or P2PE Component Providers" for more information about validating this Domain as a solution provider, key-management component provider, or merchant as a solution provider.

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

For merchant-managed solutions, the term "merchant" as used within Domains 1, 3, 4, and 5 of this document refers to merchant personnel in the encryption environments and represents requirements the merchant as a solution provider is responsible for meeting for, or on behalf of, those merchant encryption environments.

Definitions and Annex

For the purposes of this document:

- Secret Key = Symmetric key (also known as a shared secret key).
- Private Key = Asymmetric key used only for decryption operations or for creating digital signatures. No one private key should be used for both purposes (except for transaction-originating SCDs).
- Public Key = Asymmetric key used only for encryption operations or for verifying digital signatures. No one public key should be used for both purposes (except for transaction-originating SCDs). This annex provides the minimum and equivalent key sizes and strengths for the encryption of data and other cryptographic keys.

Note: *An essential part of maintaining the security of PTS POI devices and HSMs and the cryptographic keys used on those devices is for the solution provider to know where those devices and keys are—e.g., during key creation and loading onto devices, while being used at a merchant, when devices are undergoing repair, etc. Therefore, it is the responsibility of the entity managing devices and cryptographic keys to keep track of POI devices and HSMs from the point where the device is first added into the P2PE solution and has cryptographic keys loaded onto the device, until the disposal of that device or its removal from the solution.*

However, it is not the intent of these requirements that solution providers actively manage these devices when deployed at merchant encryption environments; the intent is that the solution provider maintains knowledge of the location and status of devices once deployed to merchants. Knowledge sharing and cross-cooperation may be necessary regarding the location and status of devices when different entities are responsible for managing devices and keys for different functions.

Control Objective 1: Account data is processed using equipment and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
Requirement 1: *Account data is processed in equipment that conforms to requirements for secure cryptographic devices (SCDs). Account data never appears in the clear outside of an SCD.*	
1-1 ***Not used in P2PE***	
1-2 Key-injection facilities must only inject keys into equipment that conforms to the requirements for SCDs.	**1-2** 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.
1-3 All hardware security modules (HSMs) must be either: • *FIPS 140-2* or *FIPS 140-3* Level 3 (overall) or higher certified, or • PCI PTS HSM approved ***Note 1:*** *HSM approval listings must be current—HSMs must have a non-expired PCI PTS HSM approval or a non-expired FIPS 140-2 or FIPS 140-3 certificate (i.e., the FIPS 140 HSM certificates must not be listed as historical or revoked).* ***Note 2:*** *PCI-approved HSMs may have their approvals restricted whereby the approval is valid only when the HSM is deployed in controlled environments or more robust (e.g., secure) environments as defined in ISO 13491-2 and in the device's PCI HSM Security Policy. This information is noted in the Additional Information column of approved PTS devices.* ***Note 3:*** *Key-injection platforms and systems must include hardware devices for managing (e.g., generating and storing) the keys that conform to the requirements for SCDs. This includes SCDs used in key-injection facilities (e.g., modified PEDs). A PED used for key injection must be validated and approved to the KLD approval class.*	**1-3** For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval) and the list of approved devices to verify that all HSMs are either: • Listed on the *NIST Cryptographic Module Validation Program* (CMVP) list, with a valid listing number, and approved to *FIPS 140-2* or *FIPS 140-3* Level 3 (overall), or higher. Refer to http://csrc.nist.gov. Or, • Listed on the PCI SSC website, with a valid PCI SSC reference number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.

Control Objective 1: Account data is processed using equipment and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
1-4 The approval listing must match the deployed devices in the following characteristics: • Vendor name • Model name and number • Hardware version number • Firmware version number • The PCI PTS HSM or *FIPS 140* Approval Number • For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment ***Note:*** *If the solution provider has applied a vendor security patch resulting in an updated HSM firmware version, and the PCI SSC or NIST acceptance of that updated firmware version has not yet been completed (resulting in a mismatch between the HSM firmware version in use and the listed, validated one), the solution provider must obtain documentation from the vendor regarding the update that includes confirmation the update has been submitted for evaluation per the process specified by either PCI SSC or NIST (as applicable to the HSM).*	**1-4.a** For all PCI-approved HSMs used, examine HSM devices and the *PCI SSC list of Approved PCI PTS Devices* to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The PCI PTS approval number • Any applications, including application version number, resident within the device which were included in the PTS assessment • Review the PCI approval listing(s) for any implementation-specific notes and if present, verify they are accounted for.
	1-4.b For all FIPS-approved HSMs used, examine HSM devices and review the *NIST Cryptographic Module Validation Program* (CMVP) list to verify that all of the following device characteristics match the *FIPS 140-2* or *FIPS 140-3* Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • The FIPS 140 Approval Number
	1-4.c If the solution provider has applied a vendor security patch that resulted in an updated HSM firmware version, and the PCI SSC or NIST acceptance of that updated firmware version has not yet been completed, obtain and examine the vendor documentation and verify it includes confirmation that the update has been submitted for evaluation per the process specified by PCI SSC or NIST (as applicable to the HSM).

Control Objective 1: Account data is processed using equipment and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
1-5 The KIF platform provider must: • Maintain current documentation that describes and/or illustrates the architecture of the KIF, including all KIF functionality. • Maintain documentation detailing the flow of keys from the key generation, through the functionality to the destination device.	**1-5.a** Interview personnel and examine documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the KIF.
	1-5.b Interview personnel and examine documentation that describes and/or illustrates the architecture of the KIF to verify that all KIF components, key-management flows, and personnel interaction with key-management flows are identified and documented.
	1-5.c Examine the key-management flows and interview personnel to verify: • Documentation shows all key-management flows across functions and networks from the point the key is generated through to the point the key is injected into the PTS POI device. • Documentation is kept current and updated as needed upon changes to the KIF architecture.
Note: *PIN requirements 2, 3, and 4 are all PIN-specific and are therefore omitted from P2PE.*	

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
Requirement 5: *All keys, key components, and key shares are generated using an approved random or pseudo-random function.*	
5-1 Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Generation of cryptographic keys or key components must occur within an SCD. They must be generated by one of the following: • An approved key-generation function of a PCI-approved HSM or PTS POI device • An approved key-generation function of a *FIPS 140-2 or FIPS 140-3* Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent laboratory to comply with *NIST SP800-22* ***Note:*** *Random number generation is critical to the security and integrity of all cryptographic systems. All*	**5-1.a** Examine key-management policy documentation to verify that it requires that all devices used to generate cryptographic keys meet one of the following: • An approved key-generation function of a PCI-approved HSM or PTS POI device • An approved key-generation function of a *FIPS 140-2 or FIPS 140-3* Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*. **5-1.b** Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys, or key components meet one of the following: • An approved key-generation function of a PCI–approved HSM or POI device • An approved key-generation function of a *FIPS 140-2 or FIPS 140-3* Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
cryptographic key generation relies upon good quality, randomly generated values.	**5-1.c** Examine procedures to be used for future generations and logs of past key generation to verify devices used for key-generation are those as noted above, including validation of firmware used.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
Requirement 6: *Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.*	
6-1 Implement security controls, including dual control and tamper detection, to prevent the unauthorized disclosure of keys or key components.	
6-1.1 Any cleartext output of the key-generation process must be managed under dual control. Only the assigned custodian can have direct access to the cleartext of any key component/share. Each custodian's access to cleartext output is limited to the individual component(s)/share(s) assigned to that custodian, and not the entire key.	**6-1.1.a** Examine documented procedures to verify the following. • Any key-generation process with cleartext output is performed under dual control • Any output of a cleartext component or share is overseen by only the assigned key custodian(s) for that component/share • Each custodian's access to cleartext output is limited to the individual component(s)/share(s) assigned to that custodian, and not the entire key.
	6-1.1.b Observe key-generation process demonstration and interview responsible personnel to verify: • Any key-generation process with cleartext output is performed under dual control. • Any output of cleartext component or share is overseen by only the assigned key custodian(s) for the component/share. • Each custodian's access to cleartext output is limited to the individual component(s)/share(s) assigned to that custodian and not the entire key.
6-1.2 There must be no point in the key-generation process where a single individual has the ability to determine, obtain, or ascertain any part of a cleartext key or all the components for a key.	**6-1.2.a** Examine documented procedures for all key-generation methods and observe demonstrations of the key-generation process from end-to-end to verify there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a cleartext key or all the components for a key.
Note: *Key shares derived using a recognized secret-sharing algorithm or full-length key components are not considered key parts and do not provide any information regarding the actual cryptographic key.*	**6-1.2.b** Examine key-generation logs to verify that: • The documented procedures were followed, and • At least two individuals performed the key-generation processes.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-1.3 Devices used for the generation of cleartext key components that are output in the clear must either be powered off when not in use or require re-authentication whenever key generation is invoked. Logically partitioned devices used concurrently for other processes—e.g., providing services simultaneously to host systems, such as for transaction processing—must have key-generation capabilities disabled when not in use and other activities are continuing.	**6-1.3** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate cleartext key components are powered off when not in use or require re-authentication whenever key generation is invoked; or, • If the device used for key generation is logically partitioned for concurrent use in other processes, the key-generation capabilities are enabled for execution of the procedure and disabled when the procedure is complete.
6-1.4 Key-generation equipment used for generation of cleartext key components must not show any signs of tampering (e.g., unknown cables) and must be inspected prior to the initialization of key-generation activities. Ensure there isn't any mechanism that might disclose a cleartext key or key component (e.g., a tapping device) between the key-generation device and the device or medium receiving the key or key component. ***Note:*** *This does not apply to logically partitioned devices located in data centers that are concurrently used for other purposes, such as transaction processing.*	**6-1.4.a** Examine documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering prior to use. Verify procedures include a validation step to ensure no unauthorized mechanism exists that might disclose a cleartext key or key component (e.g., a tapping device).
	6-1.4.b Observe key-generation set-up processes for all key types to verify that key-generation equipment is inspected prior to use, to ensure equipment does not show any signs of tampering. Verify procedures include a validation step to ensure no unauthorized mechanism exists that might disclose a cleartext key or key component (e.g., a tapping device).
6-1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the area during key-generation processes where cleartext keying material is in use. It must not be feasible to observe any cleartext keying material either directly or via camera monitoring.	**6-1.5.a** Examine documentation to verify that physical security controls (e.g., partitions or barriers) are defined to ensure the key component cannot be observed or accessed by unauthorized personnel.
	6-1.5.b During the demonstration for 6-1.1.b, observe the physical security controls (e.g., partitions or barriers) used, and validate that they ensure the key-generation process cannot be observed or accessed by unauthorized personnel directory or via camera monitoring (including those on cellular devices).

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-2 Multi-use/purpose computing systems must not be used for key generation where any cleartext secret key or private key, or key component thereof, appears in memory outside the tamper-protected boundary of an SCD. ***Note:*** *This requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices that do not have the ability to access cleartext cryptographic keys or components.* *Single-purpose computers with an installed SCD or a modified PED where clear keying material is injected*	**6-2.a** Examine documented procedures to verify that multi-purpose computing systems are not permitted for key generation where any cleartext secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD. **6-2.b** Observe the generation process and examine documentation for each type of key to verify that multi-purpose computing systems are not used for key generation where any cleartext secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD except where Requirement 5 and Requirement 13 are met.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
directly from a secure port on the key-generating SCD to the target (e.g., a POI device) meet this requirement. *SCDs used for key generation must meet* ***Requirement 5-1.***	**6-2.c** Where single-purpose computers with an installed SCD or a modified PED are used, examine, observe, and interview as needed to verify that: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device)
6-3 Printed key components must be protected against compromise. Key components must be printed in a way that prevents observation by any party other than the	**6-3.a** Examine documented procedures for printed key components and verify the requirement is satisfied.
	6-3.b Interview personnel and observe processes to verify the requirement is satisfied.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
approved key custodian(s) of those components. Key components transmitted electronically prior to printing must be secured during transmission, and the equipment used for the printing process must be secured to prevent compromise and storage of the components. Printers used for this purpose must not be used for other purposes, must not be networked (i.e., locally connected only), and must be managed under dual control. Location must be a secure room that meets the following requirements: ***Note:*** *This requirement includes manual (handwritten) capture.* The following sub-requirements are applicable to the printing of key components:	
6-3.1 The room must have walls made of solid materials. The walls do not have to extend from true floor to true ceiling but do need to extend from floor to ceiling.	**6-3.1** Observe the secure room designated for printing cleartext key components to verify that the walls are made of solid materials and extend from floor to ceiling.
6-3.2 Any windows into the secure room must be: • Locked and protected by alarmed sensors. • Covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**6-3.2.a** Observe all windows in the secure room to verify they are: • Locked and protected by alarmed sensors. • Covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
	6-3.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-3.3 An electronic access control system (for example, badge and/or biometrics) must be in place that: • Enforces dual-access (i.e., the presence of at least two individuals) requirements for entry into the secure room, and anti-pass-back requirements. • Supports generation of an alarm when one person remains alone in the secure room for more than 30 seconds.	**6-3.3.a** Observe authorized personnel entering the secure room to verify that a badge-control system is in place that enforces the following requirements: • Dual access for entry to the secure room • Anti-pass-back
	6-3.3.b Examine alarm mechanisms and interview alarm-response personnel to verify that the badge-control system supports generation of an alarm when one person remains alone in the secure room for more than 30 seconds.
6-3.4 CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be motion-activated, in which case the recording must continue for at least a minute after the last pixel of activity subsides.	**6-3.4** Examine the CCTV configuration and a sample of recordings to verify that CCTV monitoring includes the ability to record events during dark periods, and verify that, if motion-activated, recording continues for at least a minute after the last pixel of activity subsides.
6-3.5 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	**6-3.5** Examine 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.
6-3.6 The CCTV server and digital storage must be secured in a separate secure location that is not accessible to personnel who have access to the secure room.	**6-3.6.a** Observe the location of the CCTV server and digital storage to verify they are located in a secure location that is separate from the secure room.
	6-3.6.b Examine access-control configurations for the CCTV server/storage secure location and the key-injection secure room to identify all personnel who have access to each area. Compare access lists to verify that personnel with access to the secure room do not have access to the CCTV server/storage secure location.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-3.7 The CCTV cameras must be positioned to monitor: • The entrance door, • Any safes that are present, and • Any equipment that is used.	**6-3.7** Observe CCTV positioning and examine a sample of recordings to verify that CCTV cameras are positioned to monitor: • The entrance door, • Any safes that are present, and • Any equipment that is used.
6-3.8 CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.	**6-3.8** Observe CCTV positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.
6-3.9 Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**6-3.9.a** If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.
	6-3.9.b Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-4 Any residue that may contain cleartext keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual. ***Note:*** *Examples of where such key residue may exist include (but are not limited to):* • *Printing material, including ribbons and paper waste* • *Memory storage of a key-loading device, after loading the key to a different device or system* • *Other types of displaying or recording (e.g., printer memory, printer drum).*	**6-4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures ensure the following: • Any residue that may contain cleartext keys or components is destroyed or securely deleted immediately after generation. • Specific direction as to the method of destruction is included in the procedure. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device(s) that will use the key. Examine logs of past destructions and deletions to verify that procedures are followed.
	6-4.b Observe the destruction process of each identified type of key residue and verify the following: • Any residue that may contain cleartext keys or components is destroyed or securely deleted immediately after generation. • The method of destruction is consistent with Requirement 24. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device(s) that will use the key.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-5 Asymmetric-key pairs must either be: • Generated by the device that will use the key pair; or • If generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.	**6-5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (zeroized) immediately after the transfer to the device that will use the key pair.
	6-5.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (e.g., zeroized) immediately after the transfer to the device that will use the key pair.

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
6-6 Policy and procedures must exist to ensure that cleartext private or secret keys or their components/shares are not transmitted across insecure channels. Preclusions include but are not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying cleartext private or secret keys or components • Conveying cleartext private key shares or secret key components/shares without containing them within tamper-evident and authenticable packaging • Writing key or component values into startup instructions • Affixing (e.g., taping) key or component values to or inside devices • Writing key or component values in procedure manuals	**6-6.a** Examine documented policy and procedures to verify that they include language that prohibits transmitting cleartext private or secret keys or their components/shares across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying cleartext keys or components • Conveying cleartext private key shares or secret key components/shares without containing them within tamper-evident and authenticable packaging • Writing key or component values into startup instructions • Affixing key or component values to or inside devices • Writing key or component values in procedure manual
	6-6.b Observe key-management processes to verify that cleartext private or secret keys or their components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise electronically conveying cleartext keys or components • Conveying cleartext private or secret key components without containing them within tamper-evident, authenticable packaging • Writing key or component values into startup instructions • Affixing key or component values to or inside devices • Writing key or component values in procedure manual

Control Objective 2: Cryptographic keys used for account-data encryption/decryption and related key management are created using processes that ensure it is not possible to predict any key or determine that certain keys are more probable than other keys	
Domain 5 Requirements	**Testing Procedures**
Requirement 7: *Documented procedures must exist and must be demonstrably in use for all key-generation processes.*	
7-1 Written key-generation policies and procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of these procedures. Procedures for creating all keys must be documented.	**7-1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations and address all keys in scope.
	7-1.b Interview those responsible for the key-generation processes (including key custodians, supervisory staff, technical management, etc.) to verify that the documented procedures are known and understood by all affected parties.
	7-1.c Observe key-generation ceremonies, whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.
7-2 Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs. The minimum log contents include date and time, object name/identifier, purpose, name and signature of individual(s) involved, and tamper-evident package number(s) and serial number(s) of device(s) involved.	**7-2.a** Examine documented key-generation procedures to verify that key-generation events for higher-level keys (e.g., KEKs shared with other organizations or otherwise manually loaded as components and MFKs and BDKs) are logged.
	7-2.b Observe demonstrations for the generation of higher-level keys to verify that all key-generation events are logged.
	7-2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded and that all required elements were captured.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 8: *Secret or private keys must be transferred by:* *a) Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or* *b) Transmitting the key in ciphertext form.* *Public keys must be conveyed in a manner that protects their integrity and authenticity.* *It is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport.*	
Keys conveyed to *a key-injection facility (or applicable entity providing key-management services) must be conveyed in compliance with these requirements. Such keys can include,* ***but are not limited to****:* • *Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method;* • *Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf);* • *Terminal master keys (TMKs) used in the master key/session key key-management method;* • *PIN-encryption keys used in the fixed-transaction key method;* • *Public keys used in remote key-establishment and distribution applications;* • *Private asymmetric keys for use in remote key-loading systems.* • *HSM master keys (e.g., MFKs)* ***Keys conveyed from*** *a key-injection facility (including facilities that are device manufacturers) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:* • *Digitally signed HSM-authentication public key(s) signed by a device manufacturer's private key and subsequently loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable);* • *Device manufacturer's authentication key loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable).*	

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
8-1 Keys must be transferred either encrypted, as two or more full-length cleartext components, key shares, or within an SCD.	**8-1.a** Examine documentation and interview personnel (as needed) to determine whether keys are transmitted encrypted, as cleartext components/shares, and/or within an SCD. Carry out the additional testing procedures as applicable.
Cleartext key components/shares must be conveyed in SCDs or using tamper-evident, authenticable packaging. • If key components are transmitted in cleartext using pre-numbered, tamper-evident, authenticable mailers: – Components/shares must be conveyed using at least two separate communication channels, such as different courier services. Components/shares sufficient to form the key must not be conveyed using the same communication channel. – Details of the serial number of the package are conveyed separately from the package itself. – Documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material. *(continued on next page)*	**8-1.b** If key components are transmitted in cleartext using pre-numbered, tamper-evident, authenticable packaging, perform the following: • Examine documented procedures for sending components in tamper-evident, authenticable packaging to verify that: – They define how the details of the package serial number are to be transmitted. – There is a requirement that the package serial number is to be sent separately from the package itself. – Each component is to be sent to/from only the custodian(s) authorized for the component. – At least two communication channels are used to send the components of a given key (not just separation by sending on different days). – Prior to the use of the components, the serial numbers are to be confirmed. • Examine documentation (e.g., record of past key transfers), interview, personnel and observe as needed to verify that the process used to transport cleartext key components using pre-numbered, tamper-evident, authenticable packaging, is sufficient to ensure: – The package serial number was transmitted as prescribed. – The details of the serial number of the package were transmitted separately from the package itself. – At least two communication channels were used to send the components of a given key (not just separation by sending on different days). – Each component was sent to/from only the custodian(s) authorized for the component – Prior to the use of the component, the serial number was confirmed.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
8-1 *(continued)* • If SCDs are used for conveying components/shares, the mechanisms or data (e.g., PIN) to obtain the key component/share from the SCD must be conveyed using a separate communication from the SCD channel, or it must be conveyed in the same manner as a paper component. SCDs must be inspected for signs of tampering. • If an SCD (i.e., HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering. ***Note:*** *Components/shares of encryption keys must be conveyed using different communication channels, such as different courier services. It is not sufficient to send key components/shares for a specific key on different days using the same communication channel.*	**8-1.c** If SCDs are used to convey components/shares: • Examine documented procedures to verify that the mechanism to obtain the keying material (e.g., PIN) is conveyed using a separate communication channel from the associated SCD. • Examine documented procedures to verify that each SCD is inspected to ensure that there are not any signs of tampering. • Examine the chain-of-custody document for the SCDs and any transport logs to ensure the movement of each device is tracked and that there is evidence that the SCDs and dual-control mechanisms were separated sufficiently to ensure that no one person gained access to the SCDs and both SCD enablers.
	8-1.d If an SCD is conveyed with pre-loaded secret and/or private keys, perform the following: • Examine documented procedures to verify that the SCD requires dual-control mechanisms to become operational. • Examine the documented procedures to ensure the method of shipment of the SCD and dual-control mechanisms (e.g., smart cards or passphrases) are separated in a way that ensures there is no opportunity for one person to gain access to the SCD and both authorization mechanisms (e.g., both smartcards, etc.). • Examine documented procedures to verify that the SCD is inspected to ensure there are no signs of tampering. • Examine records of key transfers and interview responsible personnel to verify the mechanisms that make the SCD operational are conveyed using separate communication channels.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
8-2 A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. ***Note:*** *An m-of-n scheme is a component- or share-allocation scheme where m is the number of shares or components necessary to form the key, and n is the number of the total set of shares or components related to the key. Management of the shares or components must be sufficient to ensure that no one person can gain access to enough of the item to form the key alone* *E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.*	**8-2.a** Examine documented procedures to verify they include controls to ensure that no single person can gain access to components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. Verify procedures include: • Designation of person(s) permitted to convey/receive keys. • Reminder that any person with access to one component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component or shares sufficient to form the necessary threshold to derive the key. • Steps to ensure any person with access to the media conveying a component/share of a key could not have access to other components/shares of this key, or to any other medium conveying any other component of this key that is sufficient to form the necessary threshold to derive the key, without detection.
	8-2.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can gain access to components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. Verify the implemented controls ensure the following: • Only designated custodians can send/receive the component or share. • There is a clear understanding that an individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key. • There is sufficient evidence to show that a person with access to the media conveying a key component or key share could not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key without detection.
	8-2.c Examine records of past key transfers to verify that the method used did not allow for any personnel to have access to components or shares sufficient to form the key.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
8-3 E-mail must not be used for the conveyance of secret or private keys or their components/shares, even if encrypted, unless the key (or component/share) has already been encrypted in accordance with these requirements—i.e., in an SCD. This is due to the existence of these key values in memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the cleartext of any encrypted text or files conveyed through those systems. Other similar mechanisms, such as SMS, fax, or telephone must not be used to convey cleartext key values.	**8-3** Interview personnel and examine logs to verify that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components/shares.
8-4 Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of public-key certificates as defined within this Domain that are created by a trusted CA that meets the applicable requirements of this Domain • Validating a hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in *ISO 16609* • Conveyance within an SCD • Encrypted *(continued on next page)*	**8-4** For all methods used to convey public keys, perform the following: **8-4.a** Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity, such as: • Use of public-key certificates created by a trusted CA that meets the applicable requirements of this Domain • Validation of a hash of the public key sent by a separate channel (e.g., mail) • Using a MAC (message authentication code) created using the algorithm defined in *ISO 16609* • Conveyance within an SCD • Encrypted

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
8-4 *(continued)* ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.* *Self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data. The authenticity of the root certificates is based on the use of secure procedures to distribute them. Specifically, they must be directly installed into the PIN pad of the ATM or POS device and not remotely loaded to the device subsequent to manufacture.*	**8-4.b** Examine documentation, interview personnel, and observe processes as needed to verify that self-signed certificates are not used as the sole method of authentication.
	8-4.c Observe the process for conveying public keys, associated logs, and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 9: *During its transmission, conveyance, or movement between any two locations or organizational entities, any single unencrypted secret or private key component or share must at all times be protected.* *Sending and receiving locations/entities are equally responsible for the physical protection of the materials involved.* *These requirements also apply to keys moved between locations of the same organization.*	
Key components/shares conveyed to and from a key-injection facility (or applicable entity providing key-management services) must be conveyed in compliance with these requirements. Such key components/shares include but are not limited to those for key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf), or key components for the BDKs themselves, terminal master keys used in the master key/session key key-management method, or HSM master keys (e.g., MFKs). These requirements also apply to keys moved between locations of the same organization.	
9-1 During the process to convey it, any single cleartext secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • Sealed in a security container or courier mailer (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be	**9-1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single cleartext secret or private key component/share must at all times be either: • Under the continuous supervision of a person with authorized access to this component • Sealed in a security container or courier mailer (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or • Contained within a physically secure SCD.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
obtained only by a person with authorized access to it and unauthorized access would be detected, or • Contained within a physically secure SCD. ***Note:*** *No single person must be able to access or use all components or a quorum of shares of a single secret or private cryptographic key.*	**9-1.b** Observe key-management processes, examine associated logs, and interview responsible personnel to verify processes implemented ensure that any single cleartext secret or private key component/share is at all times either: • Under the continuous supervision of a person with authorized access to this component • Sealed in a security container or courier mailer (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it or contained within a physically secure SCD.
9-2 Packaging or mailers (i.e., pre-numbered, tamper-evident packaging) containing cleartext key components must be examined for evidence of tampering before being opened. Any sign of package tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If a compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the destruction and replacement of: • The set of components • Any keys encrypted under this (combined) key	**9-2.a** Examine documented procedures to verify they include requirements for all packaging or mailers containing cleartext key components to be examined for evidence of tampering before being opened.
	9-2.b Interview responsible personnel and observe processes to verify that all packaging or mailers containing cleartext key components are examined for evidence of tampering before being opened.
	9-2.c Examine documented procedures require that any sign of package tampering is identified, reported, and, if compromise is confirmed, ultimately results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
	9-2.d Interview responsible personnel and observe processes to verify that if a package shows signs of tampering indicating a component was potentially compromised, processes are implemented to identify the tampering, report/escalate it, and, if compromise is confirmed, ultimately result in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
	9-2.e Examine records related to any escalated transmittal events. Verify that if compromise is confirmed it resulted in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
9-3 Only an authorized key custodian—and designated backup(s)—must have physical access to a key component prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.	**9-3.a** Examine the list(s) of key custodians—and designated backup(s)—authorized to have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.
	9-3.b Observe implemented access controls and processes to verify that only those authorized key custodians—and designated backup(s)—have physical access to key components prior to being secured in transmittal packaging and upon removal of a secured key component from transmittal packaging.
	9-3.c Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each component.
9-4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal. • Check tamper-evident packaging upon receipt for signs of tamper prior to opening tamper-evident authenticable packaging containing key components.	**9-4.a** Examine the list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
• Check the serial number of the tamper-evident packaging upon receipt of a component package. ***Note:*** *See* ***Requirement 26*** *for logging.*	**9-4.b** Observe implemented mechanisms and processes and examine logs to verify that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packaging upon receipt of a component package.
9-5 Pre-numbered, tamper-evident, authenticable bags must be used for the conveyance of cleartext key components not in an SCD. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers. ***Note:*** *Numbered courier bags are not sufficient for this purpose.*	**9-5** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of cleartext key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport cleartext key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. • Examine logs to verify that procedures are followed.
9-6 If components or shares of multiple keys are being sent simultaneously between the same sending and receiving custodians, the component/shares for a specific custodian or custodian group can be shipped in the same TEA bag provided that: • The components inside the tamper-evident and authenticable package are in separate opaque and identifiable packaging (e.g., individually sealed within labeled, opaque envelopes or PIN mailers) to prevent	**9-6.a** Examine documents, interview personnel, and observe processes as needed to verify that: • The components inside the tamper-evident and authenticable package are in separate opaque and identifiable packaging (e.g., individually sealed within labeled, opaque envelopes or within PIN mailers) to prevent confusion and/or inadvertent observation when the package is opened. • The components are repackaged at receipt into separate tamper-evident and authenticable packages for storage at the receiving location. • Records reflect the receipt of the shipped bag and association with subsequent individual bags

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
confusion and/or inadvertent observation when the package is opened. • The components are repackaged at receipt into separate tamper-evident and authenticable packages for storage at the receiving location. Records reflect the receipt of the shipped bag and association with subsequent individual bags.	**9-6.b** Examine logs to verify that procedures are followed.

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 10: *All key-encryption keys used to transmit or convey other cryptographic keys must be at least as strong as any key transmitted or conveyed.*	
Key-encryption keys used to convey keys to a key-injection facility or between locations or systems within the same key-injection facility (or applicable entity providing key-management services) must be at least as strong as any key transmitted or conveyed. Such keys include but are not limited to, key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities, locations, or systems (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf) for system migration, or transport between injection locations owned by the same organization.	
10-1 All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be at least as strong as the key being sent, as delineated in Annex C, except as noted below for RSA keys used for key transport. • TDEA keys used for encrypting keys must be at least triple-length keys (have bit strength of 112 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. • A triple-length TDEA key must not be encrypted with a TDEA key of lesser strength. • TDEA keys must not be used to protect AES keys. • TDEA keys must not be used to encrypt keys greater in strength than 112 bits. • RSA keys encrypting keys greater in strength than 80 bits must have a bit strength of at least 112 bits. **(***continued on next page)*	**10-1.a** Examine documented procedures to verify there is a requirement that all keys used to transmit or convey other cryptographic keys must be at least as strong as any key transmitted or conveyed, as delineated in Annex C (except as noted for RSA keys). **10-1.b** Examine documented procedures and interview personnel as needed to verify the requirement is satisfied for all applicable keys. Consider keys manually transferred (e.g., cryptograms sent to an ESO) as well as those that are system-generated and transferred (e.g., KEK or TMK encrypting working keys).

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
10-1 *continued*	**10-1.c** Observe key-generation processes for the key types identified above. Verify that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed, except as noted for RSA keys. To verify this: • Interview appropriate personnel and examine documented procedures for the creation of these keys. • Using the table in Annex C, validate the respective key sizes relative to the algorithms used for key encryption. • Verify that: – TDEA keys used for encrypting keys must be at least triple-length keys (have an effective bit strength of 112 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. – A triple-length TDEA key must not be encrypted with a TDEA key of lesser strength. – TDEA keys are not used to protect AES keys. – TDEA keys are not used to encrypt keys greater in strength than 112 bits. – RSA keys encrypting keys greater in strength than 80 bits have a bit strength at least 112 bits.
	10-1.d Examine system documentation and configuration files to validate the above, including HSM settings.
10-2 ***Not used in P2PE***	
10-3 ***Not used in P2PE***	
10-4 ***Not used in P2PE***	
10-5 ***Not used in P2PE***	

Control Objective 3: Keys are conveyed or transmitted in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 11: *Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.*	
11-1 Written procedures must exist and be known to all affected parties.	**11-1.a** Observe documented procedures exist for all key transmission and conveyance processing.
	11-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.
11-2 Methods used for the conveyance or receipt of keys must be documented.	**11-2** Observe documented procedures include all methods used for the conveyance or receipt of keys.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 12: *Secret and private keys must be input into hardware (host) security modules (HSMs) and Point of Interaction (POI) devices in a secure manner:* *a) Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.* *b) Key-establishment techniques using public-key cryptography must be implemented securely.*	
Key-injection facilities (or applicable entities providing key-management services) must load keys using dual control and for cleartext secret and private keys, split knowledge. Such keys include, but are not limited to: • *Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method;* • *Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is injecting keys on their behalf);* • *Terminal master keys (TMKs) used in the master key/session key key-management method;* • *PIN-encryption keys used in the fixed-transaction key method;* • *Master keys for key-injection platforms and systems that include hardware devices (SCDs) for managing (e.g., generating and storing) the keys used to encrypt other keys for storage in the key-injection platform system;* • *Public and private key pairs loaded into the POIs for supporting remote key-establishment and distribution applications;* • *Digitally signed POI public key(s) signed by a device manufacture's private key and subsequently loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable). Dual control is not necessary where other mechanisms exist to validate the authenticity of the key, such as the presence in the device of an authentication key;* • *Device manufacturer's authentication key (e.g., vendor root CA public key) loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable).*	
12-1 The loading of secret or private keys, when from the individual key components or shares, must be performed using the principles of dual control and split knowledge. **Note:** Manual key loading may involve the use of media such as paper, smart cards, or other physical tokens. (*continued on next page*)	**12-1.a** Examine documented procedures, interview personnel, and observe processes as needed to verify the requirement is satisfied for all applicable keys. **12-1.b** Interview appropriate personnel to determine the number of key components for each manually loaded key. **12-1.c** Observe the key-loading processes for all key types (e.g., MFKs, AWKs, TMKs, DEKs, etc.). Verify the number and length of the key components against information provided through verbal discussion and written documentation.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-1 *(continued)*	**12-1.d** Observe the process to verify it includes the entry of individual key components by the designated key custodians.
	12-1.e Observe key-loading devices can only be accessed and used under dual control.
	12-1.f Examine locations where keys may have been recorded that don't meet this requirement. As applicable, examine HSM startup documentation (including Disaster Recovery or Business Continuity Planning documentation) and procedure manuals to ensure that there are no key or component values recorded.
12-2 Procedures must be established that will prohibit any one person from having access to components sufficient to form an encryption key when components are removed from and returned to storage for key loading.	**12-2.a**. Examine logs of access to security containers for key components/shares to verify that only the authorized custodian(s) have accessed. Compare the number on the current tamper-evident and authenticable package for each component to the last log entry for that component. Trace historical movement of higher-order keys (MFK, KEK, and BDK) in and out of secure storage to ensure there is no break in the package-number chain that would call into question authorized handling and sufficient storage of the component or share. This must address at a minimum the time frame from the date of the prior audit.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-3 The loading of cleartext cryptographic keys using a key-loading device must require dual control to authorize any key-loading session. It must not be possible for a single person to use the key-loading device to load clear keys alone. Dual control must be implemented using one or more of, but not limited to, the following techniques: • Two or more passwords/authentication codes of five characters or more (vendor default values must be changed) • Multiple cryptographic tokens (such as smartcards), or physical keys • Physical access controls • Separate key-loading devices for each component/share *(continued on next page)*	**12-3.a** Examine documented procedures for loading of cleartext cryptographic keys to verify: • Procedures require dual control to authorize any key-loading session. • The techniques to be used to achieve dual control are identified. • There is a requirement to change any default passwords/authentication codes and set passwords/authentication codes that have at least five characters. • There is a requirement that if passwords/authentication codes or tokens are used, they are maintained separately. **12-3.b** For each type of production SCD loaded using a key-loading device, observe for the process (e.g., a demonstration) of loading cleartext cryptographic keys and interview personnel. Verify that: • Dual control is necessary to authorize the key-loading session. • Expected techniques are used. • Default passwords/authentications codes are reset. • Any passwords/authentication codes used are a minimum of five characters. • Any passwords/authentication codes or tokens are maintained separately.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-3 *(continued)* ***Note 1:*** *For devices that do not support two or more passwords/authentication codes, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian. Each half must be a minimum of five characters.* ***Note 2:*** *Passwords/authentication codes to the same object may be assigned to a custodian group team—e.g., custodian team for component A.* ***Note 3:*** *The addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS POI Security Requirements and listed as such in the approval listings. A PED that has been modified to perform these functions must be validated and approved to the KLD approval class.,*	**12-3.c** Examine documented records of key-loading to verify the presence of two authorized persons during each type of key-loading activity.
	12-3.d Observe that any default dual-control mechanisms (e.g., default passwords/authentication codes—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.
12-4 Key components for symmetric keys must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components—e.g., via XOR'ing of full-length components. The resulting key must only exist within the SCD. ***Note:*** *Concatenation of key components together to form the key is unacceptable; e.g., concatenating two 8-hexadecimal character halves to form a 16-hexadecimal secret key.*	**12-4.a** Examine documented procedures for combining symmetric-key components and observe processes to verify that key components are combined using a process such that no active bit of the key can be determined without knowledge of the remaining components—e.g., only within an SCD.
	12-4.b Examine device configuration settings and interview personnel to verify that key components used to create a key are the same length as the resultant key.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-5 Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must use AES with a key size of at least 128 bits.	**12-5** Examine vendor documentation describing options for how the HSM MFK is created and verify the current MFK was created using AES (or triple-length TDEA for existing P2PE implementations only). Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.	**12-6** Examine documented procedures, interview personnel, and observe processes as needed to confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key.
12-7 The initial terminal master key (TMK) or initial DUKPT key must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key or an initial DUKPT key may use techniques described in this document such as: • Asymmetric techniques; • Manual techniques; • The existing TMK to encrypt the replacement TMK for download; • For AES DUKPT, using the option to derive a key-encryption key called the DUKPT Update Key so that the host can send a device a new initial key encrypted under that key. Note this also requires that a new initial key ID is also sent. Keys must not be reloaded by any methodology in the event of a compromised device and must be withdrawn from use.	**12-7.a** Examine documented procedures for the loading of TMKs and initial DUKPT keys to verify that they require asymmetric key-loading techniques or manual techniques for initial loading and allowed methods for replacement TMK or initial DUKPT key loading. **12-7.b** Examine documented procedures to verify that keys are withdrawn from use if they were loaded to a device that has been compromised or gone missing.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-8 If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, these must meet the applicable requirements detailed in this Domain of this document. For example: A public-key technique for the distribution of symmetric secret keys must: • Use public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Provide for mutual device authentication for both the host and the POI device or host-to-host if applicable, including assurance to the host that the POI device has (or can compute) the session key, and that no entity other than the POI device specifically identified can possibly compute the session key.	**12-8.a** For techniques involving public-key cryptography, examine documentation to illustrate the process, including the size and sources of the parameters involved, and the mechanisms utilized for mutual device authentication for both the host and the POI device. **12-8.b** If key-establishment protocols using public-key cryptography are used to remotely distribute secret keys, examine documented procedures, interview personnel, and observe processes as needed to verify that the applicable requirements detailed in this Domain are met, including: • Use of public and private key lengths that are in accordance with Annex C for the algorithm in question. • Use of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
12-9 Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (e.g., PTS POI devices 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* • *Separate key-loading devices for each component.*	**12-9.a** Examine documented key-injection procedures to verify that the procedures define the use of dual control and split knowledge controls for the loading of keys into devices. **12-9.b** Interview responsible personnel and observe key-loading processes and controls to verify that dual control and split-knowledge controls are in place for the loading of keys into devices. **12-9.c** Examine records of key-loading processes and controls to verify that the loading of keys does not occur without dual control and split knowledge.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 13: *The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	

Key-injection facilities (or applicable entities providing key-management services) must ensure key-loading mechanisms are not subject to disclosure of key components or keys.

Some key-injection platforms use personal-computer (PC)-based software applications, whereby cleartext secret and/or private keys and/or their components exist in memory outside the secure boundary of an SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. These weaknesses include:

- *XOR'ing of key components is performed in software.*
- *Cleartext keys and components can reside in software during the key-loading process.*
- *Some systems require only a single password.*
- *Some systems store the keys (e.g., BDKs, TMKs) on removable media or smart cards. These keys are in the clear with some systems.*
- *PCs, by default, are not managed under dual control. Extra steps (e.g., logical user IDs, physical access controls, etc.) must be implemented to prevent single control of a PC.*
- *Data can be recorded in the PC's non-volatile storage.*
- *Software Trojan horses or keyboard sniffers can be installed on PCs.*

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-1 Cleartext secret and private keys and key components must be transferred into an SCD only when it can be ensured that: • Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of cleartext key components. • There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys. • The sending and receiving SCDs must be inspected prior to key loading to ensure that they have not been subject to any prior tampering or unauthorized modification that could lead to the disclosure of cleartext keying material. • SCDs must be inspected to detect evidence of monitoring and to ensure dual control procedures are not circumvented during key loading. • An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are uniquely identified by the device.	**13-1** Observe key-loading environments, processes, and mechanisms (e.g., terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Observe cameras are positioned to ensure they cannot monitor the entering of cleartext key components. • Examine documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that: – SCDs are inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. – An SCD transfers a plaintext secret or private key only when at least two authorized individuals are identified by the device. – There is not any mechanism at the interface (including cabling) between the conveyance medium and the SCD that might disclose the transferred keys. – The SCD is inspected to ensure it has not been subject to any prior tampering or unauthorized modification, which could lead to the disclosure of cleartext keying material.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-2 Only SCDs must be used in the loading of cleartext secret or private keys or their components outside of a secure key-loading facility (i.e. a KIF). For example, computer keyboards or those attached to an HSM must never be used for the loading of cleartext secret or private keys or their components. ***Note:*** *The addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS POI Security Requirements and listed as such in the approval listings. A PED that has been modified to perform these functions must be validated and approved to the KLD approval class.*	**13-2.a** Examine documentation to verify that only SCDs are used in the loading of cleartext secret or private keys or their components outside of a secure key-loading facility, as delineated in this requirement. For example, computer keyboards or keyboards attached to an HSM must never be used for the loading of cleartext secret or private keys or their components.
	13-2.b Observe a demonstration of key loading to verify that only SCDs are used in the loading of cleartext secret or private keys or their components outside of a secure key-loading facility.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-3 The loading of cleartext secret or private key components or shares from an electronic medium—e.g., smart card, thumb drive, fob, or other device used for data transport—directly into a cryptographic device (and verification of the correct receipt of the component, if applicable) must result in either of the following • The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium in accordance with **Requirement 24**.	**13-3.a** Examine documented procedures for the loading of secret or private key components from electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key injection, including: • Instructions for the medium to be placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium, including the method to use.
	13-3.b Observe key-loading processes to verify that the injection process results in one of the following: • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.
	13-3.c Examine records/logs of erasures to confirm that: • The documented procedure was followed. • The method used was in accordance with **Requirement 24**.
13-4 Secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device must meet the following requirements (13-4.1 through 13-4.8):	**13-4** Examine documented procedures and observe processes for the use of key-loading devices. Perform the following:
13-4.1 The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected. ***Note:*** *A PCI-approved KLD meets this requirement for an SCD.*	**13-4.1** Examine documented procedures, interview personnel, and observe processes as needed to 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.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-4.2 The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it. ***Note:*** *Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.*	**13-4.2** Examine documented procedures, interview personnel, and observe processes as needed to 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.
13-4.3 The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.	**13-4.3.a** Examine documented procedures, interview personnel, and observe processes as needed to 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.
	13-4.3.b Examine documented procedures, interview personnel, and observe processes as needed to verify that both authorized personnel involved in key-loading activity inspect the key-loading device, prior to use to ensure that a key-recording device has not been inserted between the SCDs.
13-4.4 The key-loading device must not retain any information that might disclose the key (e.g., allow replay of the key for injection into a non-SCD) that was installed in the device or a key that it has successfully transferred.	**13-4.4** Examine documented procedures, interview personnel, and observe processes as needed to verify the key-loading device does not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred. For example, attempt to output the same value more than one time from the device or cause the device to display check values for its contents both before and after injection and compare.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-5 Any media (electronic or otherwise) containing secret or private key components or shares used for loading cryptographic keys must be maintained in a secure location and accessible only to authorized custodian(s). When removed from the secure storage location, media or devices containing key components or used for the injection of cleartext cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process. The media upon which a component resides must be physically safeguarded at all times when removed from secure storage. Key components that can be read (e.g., those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are never used in a manner that would result in the component being displayed in cleartext to anyone who is not a designated custodian for that component.	**13-5.a** Interview personnel and observe media locations to verify that the media is maintained in a secure location accessible only to custodian(s) authorized to access the key components.
	13-5.b Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices be in the physical possession of only the designated component holder(s). • The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.
	13-5.c Interview designated component holder(s) and examine key-management logs to verify that media or devices removed from secure storage are in the physical possession of only the designated component holder(s).
	13-5.d Interview key-injection personnel and examine logs for the removal of media/devices from secure storage to verify they are removed only for the minimum practical time necessary to complete the key-loading process.
13-6 If the component is in human-readable form it must be visible only to the designated component custodian and only for the duration of time required for this person to privately enter the key component into an SCD.	**13-6 I**f components are in human-readable form, examine documented procedures, interview personnel, and observe processes as needed to verify that they are visible only to designated component custodians and only for the duration of time required for this person to privately enter the key component into an SCD.
13-7 Written or printed key component documents must not be opened until immediately prior to use.	**13-7.a** Examine documented procedures and confirm that printed/written key component documents are not opened until immediately prior to use.
	13-7.b Observe key-loading processes and verify that printed/written key component documents are not opened until immediately prior to use.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
13-8 A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. ***Note**: E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e., m = 3) can be used to derive the key, no single individual can have access to more than two components/shares.*	**13-8.a** Examine documented procedures for the use of key components to verify that procedures ensure that any individual custodian only has access to their assigned components and never has access to sufficient key components to reconstruct a cryptographic key.
	13-8.b Examine key-component access controls and access logs to verify that any single authorized custodian can and has only had access to their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.
13-9 [Requirement removed]	

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 14: *All hardware and access/authentication mechanisms (e.g., passwords/authentication codes) used for key loading must be managed under dual control.*	
Key-injection facilities (or applicable entities providing key-management services) must ensure that the key-injection application passwords/authentication codes and associated user IDs are managed in such a way as to enforce dual control. Also, the hardware used for key-injection must be managed under dual control. Vendor default passwords/authentication codes must be changed.	
14-1 Any hardware and passwords/authentication codes used in the key-loading function must be controlled and maintained in a secure environment under dual control. Resources (e.g., passwords/authentication codes and associated hardware) must be managed such that no single individual has the capability to enable key loading of cleartext keys or their components. This is not to imply that individual access authentication mechanisms must be managed under dual control. ***Note:*** *Where key-loading is performed for PTS POI devices, the secure environment as defined in* ***Requirement 32-9*** *must additionally be met.*	**14-1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords/authentication codes and associated hardware) used in the key-loading function must be controlled and managed such that no single individual has the capability to enable key loading of cleartext keys or their components.
	14-1.b Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function is controlled and maintained in a secure environment under dual control. • All resources (e.g., passwords/authentication codes and associated hardware) used for key-loading functions are controlled and managed such that no single individual has the capability to enable key loading.
14-2 All cable attachments over which cleartext keying material traverses must be examined at the beginning of an entity's key activity operations (system power on/authorization) to ensure they have not been tampered with or compromised.	**14-2.a** Examine documented procedures to ensure they require that cable attachments are examined at the beginning of an entity's key-activity operations (system power on/authorization).
	14-2.b Observe key-loading processes to verify that all cable attachments are properly examined at the beginning of an entity's key-activity operations (system power on/authorization).

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
14-3 Key-loading equipment usage must be monitored, and a log of all key-loading activities maintained for audit purposes must contain, at a minimum, date, time, personnel involved, and the number of devices keys are loaded to.	**14-3.a** Observe key-loading activities to verify that key-loading equipment usage is monitored.
	14-3.b Examine logs of all key-loading activities and verify that they are maintained and contain all required information.
14-4 Any physical tokens (e.g., brass keys or chip cards) used to enable key loading must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys or sign applications under single control. These tokens must be secured in a manner similar to key components, including tamper-evident, authenticable packaging and the use of access-control logs for when removed or placed into secure storage.	**14-4.a** Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key loading. Verify procedures require that physical tokens must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control.
	14-4.b Examine/observe locations and controls for physical tokens to verify that tokens used to enable key loading are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control.
	14-4.c Examine storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.
	14-4.d Examine access-control logs and verify they are in use including notation of tamper-evident, authenticable bag numbers.
	14-4.e Examine documented procedures, interview personnel, and observe processes as needed to reconcile storage contents to access-control logs.
14-5 Default passwords/authentication codes used to enforce dual-control mechanisms must be changed, and documented procedures must exist to require that these password/PINs be changed when assigned personnel change.	**14-5.a** Examine documented procedures to verify they require default passwords/authentication codes used to enforce dual-control mechanisms are changed.
	14-5.b Examine documented procedures to verify they require that the passwords/authentication codes be changed when assigned personnel change.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 15: *The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured, and it can be ascertained that they have not been tampered with, substituted, or compromised.*	
15-1 A cryptographic-based validation mechanism must be in place to ensure the authenticity and integrity of keys and/or their components (e.g., testing key-check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See *ISO 11568*. Where check values are used, recorded, or displayed key-component check values and key-check values must be generated by a cryptographic process such that all portions of the key or key component are involved in generating the check value. The check value must be in accordance with the following note. ***Note:*** *Check values may be computed by two methods. TDEA may use either method. AES must only use the CMAC method. In the first method, check values are computed by encrypting an all-binary zeros block using the key or component as the encryption key, using the leftmost n-bits of the result; where n is at most 24 bits (6 hexadecimal digits/3 bytes). In the second method the KCV is calculated by MACing an all binary zeros block using the CMAC algorithm as specified in* ISO 9797-1 *(see also* NIST SP 800-38B*). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MACed using the TDEA block cipher, while a 128-bit AES key or component will be MACed using the AES-128 block cipher.*	**15-1.a** Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and/or components. **15-1.b** Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and is verified by the applicable key custodians. **15-1.c** Examine the methods used for key validation to verify they are consistent with *ISO 11568*—e.g., when check values are used, they are in accordance with this requirement.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
15-2 The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted in accordance with Annex C, or if in plaintext form, must: • Be within a certificate as defined in applicable requirements within this Domain; or • Be within a PKCS#10 (authentication and integrity occurs via other mechanisms); or • Be within an SCD; or • Have a MAC (message authentication code) created using the algorithm defined in *ISO 16609.*	**15-2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.
	15-2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.
15-3 Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange, or key establishment with POIs. POIs and key-distribution hosts (KDHs) using public-key schemes must validate authentication credentials of other such devices involved in the communication immediately prior to any key transport, exchange, or establishment. Mutual authentication of the sending and receiving devices must be performed. ***Note:*** *Examples of this kind of validation include ensuring the SCD serial number is listed in a table of "permitted" devices, checking current certificate revocation lists or embedding valid authorized KDH certificates in devices and disallowing communication with unauthorized KDHs, as delineated by techniques defined in the Technical FAQs for PCI PTS POI Security Requirements.*	**15-3.a** Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: • POI devices must validate authentication credentials of KDHs prior to any key transport, exchange, or establishment with that device. • KDHs must validate authentication credentials of POIs prior to any key transport, exchange, or establishment with that device.
	15-3.b Interview applicable personnel to verify that mutual authentication of the sending and receiving devices is performed, as follows: • POI devices validate authentication credentials of KDHs immediately prior to any key transport, exchange, or establishment with that device. • KDHs validate authentication credentials of POIs immediately prior to any key transport, exchange, or establishment with that device.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
15-4 Key-establishment and distribution procedures must be designed such that: • Within an implementation design, there must be no means available for "man-in-the-middle" attacks—e.g., through binding of the KDH certificate upon the initial communication. • System implementations must be designed and implemented to prevent replay attacks—e.g., through the use of random nonces and time stamps as noted in *ANSI TR-34*.	**15-4** Examine system and process documentation to verify that key-establishment and distribution procedures are designed such that: • There are no means available in the implementation design for "man-in-the-middle" attacks. • System implementations are designed to prevent replay attacks.
15-5 Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device and must provide for key protection in accordance with this document. That is, the secrecy of the private key and the integrity of the public key must be ensured. The process must ensure that once keys are injected, they are no longer available for injection into other POI devices—i.e., key pairs are unique per POI device.	**15-5** If key pairs are generated external to the device that uses the key pair, perform the following: • Examine documented procedures to verify that controls are defined to ensure the secrecy of private keys and the integrity of public keys during key transfer and loading. • Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured. • Observe the process to verify it ensures that key pairs are unique per PTS POI device.

Control Objective 4: Key loading to HSMs and POI devices is handled in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 16: *Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*	
16-1 Documented key-loading procedures must exist for all devices (e.g., HSMs and POI devices), and all parties involved in cryptographic key loading must be aware of those procedures.	**16-1.a** Examine documented procedures and verify they exist for all key-loading operations.
	16-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.
	16-1.c Observe the key-loading process for keys loaded as components and verify that the documented procedures are demonstrably in use. This may be done as necessary on test equipment—e.g., for HSMs.
16-2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.	**16-2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
Requirement 17: *Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems of two organizations or logically separate systems within the same organization.*	
17-1 Where two organizations or logically separate systems share a key to encrypt account data (including a key-encipherment key used to encrypt a data-encryption key) communicated between them, that key must: • Be unique to those two entities or logically separate systems And, • Not be given to any other entity or logically separate systems. ***Note:*** *This requirement does not apply after the decryption environment.*	**17-1.a** Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations or logically separate systems.
	17-1.b For all keys shared between two organizations or logically separate systems for encrypting account data (including key-encryption keys used to encrypt a data-encryption key) perform the following: • Observe and/or test to Generate or otherwise obtain key-check values for any key-encipherment keys (KEKs) to verify key uniqueness between the two organizations. A random sample may be used where more than 10 zone connections are in use. This is not intended to be based on values retained on paper or otherwise sent as part of the original conveyance of the keying material, but rather on values generated from stored zone production keys from the production host database. Cryptograms may be used for this purpose if it is verified that the same MFK variant is used to encrypt the KEKs. • If a remote key-establishment and distribution scheme is implemented between networks, examine public keys and/or hash values and/or fingerprints of the keys to verify key uniqueness of the asymmetric-key pairs. • Observe key-check values against those for known or default keys to verify that known or default key values are not used.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
Requirement 18: *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	
18-1 Synchronization errors must be monitored to help reduce the risk of an adversary's substituting a key known only to them. Procedures must exist and be followed for investigating repeated synchronization errors for online processes such as online key exchanges or transmission or processing of transactions. ***Note:*** *Multiple synchronization errors may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted.*	**18-1.a** Examine documented procedures to verify they have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.
	18-1.b Examine and/or observe the 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.
18-2 To prevent or detect usage of a compromised key, key-component packaging or containers that show signs of tampering indicating a component was potentially compromised must be assessed and the analysis formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of the component and the associated key at all locations where they exist.	**18-2.a** Examine the documented procedures to verify they require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it must result in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
	18-2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering indicating a component was potentially compromised are assessed and the analysis is formally documented. If compromise is confirmed, and the result is that one person could have knowledge of the key, it results in the discarding and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
18-3 Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods The phased implementation dates are as follows: • **Phase 1 –** Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to hardware security modules (HSM). Effective date: **1 June 2019 (past).** • **Phase 2** – Implement Key Blocks for external connections to Associations and Networks. Effective date: **1 January 2023 (past).** • **Phase 3** – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Effective date: **1 January 2025 (past).** Acceptable methods of implementing the integrity requirements include, but are not limited to: • A MAC computed over the concatenation of the cleartext attributes and the enciphered portion of the key block, which includes the key itself. • A digital signature computed over that same data, e.g., TR-34; • An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in *ANSI X9.102*.	**18-3** Using the cryptographic-key summary to identify secret keys conveyed or stored, examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of the acceptable methods or an equivalent. Where key blocks are not implemented, identify and examine project plans to implement in accordance with the prescribed timeline.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
18-4 PTS POI devices must only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate-issuing authority generates the key pair on behalf of the POI); and with KDHs for key management, normal transaction processing, and certificate (entity) status checking.	**18-4.a** Examine documented procedures to verify that: • PTS POI devices only communicate with CAs for the purpose of certificate signing, or for key injection where the certificate-issuing authority generates the key pair on behalf of the device; • POI devices only communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.
	18-4.b Interview responsible personnel and observe PTS POI configurations to verify that: • PTS POI devices only communicate with CAs for the purpose of certificate signing, or for key-injection where the certificate issuing authority generates the key pair on behalf of the device; • PTS POI devices only communicate with KDHs or key management, normal transaction processing, and certificate (entity) status checking.
18-5 KDHs must only communicate with PTS POI devices for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.	**18-5.a** Examine documented procedures to verify that: • KDHs only communicate with PTS POI devices for the purpose of key management and normal transaction processing; • KDHs only to communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.
	18-5.b Interview responsible personnel and observe KDH configurations to verify that: • KDHs only communicate with POIs for the purpose of key management and normal transaction processing; • KDHs only communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
18-6 Controls must be in place to prevent and detect the loading of unencrypted private and secret keys or their components by any one single person. ***Note:*** *Controls include physical access to the room, logical access to the key-loading application, video surveillance of activities in the key-injection room, physical access to secret or private cryptographic key components or shares, etc.*	**18-6.a** Examine documented key-injection procedures to verify that controls are defined to prevent and detect the loading of keys by any one single person.
	18-6.b Interview responsible personnel and observe key-loading processes and controls to verify that controls—e.g., viewing CCTV images—are implemented to prevent and detect the loading of keys by any one single person.
18-7 Key-injection facilities must implement controls to protect against the unauthorized substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to: • All devices loaded with keys must be tracked at each key-loading session by serial number. • Key-injection facilities must use something unique about the POI (e.g., logical identifiers) when deriving the key (e.g., DUKPT, TMK) injected into it	**18-7.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.
	18-7.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.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
Requirement 19: *Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	
• *Where test keys are used, key-injection facilities (or applicable entities providing key-management services) must use a separate test system for the injection of test keys.* • *Test keys must not be injected using the production platform, and test keys must not be injected into production equipment.* • *Production keys must not be injected using a test platform, and production keys must not be injected into equipment that is to be used for testing purposes.* • *Keys used for signing of test certificates must be test keys.* • *Keys used for signing of production certificates must be production keys.*	
19-1 Encryption keys must only be used for the purpose they were intended—i.e., key-encryption keys must not be used as data-encryption keys, data-encryption keys must not be used for key encryption, etc. Derivation Keys may be derived into multiple keys, each with its own purpose. For example, a DUKPT Initial Key may be used to derive both a PIN encryption key and a data encryption key. The derivation key would only be used for its own purpose, key derivation. This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.	**19-1.a** Examine key-management documentation (e.g., the cryptographic-key inventory) and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are defined for a specific purpose. **19-1.b** Using a sample of device types, examine/observe check values, terminal definition files, etc. to verify that keys used for key encipherment are not used for any other purpose.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-2 Private keys: • Must be used only for a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating POI devices). • Must never be used to encrypt other keys. • When used for remote key distribution, must not be used in connection with any other purpose. ***Note:*** *The restriction does not apply to certificate signing requests e.g., PKCS #10.*	**19-2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are : • Used only to create digital signatures or to perform decryption operations. • Used only for a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both. • Never used to encrypt other keys. • Not used in connection with any other purpose when used for remote key distribution.
19-3 Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).	**19-3** Examine key-management documentation and interview key custodian and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for POI devices).

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-4 Keys must never be shared or substituted between production and test/development systems. • Keys used for production must never be present or used in a test/development system, and • Keys used for testing must never be present or used in a production system. ***Note:*** *For logically partitioned HSMs and computing platforms, if one or more logical partitions of a physical device are used for production and one or more other logical partitions are used for testing, including QA or similar, the entire configuration that is impacted—computing platform(s) and networking equipment—must be managed and controlled as production.*	**19-4.a** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and test/development systems.
	19-4.b Observe processes for generating and loading keys into production systems to ensure that they are in no way associated with test or development keys.
	19-4.c Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.
	19-4.d Examine/observe check, hash, cryptogram, or fingerprint values for production and test/development keys with higher-level keys (MFKs, KEKs shared with other network nodes, and BDKs) to verify that development and test keys have different key values.
19-5 If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements. At all times, the HSMs and servers/computers must be physically and logically secured in accordance with these requirements. ***Note****: This does not apply to HSMs that are never intended to be used for production.*	**19-5** Interview personnel to determine whether production platforms are ever temporarily used for test purposes. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted, and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-6 Key pairs must not be reused for certificate renewal or replacement—i.e., new key pairs must be generated. Each key pair must result in only one certificate.	**19-6.a** Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate
	19-6.b Interview responsible personnel, examine records of past KDH-signing requests, and observe certificate issuing and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Certificates are replaced by generating a new key pair and requesting a new certificate. • Each key pair generated results in only one certificate.
19-7 KDH private keys must not be shared between devices except for load balancing and disaster recovery.	**19-7** Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.
19-8 PTS POI device private keys must not be shared between PTS POI devices.	**19-8.a** Examine documented processes to verify that POI device private keys are not permitted to be shared between POI devices.
	19-8.b Examine public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI device.
19-9 Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose—that is, keys must be used in accordance with their certificate policy. See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.	**19-9.a** Examine key-usage documentation and ensure that the usage is in accordance with the certificate policy.
	19-9.b Examine vendor documentation and device configuration settings to verify that the device mechanisms are implemented that preclude the use of a key for other than its designated and intended purpose.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-9.1 CA certificate signature keys, certificate (entity) status checking (e.g., Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorized host lists in encryption devices must not be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates. ***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.*	**19-9.1.a** Examine certificate policy and documented procedures to verify that the following: • Certificate signature keys, • Certificate status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POI devices. Are not used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
	19-9.1.b Interview responsible personnel and observe demonstration to verify that the following: • Certificate signature keys, • Status checking (e.g., Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs. Are not used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
19-9.2 CAs that issue certificates to other CAs must not be used to issue certificates to POIs (i.e., a CA cannot sign certificates to both subordinate CAs and end-entity [POI] devices).	**19-9.2** If a CA issues certificates to other CAs, examine the CA certificate policy and documented procedures to verify that the CA does not also issue certificates to POI devices.
19-10 Public-key-based implementations must provide mechanisms for restricting and controlling the use of public and private keys. For example, this can be accomplished through the use of X.509 compliant certificate extensions.	**19-10** Examine documented procedures to verify that mechanisms are defined for restricting and controlling the use of public and private keys such that they can only be used for their intended purpose.
19-11 CA private keys must not be shared between devices except for load balancing and disaster recovery.	**19-11** Examine CA's documented processes to verify that CA private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-12 Certificates used in conjunction with remote key-distribution functions must only be used for a single purpose. • Certificates associated with encryption for remote key-distribution functions must not be used for any other purpose. • Certificates associated with authentication of the KDH must not be used for any other purpose. • Certificates associated with authentication of the POI must not be used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications must not be used for any other purpose. If CA separation is used to ensure certificate segmentation: • Sub-CAs used to produce certificates used for remote key-delivery functions must not be used to produce certificates used for any other purpose. • Sub-CAs used to produce certificates for POI firmware and POI application authentication must not be used for any other purpose. *(continued on next page)*	**19-12.a** Examine implementation schematics and other relevant documentation to identify PKI architecture and where certificates are used in the implementation. **19.12.b** Identify mechanism(s) used to restrict certificates to a single-purpose use as either: • Separation of the Sub-Cas issuing the certificates, or • Policy-based certificate segmentation that depends upon a characteristic of the certificate. **19-12.c** If CA separation is used to ensure certificate segmentation, examine/observe as needed to verify that the following are true: • The designation of each Sub-CA is documented. • Policies and procedures are in place to support and require appropriate use of each Sub-CA. • Any Sub-CA used to produce certificates used for remote key-delivery functions (i.e., encryption, POI authentication, or KDH authentication) is not used to produce certificates used for any other purpose. • Any Sub-CA used to produce certificates for POI firmware and POI application authentication is not used for any other purpose.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
19-12 *(continued)* If policy-based certificate segmentation is used to achieve unique purpose certificates: • The method of segmentation between certificates must be reflected in the certificate practice statement (CPS) for the CA. • Certificates issued for remote key-distribution purposes must include a mechanism to identify designation for this purpose. • Each SCD using a certificate in a remote key-delivery function must ensure there is a designation included in the certificate indicating that it is for use in the remote key-delivery function for which it is being used. Each SCD using a certificate in a remote key-delivery function must ensure that if there is a designation included in a certificate that indicates it is for use in a remote key-delivery function, the SCD does not use it for any other purpose.	**19-12.d** If policy-based certificate segmentation is used to ensure certificate segmentation, examine/observe as needed to confirm that all of the following are true: • The method of segmentation between certificates is clearly stated in the certificate practice statement (CPS) for the CA. • Certificates issued for all of the remote key-distribution functions (i.e., encryption, POI authentication, or KDH authentication) include a mechanism to identify designation for this purpose. • Policies and procedures are in place to support and require specific function designation for each certificate issued, and there is evidence that such procedures are followed. • The SCDs involved in the remote key-delivery functions ensure that the certificates used for these functions are designated for the purpose for which they are being used. • The SCDs involved in remote key delivery ensure that certificates with remote key-delivery designation are not used for some other purpose.
	19-12.e Examine/observe as needed to confirm that the mechanisms in place are effective in restricting the certificates to a single purpose use as noted below: • Certificates associated with encryption for remote key-distribution functions are not used for any other purpose. • Certificates associated with authentication of the KDH are not used for any other purpose. • Certificates associated with authentication of the POI are not used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications are not used for any other purpose.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
Requirement 20: *All secret and private cryptographic keys ever present and used for any function (e.g., key encipherment or account-data encipherment) by a POI device that processes account data must be unique (except by chance) to that device.*	
20-1 PTS POI devices must each implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device. ***Note**: This means not only the account-data-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.* *POI device private keys must not exist anywhere but the specific POI device they belong to, except where generated external to the POI device and prior to the injection into the POI device.*	**20-1.a** Examine documented procedures for the loading and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations. **20-1.b** Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POI devices to verify that unique keys are generated and used for each POI device. **20-1.c** Examine check values, hash, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI device vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
20-2 [Requirement removed]	
20-3 Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in *ISO 11568* so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto PTS POI devices—i.e., only the derived key is loaded to the PTS POI device. This requirement refers to the use of a single "base" key to derive initial keys for many different PTS POI devices, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for the derivation of other keys once loaded—e.g., as done with DUKPT. ***Note**: The same BDK with the same KSN installed in multiple injection systems or installed multiple times within the same injection system will not meet uniqueness requirements.*	**20-3.a** Examine documented procedures and observe processes for generating initial keys. Verify the following is implemented where initial keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POI devices receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating PTS POI device. • Examine key-generation/injection logs to ensure that sequential values included in unique key derivation are not repeated.
	20-3.b Examine/observe to verify that derivation keys used to generate keys for multiple devices are never loaded into a PTS POI device.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage	
Domain 5 Requirements	**Testing Procedures**
20-4 Entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring organizations must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques: • Different BDKs for each financial institution; • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model; • Different BDKs by geographic region, market segment, processing platform, or sales unit. ***COMPONENT PROVIDERS ONLY:*** *Must use at least one unique Base Derivation Key (BDK) per acquiring organization and must be able to support segmentation of multiple BDKS of acquiring organizations.*	**20-4** Examine documented key-generation and injection procedures to verify that entities processing or injecting DUKPT or other key-derivation methodologies incorporate a segmentation strategy in their environments using one or more of the following techniques: • Different BDKs for each financial institution; • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model; • Different BDKs by geographic region, market segment, processing platform, or sales unit; ***FOR COMPONENT PROVIDERS ONLY:*** *Examine documented key-generation and injection procedures to verify that key-injection vendors use at least one unique Base Derivation Key (BDK) per acquiring organization and are able to support segmentation of multiple BDKs of acquiring organizations.*
20-5 Key-injection facilities that load DUKPT keys for various PTS POI device 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.	**20-5.a** If the key-injection facility loads DUKPT keys, examine documented procedures for generation and use of BDKs to verify they require use of separate BDKs per terminal type. **20-5.b** Observe key-loading processes for a sample of terminal types used by a single entity, to verify that separate BDKs are used for each terminal type.
20-6 Remote Key-Establishment and Distribution Applications The following requirements apply to key-injection facilities participating in remote key-establishment and distribution applications: • Keys must be uniquely identifiable in all hosts and PTS POI Devices. Keys must be identifiable via cryptographically verifiable means—e.g., through the use of digital signatures or key check values • Key pairs must be unique per PTS POI device	**20-6.a** For techniques involving public key cryptography, examine documentation and develop a schematic to illustrate the process, including: • The size and sources of the parameters involved, and • The mechanisms utilized for mutual device authentication for both the host and the POI device. **20-6.b** If key-establishment protocols using public-key cryptography are used to distribute secret keys, examine/observe to verify that: • Cryptographic mechanisms exist to uniquely identify the keys. • Key pairs used by PTS POI devices are unique per device.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 21: *Secret keys used for enciphering account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.*	
Key-injection facilities (or applicable entities providing key-management services) must ensure that KEKs and account-data-encryption keys do not exist outside of SCDs except when encrypted or stored under dual control and split knowledge. *Some key-injection platforms use personal-computer (PC)-based software applications or similar devices whereby cleartext secret and/or private keys and/or their components exist in memory outside the secure boundary of an SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key-injection facilities that use PC-based key-loading software platforms whereby cleartext secret and/or private keys and/or their components exist in memory outside the secure boundary of an SCD must minimally implement the compensating controls outlined in* ***Requirement 13.***	
Note for hybrid decryption solutions: *Requirements specific to hybrid decryption solutions are denoted throughout* ***Control Objective 6****.*	
21-1 Secret or private keys must only exist in one or more of the following forms: • At least two separate key shares (secret or private) or full-length components (secret) • Encrypted with a key of equal or greater strength as delineated in Annex C • Contained within a secure cryptographic device	**21-1.a** Examine documented procedures for key storage and usage to verify that secret or private keys only exist in one or more approved forms at all times when stored *(with the exception of DDKs used on the Host System for hybrid decryption solutions)*.
Note: *Key-injection facilities may have cleartext keying material outside of an SCD when used within a secure room in accordance with Requirement 32.* ***Note for hybrid decryption solutions:*** *Cleartext data Decryption Keys (DDKs) may temporarily be retained by the Host System in volatile memory for the purpose of decrypting account data.*	**21-1.b** Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored *(with the exception of DDKs used on the Host System for hybrid decryption solutions)*.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
21-2 Wherever key components/shares are used, they must have the following properties:	**21-2** Examine documented procedures and interview responsible personnel to determine all instances where key components/shares are used.
21-2.1 Knowledge of any one key component/share must not convey any knowledge of any part of the actual cryptographic key.	**21-2.1** Examine processes for creating key components/shares to verify that knowledge of any one key component/ share does not convey any knowledge of any part of the actual cryptographic key.
21-2.2 Construction of the cryptographic key must require the use of at least two key components/shares.	**21-2.2** Observe processes for constructing cryptographic keys to verify that at least two key components/shares are required for each key construction.
21-2.3 Each key component/share must have one or more specified authorized custodians.	**21-2.3.a** Examine documented procedures for the use of key components/shares and interview key custodians and key-management supervisory personnel to verify that each key component/share is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component/share.
	21-2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components or shares are designated as key custodians for those particular components/shares.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
21-2.4 Procedures must exist to ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private key cryptographic key. ***Note:*** *For example, in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three shares are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one share. If a custodian was previously assigned share A, which was then reassigned, the custodian must not then be assigned share B or C, as this would give them knowledge of two shares, which gives them the ability to recreate the key.* *In an m-of-n scheme where n=5, where three shares are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key shares (e.g., share A and share B; and a second custodian (with, in this example, share C) would be required to reconstruct the final key, ensuring that dual control is maintained.*	**21-2.4.a** Examine documented procedures for the use of key components/shares to verify that procedures ensure that no custodian ever has access to sufficient key components or shares to reconstruct a secret or private cryptographic key. **21-2.4.b** Examine key-component/share access controls and access logs to verify that authorized custodians cannot access sufficient key components or shares to reconstruct a secret or private cryptographic key.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
21-3 Key components/shares must be stored as follows:	**21-3** Examine documented procedures, interview responsible personnel and inspect key-component/share storage locations to verify that key components/shares are stored as outlined in Requirements **21-3.1** through **21-3.3** below:
21-3.1 Key components that exist in cleartext outside of an SCD must be sealed in individual opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging. ***Note:*** *Tamper-evident authenticable packaging—opacity may be envelopes within tamper-evident packaging—used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.*	**21-3.1.a** Examine key components and storage locations to verify that components are stored in individual opaque, pre-numbered, tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging.
	21-3.1.b Examine tamper-evident packaging used to secure key components—e.g., is the package sufficiently opaque to prevent reading of a component—and ensure that it prevents the determination of the key component without visible damage to the packaging.
	21-3.1.c Examine/observe cleartext key components to verify they do not exist in non-secure containers, such as databases or in software programs.
	21-3.1.d Examine/observe to 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).
21-3.2 Key components/shares for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys—e.g., desk drawers—are not sufficient to meet this requirement.* *Components/shares for a specific key that are stored in separate envelopes, but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers.*	**21-3.2** Examine/observe each key component/share storage container and verify the following: • Key components/shares for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s).

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
21-3.3 If a key component /share is stored on a token, and an access code (e.g., a PIN or similar access-control mechanism) is used to access the token, only that token's owner or designated backup(s) must have possession of both the token and its access code.	**21-3.3** Interview responsible personnel and observe implemented processes to verify that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its access code.
21-4 Private keys used to sign certificates, certificate status lists, messages, or for key protection must exist only in one or more of the following forms: • Within a secure cryptographic device that meets applicable PCI PTS or FIPS 140-2/140-3 level 3 or higher requirements for such a device, • Encrypted using an algorithm and key size of equivalent or greater strength as delineated in Annex C, or • As components using a recognized secret-sharing scheme (e.g., Shamir) that are at all times managed under dual control and split knowledge.	**21-4.a** Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times. **21-4.b** Observe key-management operations and interview key custodians and key-management supervisory personnel to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.
Requirement 22: *Procedures must exist and must be demonstrably in use to replace any key determined to be compromised, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to values not feasibly related to the original keys.*	
Key-injection facilities (or applicable entities providing key-management services) must have written procedures to follow in the event of compromise of any key associated with the key-injection platform and process. Written procedures must exist, and all parties involved in cryptographic key loading must be aware of those procedures. All key-compromise procedures must be documented.	
22-1 Procedures for known or suspected compromised keys must include the following:	**22-1** Examine documented procedures for replacing known or suspected compromised keys to verify they include all of the following (**22-1.1** through **22-1.5** below):
22-1.1 Key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD *(or, for hybrid decryption solutions, the Host System)* has been compromised.	**22-1.1** Interview responsible personnel and observe implemented processes to verify key components/shares are never reloaded when there is any suspicion that either the originally loaded key or the SCD *(or, for hybrid decryption solutions, the Host System)* has been compromised.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
22-1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD *(or, for hybrid decryption solutions, the Host System)* has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.	**22-1.2** Interview responsible personnel and observe implemented processes to verify that if unauthorized alteration is suspected, new keys are not installed until the SCD *(or, for hybrid decryption solutions, the Host System)* has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.
22-1.3 A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s). ***Note:*** *The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.* *Known or suspected substitution of a secret key must result in the replacement of that key and based on an analysis of how the key was substituted, any associated key-encipherment keys that may have been compromised.*	**22-1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, and all the following are performed: • Use of that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.
22-1.4 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including:	**22-1.4.a** Interview responsible personnel and examine documented processes to verify key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s).

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
• Identification of key personnel • A damage assessment including, where necessary, the engagement of outside consultants • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	**22-1.4.b** Examine/observe notifications to verify they include the following: • A damage assessment including, where necessary, the engagement of outside consultants. • Details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.
22-1.5 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: • Missing secure cryptographic devices • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • Host System tamper-detection mechanism has been activated, for hybrid decryption solutions	**22-1.5** Interview responsible personnel and examine documented procedures to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries • Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities • Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation • Host System tamper-detection mechanism has been activated, for hybrid decryption solutions
22-2 If attempts to load a secret key or key component into a KLD or POI device (or a Host System, for hybrid decryption solutions) fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (or Host System).	**22-2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an KLD or POI device (or a Host System, for hybrid decryption solutions) fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original KLD or POI device (or Host System).

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
22-3 Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.	**22-3** Examine documented procedures, interview personnel, and observe processes to confirm that Root CAs provide for segmentation of risk to address key compromise.
22-4 Mechanisms must be in place to respond to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke or otherwise invalidate the usage of subordinate certificates, and notification of affected entities.	**22-4.a** Examine documented procedures to verify that mechanisms are defined to respond to compromise of a CA. Verify the mechanisms include procedures to: • Revoke subordinate certificates, and • Notify affected entities.
	22-4.b Interview responsible personnel to verify that the defined mechanisms to respond to compromise of a CA are in place and include: • Revoke subordinate certificates, and • Notify affected entities.
22-4.1 The CA must cease issuance of certificates if a compromise is known or suspected and perform a damage assessment, including a documented analysis of how and why the event occurred.	**22-4.1.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.
	22-4.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: • The CA will cease issuance of certificates. • The CA will perform a damage assessment, including a documented analysis of how and why the event occurred.
22-4.2 In the event of confirming a compromise, the CA must determine whether to revoke and reissue all signed certificates with a newly generated signing key.	**22-4.2.a** Examine documented procedures to verify that in the event of a confirmed compromise, procedures are defined for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.
	22-4.2.b Interview responsible personnel to verify procedures are followed for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
22-4.3 Mechanisms (e.g., time stamping) must exist to prevent the usage of fraudulent certificates, once identified.	**22-4.3.a** Examine documented procedures to verify that mechanisms are defined to prevent the usage of fraudulent certificates.
	22-4.3.b Interview responsible personnel and observe implemented mechanisms to verify the prevention of the use of fraudulent certificates.
22-4.4 The compromised CA must notify any superior or subordinate CAs of the compromise. The compromise damage analysis must include a determination of whether subordinate CAs and KDHs must have their certificates reissued and distributed to them or be notified to apply for new certificates.	**22-4.4.a** Examine documented procedures to verify that the following procedures are required in the event of a compromise: • The CA will notify any superior CAs. • The CA will notify any subordinate CAs. • The CA will perform a damage assessment to determine the need to either: – Reissue and distribute certificates to affected parties, or – Notify the affected parties to apply for new certificates.
	22-4.4.b Interview responsible personnel to verify that the following procedures are performed in the event a compromise: • The CA notifies any superior CAs. • The CA notifies any subordinate CAs. • The CA performs a damage assessment to determine the need to either: – Reissues and distributes certificates to affected parties, or – Notifies the affected parties to apply for new certificates.
22-5 Minimum cryptographic strength for the CA system must be: • Root and subordinate CAs have a minimum RSA 2048 bits or equivalent; • POI devices and KDHs have a minimum RSA 2048 bits or equivalent. The key-pair lifecycle must result in expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.	**22-5.a** Interview appropriate personnel and examine documented procedures for the creation of these keys.
	22-5.b Examine/observe as needed to verify that the following minimum key sizes exist for RSA keys or the equivalent for the algorithm used as defined in Annex C: • 2048 for CAs • 2048 for KDHs and POI devices
	22-5.c Examine/observe as needed to verify that KDH keys expire every five years unless another mechanism exists to prevent the use of a compromised KDH private key.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 23: *Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.* *Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.* *Keys generated with a non-reversible process, such as key derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*	
23-1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from account-data keys. ***Note:*** *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*	**23-1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.
	23-1.b Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
23-2 An MFK used by host processing systems for encipherment of keys for local storage—and variants of the MFK—must not be used external to the (logical) configuration that houses the MFK itself. For example, MFKs and their variants used by host processing systems for encipherment of keys for local storage must not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration. ***Note:*** *A logical configuration is defined as one where all the components form a system used to undertake a particular task and are managed and controlled under a single operational and security policy.*	**23-2.a** Interview responsible personnel to determine which host MFKs keys exist as variants. ***Note:*** *Some HSMs may automatically generate variants or control vectors for specific keys, but it is still up to the entity to specify exact usage.* **23-2.b** Examine vendor documentation to determine support for key variants. **23-2.c** Examine network schematics detailing transaction flows with the associated key usage and identification of the sources of the keys used to verify that variants of the MFK are not used external to the logical configuration that houses the MFK.
23-3 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys e.g., DEKs from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key or working keys with different purposes from another working key. ***Note:*** *Using transformations of keys across different levels of a key hierarchy—e.g., generating a DEK from a key-encrypting key—increases the risk of exposure of each of those keys.* *It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.*	**23-3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys • Variants of working keys must only be calculated from other working keys.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 24: *Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.*	
24-1 Instances of secret or private keys, and their key components, that are no longer used or that have been replaced by a new key must be destroyed.	**24-1.a** Examine documented procedures to verify they are in place for destroying secret or private keys, and their key components that are no longer used or that have been replaced by a new key.
	24-1.b Observe a sample of keys and key components to verify that they 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.
	24-1.c Examine storage locations for the sample of destroyed keys to verify they are no longer kept.
24-2 The procedures for destroying key components or shares that are no longer used or have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered. For written components, this must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient. ***Note:*** *Key destruction for keys installed in HSMs and POI devices is addressed in* ***Requirement 31****.*	**24-2.a** Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.
	24-2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.
24-2.1 Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic database backups of cryptograms), or components—must be destroyed following the procedures outlined in *ISO–9564* or *ISO–11568*. ***Note:*** *For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.*	**24-2.1.a** Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—must be destroyed following the procedures outlined in *ISO–9564* or *ISO–11568.*
	24-2.1.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or component—are destroyed following the procedures outlined in *ISO–9564* or *ISO–11568.*

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
24-2.2 The key-destruction process must be observed by a third party other than the custodians of any component of that key—i.e., the third party must not be a key custodian for any part of the key being destroyed. The third-party witness must sign an affidavit of destruction, and this affidavit is retained for a minimum of two years.	**24-2.2.a** Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian for any component of that key.
	24-2.2.b Examine key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key-destruction process.
24-2.3 Key components for keys other than the HSM or KLD MFKs that have been successfully loaded and confirmed as operational must also be destroyed, unless the HSM does not store the encrypted values on a database but only stores the subordinate keys internal to the HSM. BDKs used in KLDs may also be stored as components where necessary to reload the KLD.	**24-2.3.a** Examine documented procedures to verify they include destroying key components of keys once the keys are successfully loaded and validated as operational.
	24-2.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.
Requirement 25: *Access to secret and private cryptographic keys and key material must be:* *a) Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and* *b) Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.*	
25-1 To reduce the opportunity for key compromise, the number of key custodians must be limited to the minimum required for operational efficiency. Controls must include:	**25-1** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:
25-1.1 Designate key custodian(s) for each component, such that the fewest number (e.g., a primary and a backup) of key custodians are assigned as necessary to enable effective key management. Key custodians must be employees or contracted personnel.	**25-1.1** Examine key-custodian assignments for each component to verify that: • Key custodian(s) are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.	**25-1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form.
	25-1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form.
25-1.3 Each key-custodian form provides the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access	**25-1.3** Examine all key-custodian forms to verify that they include the following: • Specific authorization for the custodian • Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them • Signature of the custodian acknowledging their responsibilities • An effective date and time for the custodian's access • Signature of management authorizing the access

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-1.4 In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual except as noted below for organizations of insufficient size. ***Note**: For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual.* The components collectively held by an individual and his or her direct reports must not constitute a quorum (or must not provide any information about the value of the key that is not derivable from a single component). A custodian must not become a custodian for a component/share of a key where the custodian has previously been or is currently a custodian for another component/share of that key if that would collectively constitute a quorum to form the actual key. When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented. *(continued on next page)*	**25-1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisors possess the necessary threshold of key components sufficient to form any given key. • A key custodian is not and has not been a custodian for another component/share of a key where that collectively would constitute a quorum to form the actual key.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-1.4 *continued* Organizations that are of insufficient size that they cannot support the reporting-structure requirement must: • Ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian); • Receive explicit training to instruct them from sharing key components with their direct manager; • Sign key-custodian agreements that include an attestation to the requirement; and • Receive training that includes procedures to report any violations.	**25-1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, examine documented procedures and observe they are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes procedures to report any violations.
25-2 All user access to material that can be used to construct secret and private keys (such as key components or key shares used to reconstitute a key) must be directly attributable to an individual user (e.g., through the use of unique IDs). ***Note:*** *Individual user IDs may be assigned to a role or group.*	**25-2.a** Examine documented procedures to confirm that access to material that can be used to construct secret and private keys is directly attributable to an individual user.
	25-2.b Observe the access-control mechanisms in place to verify that access to material that can be used to construct secret and private keys is directly attributable to an individual user.
25-2.1 All user access must be restricted to actions authorized for that role. ***Note:*** *Examples of how access can be restricted include the use of CA software and operating-system and procedural controls.*	**25-2.1.a** Examine documented procedures to confirm that access to material that can be used to construct secret and private keys must be restricted to actions authorized for that role.
	25-2.1.b Observe user role assignments and access-control mechanisms to verify that access to material that can be used to construct secret and private keys is restricted to actions authorized for that role.
25-3 The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include the following:	

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-3.1 CA systems that issue certificates to other CAs and KDHs must be operated offline using a dedicated closed network (not a network segment). • The network must only be used for certificate issuance and/or revocation. • Outside network access (e.g., using a separate platform in the DMZ) must exist only for the purposes of "pushing" certificate-status information to relying parties (e.g., KDHs).	**25-3.1** Examine network diagrams and observe network and system configurations to verify: • CA systems that issue certificates to other CAs and KDHs are operated offline using a dedicated closed network (not a network segment). • The network is only used for certificate issuance, revocation, or both certificate issuance and revocation. • Outside network access must exist only for the purposes of "pushing" certificate-status information to relying parties (e.g., KDHs).
25-3.2 For CAs operated online—e.g., POI-signing CAs: CA or Registration Authority (RA) software updates must not be done over the network (local console access must be used for CA or RA software updates).	**25-3.2** Examine software update processes to verify that local console access is used for all CA or RA software updates.
25-3.3 For CAs operated online—e.g., POI-signing CAs: Non-console access must use multi-factor authentication. This also applies to the use of remote console access.	**25-3.3** Examine remote-access mechanisms and system configurations to verify that all non-console access, including remote access, requires multi-factor authentication.
25-3.4 For CAs operated online—e.g., POI-signing CAs: Non-console user access to the CA or RA system environments must be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. ***Note:*** *Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.*	**25-3.4.a** Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions. **25-3.4.b** Observe an authorized CA personnel attempt non-console access to the host platform using valid CA credentials without using an authenticated encrypted session to verify that non-console access is not permitted.
25-3.5 CA certificate (for POI/KDH authentication and validity status checking) signing keys must only be enabled under at least dual control. ***Note:*** *Certificate requests may be vetted (approved) using single user logical access to the RA application.*	**25-3.5.a** Examine the certificate security policy and certification practice statement to verify that CA certificate-signing keys must only be enabled under at least dual control. **25-3.5.b** Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-4 The CA must require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as "dual control." At a minimum, there must be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).	**25-4.a** Examine documented procedures to verify they include the following: • Definition of critical functions of the CA • Separation of duties to prevent one person from maliciously using a CA system without detection • Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s)
	25-4.b Observe CA operations and interview responsible personnel to verify: • Definition of Critical functions of the CA • Separation of duties to prevent one person from maliciously using a CA system without detection • Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s)
25-5 All CA systems that are not operated exclusively offline must be hardened to prevent insecure network access, to include: • Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, telnet, ftp, etc.) must be removed or disabled. • Unnecessary ports must also be disabled. • Documentation must exist to support the enablement of all active services and ports.	**25-5.a** Examine system documentation to verify the following is required: • Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, etc., commands in UNIX) must be removed or disabled. • Unnecessary ports must also be disabled. • Documentation must exist to support the enablement of all active services and ports.
	25-5.b For a sample of systems, examine documentation supporting the enablement of active services and ports, and observe system configurations to verify: • Services that are not necessary or that allow non-secure access (e.g., rlogin, rshell, etc., commands in UNIX) are removed or disabled. • Unnecessary ports are disabled. • There is documentation to support all active services and ports.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-5.1 All vendor-default IDs must be changed, removed, or disabled unless necessary for a documented and specific business reason. Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades must only be enabled when necessary and otherwise must be disabled from login.	**25-5.1.a** Examine documented procedures to verify that: • Vendor-default IDs are changed, removed, or disabled unless necessary for a documented and specific business reason. • Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades are only be enabled when required and otherwise must be disabled from login.
	25-5.1.b Examine system configurations and interview responsible personnel to verify that: • Vendor-default IDs are changed, removed or disabled unless necessary for a documented and specific business reason. • Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades are only be enabled when required and otherwise must be disabled from login.
25-5.2 Vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step must be changed, removed, or disabled before installing a system on the network.	**25-5.2.a** Examine documented procedures to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.
	25-5.2.b Examine system configurations and interview responsible personnel to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-6 Audit trails must include but not be limited to the following: • All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, destruction, and certificate generation or revocation • The identity of the person authorizing the operation • The identities of all persons handling any key material (such as key components or keys stored in portable devices or media) • Protection of the logs from alteration and destruction	**25-6.a** Examine system configurations and audit trails to verify that all key-management operations are logged.
	25-6.b For a sample of key-management operations, examine audit trails to verify they include: • The identity of the person authorizing the operation • The identities of all persons handling any key material • Mechanisms exist to protect logs from alteration and destruction
25-6.1 Audit logs must be archived for a minimum of two years.	**25-6.1** Examine audit trail files to verify that they are archived for a minimum of two years.
25-6.2 Records pertaining to certificate issuance and revocation must be retained for the life of the associated certificate, at a minimum.	**25-6.2.a** For a sample of certificate issuances, examine audit records to verify that the records are retained for at least the life of the associated certificate.
	25-6.2.b For a sample of certificate revocations, examine audit records to verify that the records are retained for at least the life of the associated certificate.
25-6.3 Logical events are divided into operating-system and CA application events. For both, the following must be recorded in the form of an audit record: • 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	**25-6.3.a** Examine audit trails to verify that logical events are divided into operating-system and CA application events.
	25-6.3.b Examine a sample of operating-system logs to verify they contain the following information: • Date and time of the event, • Identity of the entity and/or user that caused the event, • Type of event, and • Success or failure of the event

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
	25-6.3.c Examine a sample of application logs to verify they contain the following information: • Date and time of the event, • Identity of the entity and/or user that caused the event, • Type of event, and • Success or failure of the event
25-7 CA application logs must use a digital signature or a symmetric MAC (based on one of the methods stated in *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration. The signing/MACing key(s) used for this must be protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document.	**25-7.a** Examine log security controls to verify that CA application logs use a digital signature or a symmetric MAC (based on one of the methods stated in *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration.
	25-7.b Examine documentation and interview personnel and observe to verify that signing/MACing key(s) used for this are protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-7.1 Certificate-processing system components operated online must be protected by a firewall(s) from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to: • Deny all services not explicitly permitted. • Disable or remove all unnecessary services, protocols, and ports. • Fail to a configuration that denies all services and require a firewall administrator to re-enable services after a failure. • Disable source routing on the firewall. • Not accept traffic on its external interfaces that appears to be coming from internal network addresses. • Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. • Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled.	**25-7.1.a** Examine network and system configurations to verify that certificate-processing system components operated online are protected from unauthorized access by firewall(s). **25-7.1.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. • 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.
25-7.2 Online certificate-processing systems must employ individually, or in combination, network and host-based intrusion detection systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments, must be covered.	**25-7.2.a** Observe network-based and/or host-based IDS configurations to verify that on-line certificate-processing systems are protected by IDS to detect inappropriate access. **25-7.2.b** Examine/observe that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25-8 Implement user-authentication management for all system components as follows:	
25.8.1 Initial, assigned passphrases are pre-expired (user must replace at first logon).	**25.8.1** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and are pre-expired.
25.8.2 Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.	**25.8.2.a** For a sample of system components, examine user ID lists to verify the following: • Generic user IDs and accounts are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used.
	25.8.2.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.
	25.8.2.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.
25.8.3 If passwords are used, system-enforced expiration life must not exceed 90 days and a minimum life at least one day.	**25.8.3** For a sample of system components, examine system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days and have a minimum life of at least one day.
25.8.4 Passwords must have a minimum length of eight characters using a mix of alphabetic, numeric, and special characters or equivalent strength as defined in *NIST SP 800-63b.*	**25.8.4** For a sample of system components, examine system configuration settings to verify that password parameters are set to require passwords to be at least eight characters long and contain numeric, alphabetic, and special characters or equivalent strength as defined in *NIST SP 800-63b.*
25.8.5 Limit repeated access attempts by locking out the user ID after not more than five attempts.	**25.8.5** For a sample of system components, examine 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.
25.8.6 Authentication parameters must require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.	**25.8.6** For a sample of system components, examine system configuration settings to verify that authentication parameters are set to require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
25.8.7 Passwords are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.	**25.8.7** For a sample of system components, examine system configuration settings to verify that passwords are not stored unless encrypted as part of a proprietary one-way hash.
25.8.8 The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.	**25.8.8.a** Examine policies and procedures and interview personnel to determine that the embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.
	25.8.8.b Examine a sample of shell scripts, command files, communication scripts, etc. to verify that passwords are not embedded in shell scripts, command files, or communication scripts.
25.8.9 Where log-on security tokens (e.g., smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage. The PIN/passphrase must be at least eight decimal digits in length, or equivalent. ***Note:*** *Log-on security tokens (e.g., smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.*	**25.8.9.a** If log-on security tokens are used, observe devices in use to verify that the security tokens have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage.
	25.8.9.b Examine token-configuration settings to verify parameters are set to require that PINs/passwords be at least eight decimal digits in length, or equivalent.
25.9 Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.	**25.9.a** Examine documented procedures and system configuration standards to verify a method is defined to synchronize all critical system clocks and times for all systems involved in key-management operations.
	25.9.b For a sample of critical systems, examine the time-related system parameters to verify that system clocks and times are synchronized for all systems involved in key-management operations.
	25.9.c If a manual process is defined, examine documented procedures to verify they require that it occur at least quarterly.
	25.9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 26: *Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.*	
Key-injection facilities (or applicable entities providing key-management services) must maintain logs for the key management of all keys and keying material used in all key-loading sessions. These include keys and materials removed from safes and used in the loading process.	
26-1 Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. The logs must be securely stored, for example, in a secure container with the associated key components. These logs must be archived for a minimum of two years subsequent to key destruction. At a minimum, logs must include the following: • Date and time in/out • Key-component identifier • Purpose of access • Name and signature of custodian accessing the component • Name and signature of a non-custodian (for that component/share) witness • Tamper-evident and authenticable package number (if applicable)	**26-1.a** Interview responsible personnel and examine documented procedures to determine the following: • Logs are kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. • Logs are securely stored, for example, in a secure container with the associated key components. • Logs must be archived for a minimum of two years subsequent to key destruction
	26-1.b Examine log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD
	26-1.c Examine log files and verify they are: • Archived for a minimum of two years subsequent to key destruction • Securely stored
	26-1.d Examine log files and audit log settings to verify that logs include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Name and signature of a non-custodian (for that component/share) witness • Tamper-evident and authenticable package number (if applicable)

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 27: *Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.* ***Note:*** *It is not a requirement to have backup copies of key components or keys.*	
Note for hybrid decryption solutions: *Cleartext cryptographic keys used on the Host System must not be included in any system back-up (refer to Requirement 4D-1.14)*	
27-1 If backup copies of secret and/or private keys exist, they must be maintained in accordance with the same requirements as are followed for the primary keys.	**27-1.a** Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following:
	27-1.b Observe backup processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys.
	27-1.c Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: • Securely stored with proper access controls • Under at least dual control • Subject to at least the same level of security control as operational keys as specified in this document
27-2 If backup copies are created, the following must be in place: • Creation (including cloning) of top-level keys—e.g., MFKs—must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components.	**27-2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies for top-level keys requires at least two authorized individuals to enable the process • All requirements applicable for the original keys also apply to any backup copies of keys and their components.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 28: *Documented procedures must exist and must be demonstrably in use for all key-administration operations.*	
28-1 Written procedures must exist, and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as: • Training of all key custodians regarding their responsibilities, and forming part of their annual security training • Role definition—nominated individual with overall responsibility • Background checks for personnel (within the constraints of local laws) • Management of personnel changes, including revocation of access control and other privileges when personnel move	**28-1.a** Examine documented procedures for key-administration operations to verify they cover all activities related to key administration, and include: • Training of all key custodians regarding their responsibilities, and forming part of their annual security training • Role definition—nominated individual with overall responsibility • Background checks for personnel (within the constraints of local laws) • Management of personnel changes, including revocation of access control and other privileges when personnel move
	28-1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.
	28-1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.
	28-1.d Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).
28-2 CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.	**28-2.a** Examine documented procedures to verify: • CA operations must be dedicated to certificate issuance and management. • All physical and logical CA system components must be separated from key-distribution systems.
	28-2.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.
	28-2.c Observe system and network configurations and physical access controls to verify that all physical and logical CA system components are separated from key-distribution systems.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
28-3 Each CA operator must develop a certification practice statement (CPS). (See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.) • The CPS must be consistent with the requirements described within this document. • The CA must operate in accordance with its CPS. ***Note:*** *This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific, single document or a collection of specific documents.* The CPS must be consistent with the requirements described within this document. The CA must operate in accordance with its CPS.	**28-3.a** Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document. **28-3.b** Examine documented operating procedures to verify they are defined in accordance with the CPS. **28-3.c** Interview personnel and observe CA processes to verify that CA operations are in accordance with its CPS.
28-4 Each CA operator must develop a certificate policy. (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content.)	**28-4** Examine documented certificate policy to verify that the CA has one in place.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**

28-5 Documented procedures exist and are demonstrably in use by CAs to validate the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key where the certificate request is not generated within the same secure room meeting the requirements of the Level 3 environment defined below. These procedures must include at a minimum, two or more of the following for KDH certificate requests:
• Verification of the certificate applicant's possession of the associated private key through the use of a digitally signed certificate request pursuant to PKCS #10 or another cryptographically equivalent demonstration;
• Determination that the requestor is valid, which may include but not limited to verifying that the:
  • organization exists by using at least one third-party identity-proofing service or database, or,
  • organizational documentation issued by or filed with the applicable government agency or competent authority confirms the existence of the organization;
• Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant to confirm that the organization has authorized the certificate application, confirmation of the employment of the representative submitting the certificate application on behalf of the certificate applicant, and confirmation of the authority of the representative to act on behalf of the certificate applicant;
• Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant's representative to confirm that the person
	28-5.a Examine documented procedures to verify that unless the certificate request is generated within the same secure room meeting the requirements of the Level 3 environment, they include validating the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.
	
	28-5.b Observe certificate-issuing processes to verify that the identities of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key.

Control Objective 6: Keys are administered in a secure manner	
Domain 5 Requirements	**Testing Procedures**
named as representative has submitted the certificate application.	
28-5.1 For CA and KDH certificate-signing requests, including certificate or key-validity status changes—e.g., revocation, suspension, replacement—verification must include validation that: • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.	**28-5.1.a** Examine documented procedures to verify that certificate-signing requests, including certificate or key-validity status changes, require validation that: • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.
	28-5.1.b Observe certificate-signing requests, including certificate or key-validity status changes, to verify they include validation that: • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.
28-5.2 RAs must retain documentation and audit trails relating to the identification of entities for all certificates issued and certificates whose status had changed for the life of the associated certificates.	**28-5.2** Examine documentation and audit trails to verify that the identification of entities is retained for the life of the associated certificates: • For all certificates issued • For all certificates whose status had changed

Control Objective 7: Equipment used to process account data and keys is managed in a secure manner	
Domain 5 Requirements	**Testing Procedures**
Requirement 29: *Equipment used to protect account data (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device—both prior to and subsequent to the loading of cryptographic keys—and that precautions are taken to minimize the threat of compromise once deployed.*	
Note: *Where POI is mentioned in* ***Requirement 29****, the requirements apply to the solution provider managing PTS POI devices prior to deployment to distribution channels or to the merchants that will process payments with the POI device. Merchant protection and use of PTS POI devices once deployed are not the subject of these P2PE requirements and are instead covered by guidance provided to merchants by the solution provider in the P2PE Instruction Manual (PIM). See the PIM Template for more information about guidance required to be included in the PIM.* *Likewise, distribution channels used by a solution provider to distribute POI devices to the end merchant are also not the subjects of these P2PE requirements. However, regardless of the distribution channel used, the merchant that will process payments with the device must be able to confirm that the device and packaging have not been tampered with via instructions provided in the PIM. For example, this could be done via secure inner packaging that easily shows evidence that it has been tampered with or opened previously via instructions provided to the merchant in the PIM. The merchant in such scenarios must also be able to establish secure, confirmed communications with the solution provider via the POI device keys, also with instructions provided in the PIM.*	
Key-injection facilities (or applicable entities providing key-management services) must ensure that only legitimate, unaltered devices are loaded with cryptographic keys. *Secure rooms must be established for inventory that includes securing POI devices that have not had keys injected. The area must have extended walls from the real floor to the real ceiling using sheetrock, wire mesh, or equivalent. Equivalence can be steel cages extending floor to real ceiling. The cages can have a steel cage top in lieu of the sides extending to the real ceiling. The cages must have locks (with logs) or badge control with logging for entry.*	

Control Objective 7: Equipment used to process account data and keys is managed in a secure manner	
Domain 5 Requirements	**Testing Procedures**
29-1 Secure cryptographic devices—such as HSMs and PTS POI devices—must be placed into service only if there is assurance that the equipment has not been subjected to unauthorized modifications, substitution, or tampering and has not otherwise been subject to misuse prior to deployment. ***Note**: This also applies to SCDs used for key injection.*	**29-1.a** Examine documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key-injection/loading have not been substituted or subjected to unauthorized modifications or tampering.
	29-1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POI devices have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key-injection/loading have not been substituted or subjected to unauthorized modifications or tampering.
29-1.1 All POI devices and other SCDs must be protected against compromise. Any compromise must be detected. Loading and use of any financial keys after the compromise must be prevented. Controls must include the following:	**29-1.1** Examine documented procedures to verify controls are defined to protect POI devices and other SCDs from unauthorized access up to point of deployment.

29-1.1.1 Access to all PTS POI devices and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection. The minimum log contents include date and time, object name/identifier, purpose, name of individual(s) involved, signature or electronic capture (e.g., badge) of individual involved and, if applicable, tamper-evident package number(s) and serial number(s) of device(s) involved. Electronic logging—e.g., using bar codes—is acceptable for device tracking.	**29-1.1.1.a** Examine access-control documentation and device configurations to verify that access to all POI devices and key-injection/loading devices is defined and documented.
	29-1.1.1.b For a sample of POI device types and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POI devices and other SCDs is logged.
	29-1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI device or other SCD.
29-1.1.2 All personnel with access to PTS POI devices and other SCDs **prior to deployment** are documented in a formal list and authorized by management. A documented security policy must exist that requires the specification of personnel with authorized access to all secure cryptographic devices. This includes documentation of all personnel with access to PTS POI devices and other SCDs as authorized by management. The list of authorized personnel is reviewed at least annually. ***Note:*** *"Prior to deployment" for this requirement means prior to the solution provider (or component provider) sending POI devices to either a distribution channel or the end merchant who will use the POI device to process payment transactions.*	**29-1.1.2.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POI devices and other SCDs are authorized by management in an auditable manner. • The authorizations are reviewed annually.
	29-1.1.2.b For a sample of POI device types and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in an auditable manner have access to devices.
29-1.2 PTS POI devices and other SCDs must not use default keys or data (such as keys that are pre-installed for testing purposes) or passwords/authentication codes.	**29-1.2.a** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data.
	29-1.2.b Observe implemented processes and interview personnel to verify that default keys or passwords are not used.

29-2 Implement a documented “chain of custody” to ensure that all devices are controlled from receipt to placement into service. The chain of custody must include records to identify responsible personnel for each interaction with the devices. ***Note:*** *Chain of custody includes procedures, as stated in* ***Requirement 29-1****, that ensure that access to all PTS POI devices and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection.*	**29-2.a** Examine documented processes to verify that the chain of custody is required for devices from receipt to placement into service.
	29-2.b For a sample of devices, examine documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to placement into service.
	29-2.c Examine the chain-of-custody records to verify they identify responsible personnel for each interaction with the device.

29-3 Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion or deployment, through one or more of the following: • Transportation using a trusted courier service (e.g., via bonded carrier). The devices are then securely stored until key-insertion occurs. • Use of physically secure and trackable packaging (e.g., pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored in such packaging, or in secure storage, until key-insertion occurs. • A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. The SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key, and the device is further protected until deployment. • Upon tamper of the device, it becomes infeasible to load any keying material. • Shipped and stored containing a secret that: – Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and – Can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel. *(continued on next page)*	**29-3.a** Examine documented procedures to verify they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods.

29-3 *(continued)* • Each cryptographic device is carefully inspected and tested immediately prior to key-insertion and deployment using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized access or modifications. ***Note:*** *Unauthorized access includes that by customs officials.* ○ Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised. *(**Note**: this control must be used in conjunction with one of the other methods.)* ○ Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.	**29-3.b** Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion and deployment.
29-4 Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or backup devices—throughout their lifecycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs, but cannot supplant the implementation of dual-control mechanisms. ***Note:*** *Dual-control mechanisms can include any manner of physical and/or logical means that satisfies the objective.*	**29-4.a** Examine documented procedures to verify that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.
	29-4.b Interview responsible personnel and physically verify the dual-control mechanism used to prevent substitution or tampering of HSMs—both in service and spare or back-up devices—throughout their life cycle.

29-4.1 HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment. An example of how serial numbers may be documented by the sender includes but is not limited to manufacturer's invoice or similar document.*	**29-4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.
	29-4.1.b For a sample of received devices, examine sender documentation sent by a different communication channel than the device's shipment (e.g., the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.
29-4.2 The security policy functionality enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required to support specified functionality must be disabled before the equipment is commissioned. Documentation (e.g., a checklist or similar suitable to use as a log) of configuration settings must exist and be signed and dated by personnel responsible for the implementation. This documentation must include identifying information for the HSM, such as serial number and/or asset identifiers. This documentation must be retained and updated for each affected HSM any time changes to configuration settings would impact security.	**29-4.2.a** Examine the defined security policy to be enforced by the HSM.
	29-4.2.b Examine documentation of the HSM configuration settings from past commissioning events to determine that the functions and commands enabled are in accordance with the security policy.
	29-4.2.c For a sample of HSMs, examine the configuration settings to determine that only authorized functions are enabled.
	29-4.2.d *Not used in P2PE*
	29-4.2.e *Not used in P2PE*
	29-4.2.f Examine documentation to verify: • Configuration settings are defined, signed, and dated by personnel responsible for implementation. • It includes identifying information for the HSM, such as serial number and/or asset identifiers. • The documentation is retained and updated anytime configuration setting impacting security occur for each affected HSM.

29-4.3 When HSMs are connected to online systems, controls are in place to prevent the use of an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. ***Note:*** *Examples of sensitive functions include but are not limited to: loading of key components, outputting cleartext key components, and altering HSM configuration.*	**29-4.3** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.
29-4.4 Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised. Processes must include:	**29-4.4** Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify the integrity of the device and include requirements specified at **29-4.4.1** through **29-4.4.4** below.
29-4.4.1 Running self-tests to ensure the correct operation of the device.	**29-4.4.1** Examine records of device inspections and test results to verify that self-tests are run on devices to ensure the correct operation of the device.
29-4.4.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.	**29-4.4.2** Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised.
29-4.4.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed.	**29-4.4.3** Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.
29-4.4.4 Maintaining records of the tests and inspections and retaining records for at least one year.	**29-4.4.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	29-4.4.4.b Examine records of inspections to verify records are retained for at least one year.
29-5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	**29-5.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.
	29-5.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.

Requirement 30: *Physical and logical protections must exist for deployed POI devices.*	
Key-injection facilities (or applicable entities providing key-management services) must ensure protection against unauthorized use of SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.	
30-1 Not used in P2PE	
30-2 Not used in P2PE	
30-3 Processes must exist to ensure that key-injection operations are performed and reconciled on a defined inventory of devices. Processes must include the following: • Each production run must be associated with a predefined inventory of identified POI devices to be injected or initialized with keys. • Unauthorized personnel must not be able to modify this inventory without detection. • All POI devices to be initialized with keys on a production run must be identified and accounted for against the inventory. • Unauthorized POI devices submitted for injection or initialized must be rejected by the injection platform and investigated. • Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices must be identified and accounted for against the inventory. ***Note:*** *The KIF platform must ensure that only authorized devices can ever be injected or initialized with authorized keys. Processes must prevent (1) substitution of an authorized device with an unauthorized device, and (2) insertion of an unauthorized device into a production run.*	**30-3.a** Obtain and examine documentation of inventory control and monitoring procedures. Determine that the procedures cover: • Each production run is associated with a predefined inventory of identified POI devices to be injected or initialized with keys. • Unauthorized personnel are not able to modify this inventory without detection. • All POI devices to be initialized with keys on a production run are identified and accounted for against the inventory. • Unauthorized POI devices submitted for injection or initialized are rejected by the injection platform and investigated. • Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices are identified and accounted for against the inventory. **30-3.b** Interview applicable personnel to determine that procedures are known and followed.

Requirement 31: *Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*	
Key-injection facilities (or applicable entities providing key-management services) must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any SCDs (e.g., HSM) used in the key-injection platform, as well as to any devices that have been loaded with keys and securely stored or warehoused on site that are subsequently deemed to be unnecessary and never to be placed into service. *If a key-injection facility receives a used device to reload with keys, procedures must ensure that old keys that may be in the device are destroyed prior to loading of new keys. (The used device should have had its keys destroyed when it was removed from service, but this is a prudent secondary check that the keys were destroyed.)*	
Note: *The requirements within* ***Requirement 31*** *apply to the solution provider managing POI devices when removed from service, retired at the end of the deployment lifecycle, or returned for repair. Merchant protection and use of POI devices once deployed are not the subjects of these P2PE requirements and are instead covered by guidance provided to merchants by the solution provider in the P2PE Instruction Manual (PIM). See the PIM Template for more information about guidance required to be included in the PIM.*	
31-1 Procedures must be in place to ensure that any SCDs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including rendering all secret and private keys, key material, and account data stored within the device irrecoverable. Processes must include the following: ***Note:*** *Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*	**31-1** Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all secret and private keys, key material, and all account data stored within the device be securely destroyed. • Procedures cover all devices removed from service permanently or for repair. • Procedures cover requirements at **31-1.1** through **31-1.6** below.
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement all critical decommissioning processes. ***Note:*** *Dual control is not explicitly required by the HSM itself. E.g., an HSM with a decommission-type physical button (e.g., a zeroize button) is acceptable provided physical access to the HSM (and therefore the mechanism for decommissioning) requires dual control.*	**31-1.1.a** Examine documented procedures for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes. **31-1.1.b** Interview personnel and observe demonstration (if HSM is available) of processes for removing HSMs from service to verify that dual control is implemented for all critical decommissioning processes.

31-1.2 Keys and account data are rendered irrecoverable (e.g., zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.	**31-1.2** Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material and account data are rendered irrecoverable (e.g., zeroized), or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys.
31-1.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	**31-1.3** Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable.
31-1.4 Affected entities are notified before devices are returned.	**31-1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
31-1.5 Devices are tracked during the return process.	**31-1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
31-1.6 Records of the tests and inspections are maintained for at least one year.	**31-1.6** Interview personnel and observe records to verify that records of the tests and inspections are maintained for at least one year.
Requirement 32: *Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key or signing applications to be loaded onto a POI device, must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:* *a) Dual access controls required to enable the key-encryption function* *b) Physical protection of the equipment (e.g., locked access to it) under dual control* c) *Restriction of logical access to the equipment*	
Key-injection facilities (or applicable entities providing key-management services) 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.	
32-1 For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:	**32-1.a** Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices. **32-1.b** Verify that documented procedures cover requirements **32-1.1** through **32-1.5** below.

32-1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. ***Note:*** *Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords/authentication codes (at least five characters in length), or for physical access via a physical lock that requires two individuals each with a different high-security key.* *For devices that do not support two or more passwords/authentication codes, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian. Each half must be a minimum of five characters.* *Physical keys, authorization codes, passwords/authentication codes, or other enablers must be managed so that no one person can use both the enabler(s) and the device, which can create cryptograms of known keys or key components under a key-encipherment key used in production.*	**32-1.1** Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.
32-1.2 Passwords/authentication codes used for dual control must each be of at least five numeric and/or alphabetic characters.	**32-1.2** Observe password policies and configuration settings to confirm that passwords/authentication codes used for dual control must be at least five numeric and/or alphabetic characters.
32-1.3 Dual control must be implemented for the following: • To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of cleartext key components; • For all access to key-loading devices (KLDs) and authenticated application-signing devices.	**32-1.3** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: • To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing; • To enable application-signing functions; • To place the device into a state that allows for the input or output of cleartext key components; • For all access to KLDs and authenticated application-signing devices.

32-1.4 Devices must not use default passwords/authentication codes.	**32-1.4.a** Examine password policies and documented procedures to confirm default passwords/authentication codes must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists.
	32-1.4.b Observe device configurations and interview device administrators to verify that HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords/authentication codes.
32-1.5 To detect any unauthorized use, devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging, or • Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected. ***Note:*** *For key-injection facilities, or applicable entities providing key-management services, POI devices may be secured by storage in the dual-control access key-injection room.*	**32-1.5.a** Examine and confirm documented procedures require devices are within a secure room and are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
	32-1.5.b Interview responsible personnel and observe devices and processes to confirm that devices are at all times within a secure room and either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.

32-2 Intentionally left blank	
32-2.1 The certificate-processing operations center must implement a three-tier physical security boundary, as follows: • Level One Barrier – Consists of the entrance to the facility. • Level Two Barrier – Secures the entrance beyond the foyer/reception area to the CA facility. • Level Three Barrier – Provides access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices.	**32-2.1.a** Examine physical security policies to verify three tiers of physical security are defined as follows: • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices
	32-2.1.b Observe the physical facility to verify three tiers of physical security are implemented as follows: • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices
Level 1 Barrier	
32-2.2 The entrance to the CA facility/building must include the following controls:	
32-2.2.1 The facility entrance only allows authorized personnel to enter the facility.	**32-2.2.1.a** Examine physical-security procedures and policies to verify they require that the facility entrance allows only authorized personnel to enter the facility.
	32-2.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed to enter the facility.
32-2.2.2 The facility has a guarded entrance or a foyer with a receptionist. No entry is allowed for visitors if the entryway is not staffed—i.e., only authorized personnel who badge or otherwise authenticate themselves can enter when entryway is unstaffed.	**32-2.2.2.a** Examine physical-security procedures and policies to verify they require that the facility have a guarded entrance or a foyer with a receptionist or the entryway prevents access to visitors.
	32-2.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.

32-2.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.	**32-2.2.3.a** Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.
	32-2.2.3.b Observe the facility entrance and observe personnel entering the facility to verify that visitors are authorized and registered in a logbook.
Level 2 Barrier	
32-2.3 The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.	**32-2.3.a** Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the Level 2 barrier/entrance.
	32-2.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.
32-2.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.	**32-2.3.1.a** Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.
	32-2.3.1.b Interview personnel and observe visitors entering the environment to verify that visitors are authorized and escorted at all times within the Level 2 environment.
32-2.3.2 Access logs must record all personnel entering the Level 2 environment. ***Note:*** *The logs may be electronic, manual, or both.*	**32-2.3.2.a** Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.
	32-2.3.2.b Observe personnel entering the Level 2 barrier and examine corresponding access logs to verify that all entry through the Level 2 barrier is logged.
32-2.4 The Level 2 entrance must be monitored by a video-recording system.	**32-2.4.a** Observe the Level 2 entrance to verify that a video-recording system is in place.
	32-2.4.b Examine a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.

Level 3 Barrier	
32-2.5 The Level 3 environment must consist of a physically secure, dedicated room not used for any other business activities but certificate operations. ***Note:*** *All certificate-processing operations must operate in the Level 3 environment.*	**32-2.5.a** Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.
	32-2.5.b Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.
	32-2.5.c Observe operations and interview personnel to confirm that the Level 3 secure room is not used for any business activity other than certificate operations.
32-2.5.1 Doors to the Level 3 secure room must have locking mechanisms.	**32-2.5.1** Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.
32-2.5.2 The Level 3 environment must be enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars. ***Note:*** *For example, the Level 3 environment may be implemented within a "caged" environment.*	**32-2.5.2.a** Examine physical security documentation for the Level 3 environment to verify that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as have true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars
	32-2.5.2.b Examine the physical boundaries of the Level 3 environment to verify that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars and protection from entry from below floors and above ceilings.
32-2.6 Documented procedures must exist for: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical	**32-2.6.a** Examine documented procedures to verify they include the following: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical
	32-2.6.b Interview responsible personnel to verify that the documented procedures are followed for: • Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA • Specific access authorizations, whether logical or physical
32-2.6.1 All authorized personnel with access through the Level 3 barrier must: *(continued on next page)*	**32-2.6.1.a** Examine documented policies and procedures to verify they require personnel authorized as having access through the Level 3 barrier to: • Have successfully completed a background security check. • Be assigned resources of the CA operator with defined business needs and duties.

32-2.6.1 *(continued)* • 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.*	**32-2.6.1.b** Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws) on CA personnel prior such personnel being authorized for access through the Level 3 barrier.
	32-2.6.1.c Interview a sample of personnel authorized for access through the Level 3 barrier to verify that they are assigned resources of the CA with defined business needs and duties.
32-2.6.2 Other personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.	**32-2.6.2.a** Examine documented policies and procedures to verify that personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.
	32-2.6.2.b Interview a sample of responsible personnel to verify that personnel requiring entry to this level are accompanied by two (2) authorized and assigned resources at all times.
32-2.7 The Level 3 environment must require dual-control access and dual-occupancy such that the room is never occupied by one person for more than thirty (30) seconds—i.e., one person may never be in the room for more than 30 seconds alone. ***Note****: For example: The Level 3 room is never occupied by one person except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.*	**32-2.7.a** Examine documented policies and procedures to verify that the Level 3 environment requires dual-control access and dual-occupancy such that the room is never occupied by one person alone for more than thirty (30) seconds.
	32-2.7.b Observe authorized personnel accessing the Level 3 environment to verify that dual-control access and dual-occupancy is enforced such that the room is never occupied by one person alone for more than thirty (30) seconds.
32-2.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated.	**32-2.7.1.a** Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.
	32-2.7.1.b Observe enforcement mechanism configuration to verify it is automated.
32-2.7.2 The system must enforce anti-pass-back.	**32-2.7.2.a** Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.
	32-2.7.2.b Observe mechanisms in use and authorized personnel within the environment to verify that anti-pass-back is enforced by the conduct of a test.

32-2.7.3 Dual occupancy requirements are managed using electronic (e.g., badge and/or biometric) systems.	**32-2.7.3.a** Examine documented policies and procedures to verify that dual occupancy requirements are defined to be managed using electronic (e.g., badge and/or biometric) systems.
	32-2.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic systems.
32-2.7.4 Any time a single occupancy exceeds 30 seconds, the system must automatically generate an alarm and audit event that is followed up by security personnel.	**32-2.7.4.a** Examine documented policies and procedures to verify that any time one person is alone in the room for more than 30 seconds, the system must automatically generate an alarm and an audit event that is followed up by security personnel.
	32-2.7.4.b Observe mechanisms in use to verify that the system automatically generates an alarm event and an audit event when one person is alone in the room for more than 30 seconds.
	32-2.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.
32-2.8 Access to the Level 3 room must create an audit event, which must be logged.	**32-2.8** Observe authorized personnel enter the environment and examine correlating audit logs to verify that access to the Level 3 room creates an audit log event.
32-2.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel	**32-2.8.1** Observe an invalid access attempt and examine correlating audit logs to verify that invalid access attempts to the Level 3 room create an audit log event.
32-2.9 The Level 3 environment must be monitored as follows:	
32-2.9.1 A minimum of one or more cameras must provide continuous monitoring (e.g., CCTV system) of the Level 3 environment, including the entry and exit. ***Note:*** *Motion-activated systems that are separate from the intrusion-detection system may be used to activate recording activity.*	**32-2.9.1.a** Observe the Level 3 physical environment to verify that cameras are in place to monitor the Level 3 environment, including the entry and exit.
	32-2.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.
	32-2.9.1.c If motion-activated systems are used for monitoring, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.

32-2.9.2 The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.	**32-2.9.2** Examine monitoring system configurations to verify; • The system records to time-lapse VCRs or similar mechanisms. • A minimum of five frames are recorded every three seconds.
32-2.9.3 Continuous or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (e.g., when infrared cameras are used).*	**32-2.9.3.a** Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for each camera monitoring the environment.
	32-2.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.
32-2.9.4 Surveillance cameras must be configured to prevent the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data. Cameras must not be able to be remotely adjusted to zoom in or otherwise observe the aforementioned.	**32-2.9.4.a** Observe each camera locations in the Level 3 environment to verify they are not set to monitor computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.
	32-2.9.4.b Examine a sample of captured footage to verify it does not allow for the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.
32-2.9.5 Personnel with access to the Level 3 environment must not have access to the media (e.g., VCR tapes, digital-recording systems, etc.) containing the recorded surveillance data.	**32-2.9.5.a** Examine documented access policies and procedures to verify that personnel with access to the Level 3 environment are not permitted to have access to the media containing recorded surveillance data for that environment.
	32-2.9.5.b Examine Level 3 access lists as well as access controls to the media containing surveillance data, to verify that personnel with access to the Level 3 environment do not have access to the media containing recorded surveillance data.
32-2.9.6 Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy (primary and backup) to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**32-2.9.6.a** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.
	32-2.9.6.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.

32-2.9.7 CCTV images must be backed up daily. The backup recording must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users (personnel accessing the secure room) and administrators of the system. Alternatively, backups may be stored in other facilities via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements.	**32-2.9.7** Examine backup techniques utilized to ensure that: • Backups are securely stored in a separate location from the primary. • Ensure that segregation is maintained between users and administrators of the system.
32-3 The environment must have continuous (24/7) intrusion-detection systems in place, which protects the secure room by motion detectors when unoccupied.	**32-3.a** Examine security policies and procedures to verify they require: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment • Motion detectors must be active when the environment is unoccupied.
	32-3.b Examine intrusion-detection system configurations to verify: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place • Motion detectors are active when the environment is unoccupied.
32-3.1 Any windows in the secure room must be locked and protected by alarmed sensors.	**32-3.1.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	32-3.1.b Examine the configuration of window sensors to verify that the alarm mechanism is active.
	32-3.1.c Test at least one window (if they can be opened) to verify that the alarms function appropriately.
32-3.2 Any windows or glass walls must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**32-3.2** Observe all windows and glass walls in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.
32-3.3 The intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have performed an authenticated	**32-3.3.a** Examine security system configurations to verify: • The intrusion-detection system(s) is connected to the alarm system. • The intrusion-detection system(s) is automatically activated every time all authorized personnel have exited the secure room.

exit of the secure room. The system must be configured to activate within 30 seconds.	**32-3.3.b** Observe the IDS and alarms function correctly by: • Having all authorized personnel who badged or otherwise authenticated into the area exit and one person remain behind even though they have badged out • Having all but one authorized person who badged or otherwise authenticated into the system badge out and exit
32-3.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.	**32-3.4** Examine security-system configurations to verify that an alarm event is generated for: • Unauthorized entry attempts • Actions that disable the intrusion-detection system

32-4 All non-CA personnel must sign an access logbook when entering the Level 3 environment. ***Note:*** *This log is in addition to those provided by the access-control system.*	**32-4.a** Examine security policies and procedures to verify they require all non-CA personnel to sign an access logbook when entering the Level 3 environment.
	32-4.b On the escorted entry into the secure room, observe that all non-CA personnel appropriately sign the access logbook.
32-4.1 The access log must include the following details: • Name and signature of the individual • Organization • Date and time in and out • Reason for access or purpose of visit • For visitor access, the initials of the person escorting the visitor	**32-4.1** Examine the access logbook to verify it contains the following information: • Name and signature of the individual • Organization • Date and time in and out • Reason for access or purpose of visit • For visitor access, the initials of the person escorting the visitor
32-4.2 The logbook must be maintained within the Level 3 secure environment.	**32-4.2** Observe the location of the access logbook and verify that it is maintained within the Level 3 secure environment.
32-5 All access-control and monitoring systems (including intrusion-detection systems) are powered through an uninterruptible power source (UPS).	**32-5** Examine uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems, including intrusion-detection systems, are powered through the UPS.
32-6 All alarm events must be documented.	**32-6.a** Examine security policies and procedures to verify they require that all alarm events be logged.
	32-6.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
32-6.1 An individual must not sign off on an alarm event in which they were involved.	**32-6.1.a** Examine documented procedures for responding to alarm events to verify that the procedure does not permit a person who was involved in an alarm event to sign-off on that alarm event.
	32-6.1.b Observe who is authorized to sign off on alarm events.
	32-6.1.c For a sample of documented alarm events, examine the record to verify that personnel authorized to sign off on alarm events were not also the cause of that event.
32-6.2 The use of any emergency entry or exit mechanism must cause an alarm event.	**32-6.2.a** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
	32-6.2.b Test to verify the mechanisms work appropriately.

32-6.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.	**32-6.3.a** Examine documented procedures to verify they require that all alarms for physical intrusion must be responded to within 30 minutes by personnel assigned security duties.
	32-6.3.b Examine a sample of alarm events and interview personnel assigned with security-response duties to verify that alarms for physical intrusion are responded to within 30 minutes.
	32-6.3.c Test to verify the appropriate response occurs.
32-7 A process must be implemented for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs. It must be ensured that synchronization errors between CCTV, intrusion detection, and access control cannot exceed one minute. ***Note:*** *This may be done by either automated or manual mechanisms.*	**32-7.a** Examine documented procedures to verify that mechanisms are defined (may be automated or manual) for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs.
	32-7.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	32-7.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
32-7.1 If a manual synchronization process is used, synchronization must occur at least quarterly; events must be recorded and variances documented; and documentation of the synchronization must be retained for at least a one-year period.	**32-7.1.a** If a manual synchronization process is implemented, interview responsible personnel and examine records of synchronization to verify the mechanism is performed at least quarterly.
	32-7.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.
Functionality of a key-injection facility (or applicable entity providing key-management services) may be located at a single physical location or distributed over a number of separate physical locations. Distributed KIF functionality may include key generation, CA functionality, key distribution, and key injection. In order to mitigate the expanded attack surface of a distributed KIF, specific controls apply to a distributed architecture. If any secret or private keys or their components/shares appear in the clear outside of a SCD, ***Requirement 32-9*** *for a secure room must be met.*	
32-8 Distributed functionality of the KIF that is used for generation and transfer of keys must communicate via mutually authenticated channels. All key transfers between distributed KIF functions must meet the requirements of **Control Objective 3**.	

32-8.1 The KIF must ensure that keys are transmitted between KIF components in accordance with **Control Objective 3**.	**32-8.1.a** Examine documented procedures for key conveyance or transmittal to verify that keys used between KIF components are addressed in accordance with applicable criteria in **Control Objective 3**.
	32-8.1.b Interview responsible personnel and observe conveyance processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.
32-8.2 The KIF must implement mutually authenticated channels for communication between distributed KIF functions—e.g., between a host used to generate keys and a host used to distribute keys.	**32-8.2** Examine documented procedures to confirm they specify the establishment of a channel for mutual authentication of the sending and receiving devices.
32-8.3 The KIF must ensure that injection of enciphered secret or private keys into POI devices meets the requirements of **Control Objective 4**.	
32-8.4 The channel for mutual authentication is established using the requirements of **Control Objective 4**.	**32-8.4.a** Examine documented procedures for key loading to hosts and POI devices to verify that they are in accordance with applicable criteria in **Control Objective 4**.
	32-8.4.b Interview responsible personnel and observe key-loading processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.
32-8.5 The KIF must implement a mutually authenticated channel for the establishment of enciphered secret or private keys between POI devices and an HSM at the KIF.	**32-8.5** Examine documented procedures to confirm they specify the establishment of a mutually authenticated channel for establishment of enciphered secret or private keys between sending and receiving devices—e.g., POI devices and HSMs.

32-8.6 Mutual authentication of the sending and receiving devices must be performed. • KIFs must validate authentication credentials of a POI device prior to any key transport, exchange, or establishment with that device. • POI devices must validate authentication credentials of KDHs prior to any key transport, exchange, or establishment with that device. • When a KLD is used as an intermediate device to establish keys between POI devices and a KIF HSM it must not be possible to insert an unauthorized SCD into the flow without detection.	**32-8.6** Interview responsible personnel and observe processes for establishment of enciphered secret or private keys between sending and receiving devices to verify: • KIFs validate authentication credentials of a POI device prior to any key transport, exchange, or establishment with that device. • POI devices validate authentication credentials of KLDs prior to any key transport, exchange, or establishment with that device. • When a KLD is used as an intermediate device to establish keys between POI devices and a KIF HSM, it is not possible to insert an unauthorized SCD into the flow without detection
32-8.7 Mechanisms must exist to prevent a non-authorized host from injecting keys into POI devices or an unauthorized POI device from establishing a key with a legitimate KIF component.	**32-8.7** Examine documented procedures to confirm they define mechanisms to prevent an unauthorized host from performing key transport, key exchange, or key establishment with POI devices.
32-9 The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD. The secure room for key injection must include the following: • **Effective 1 January 2024** the injection of cleartext secret or private keying material must not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of POI v5 and higher devices. Subsequent to that date, only encrypted key injection will be allowed for POI v5 and higher devices. (**past**) • **Effective 1 January 2026**, the same restriction applies to entities engaged in key injection of devices for which they are the processors. ***Note:*** *This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the PCI PTS POI Security Requirements. It does apply to all other methods of loading of cleartext keying material for PTS POI v5 and higher devices.*	

32-9.1 The secure room must have walls made of solid materials. In addition, if the solid walls do not extend from the real floor to the real ceiling, the secure room must also have extended walls from the real floor to the real ceiling using sheetrock or wire mesh. ***Note:*** *In KIF environments where Level 1 and Level 2 physical barrier controls are in place and confirmed, the secure room may be implemented within a "caged" environment. A caged environment is an enclosed secure room that meets the criteria of Requirement 32 but is not made of solid walls. Refer to applicable requirements within this Domain for additional information on Level 1 and Level 2 physical barrier controls. All other criteria stated in 32-9 relating to cleartext secret and/or private keys and/or their components existing in unprotected memory outside the secure boundary of an SCD for loading keys apply.*	**32-9.1** Inspect the secure room designated for key injection to verify that it is constructed with extended walls from the real floor to the real ceiling using sheetrock or wire mesh.
32-9.2 Any windows into the secure room must be locked and protected by alarmed sensors.	**32-9.2.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	32-9.2.b Examine the configuration of window sensors to verify that the alarm mechanism is active.
32-9.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	**32-9.3** Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
32-9.4 A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.	**32-9.4** Inspect the secure room to verify that it is only accessed through a solid-core or a steel door, with door hinges that cannot be removed from outside the room.
32-9.5 An electronic access-control system (e.g., badge and/or biometrics) must be in place that enforces: • Dual-access requirements for entry into the secure room, and • Anti-pass-back requirements.	**32-9.5** Observe authorized personnel entering the secure room to verify that a badge-control system is in place that enforces the following requirements: • Dual-access for entry to the secure room • Anti-pass-back

32-9.6 The badge-control system must support generation of an alarm when one person remains alone in the secure room for more than 30 seconds. ***Note:*** *Examples of alarm-generation mechanisms include but are not limited to motion detectors, login/logout controls, biometrics, badge sensors, etc.*	**32-9.6** Examine alarm mechanisms and interview alarm-response personnel to verify that the badge-control system supports generation of an alarm when one person remains alone in the secure room for more than 30 seconds.
32-9.7 CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be motion-activated. The recording must continue for at least a minute after the last pixel of activity subsides.	**32-9.7** Inspect CCTV configuration and examine a sample of recordings to verify that CCTV monitoring is in place on a 24/7 basis, including the ability to record events during dark periods, and if motion activated verify that recording continues for at least a minute after the last pixel of activity subsides.
32-9.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	**32-9.8** Inspect configuration of monitoring systems and interview monitoring personnel to verify that monitoring is supported on a continuous (24/7) basis and alarms can be resolved by authorized personnel.
32-9.9 The CCTV server and digital storage must be secured in a separate secure location that is not accessible to personnel who have access to the key-injection secure room.	**32-9.9.a** Inspect location of the CCTV server and digital-storage to verify they are located in a secure location that is separate from the key-injection secure room.
	32-9.9.b Inspect access-control configurations for the CCTV server/storage secure location and the key-injection secure room to identify all personnel who have access to each area. Compare access lists to verify that personnel with access to the key-injection secure room do not have access to the CCTV server/storage secure location.
32-9.10 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.	**32-9.10** Inspect CCTV positioning and examine 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.
32-9.11 CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.	**32-9.11** Inspect CCTV positioning and examine a sample of recordings to verify that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials.

32-9.12 Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	**32-9.12.a** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.
	32-9.12.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.
Requirement 33: *Documented procedures must exist and be demonstrably in use to ensure the security and integrity of account-data processing equipment (e.g., POI devices and HSMs) placed into service, initialized, deployed, used, and decommissioned.*	
33-1 Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed on account-data processing devices before they are placed into service, as well as devices being decommissioned.	**33-1.a** Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for account-data processing devices placed into service, initialized, deployed, used, and decommissioned
	33-1.b Examine/observe that written records exist for the tests and inspections performed on devices before they are placed into service, as well as devices being decommissioned.

Requirement 5A: Account data is processed using algorithms and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
***5A-1** Account data is protected with appropriate cryptographic algorithms, key sizes and strengths, and key-management processes.*	
5A-1.1 Only approved encryption algorithms and key sizes must be used to protect account data and cryptographic keys, as listed in Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.	**5A-1.1.a** Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms and key sizes that are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.
	5A-1.1.b Observe key-management operations and devices to verify that all cryptographic algorithms and key sizes are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.
5A-1.2 Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (e.g., after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (e.g., *NIST Special Publication 800-57*). ***Note**: See Domain 5 Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.*	**5A-1.2.a** Examine documented key-management procedures to verify: • Crypto-periods are defined for every type of key in use. • Crypto-periods are based on industry best practices and guidelines (e.g., *NIST Special Publication 800-57*). • A process/methodology is in place to determine when the crypto-period is reached for each cryptographic key. • Cryptographic key changes are implemented whenever a key reaches the end of its defined crypto-period.
	5A-1.2.b [Removed]
5A-1.3 Documentation describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution must exist and must be demonstrably in use for all key-management processes.	**5A-1.3.a** Examine documentation to verify it describes the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution.
	5A-1.3.b Observe architecture and key-management operations to verify that the documentation reviewed in **5A-1.3.a** is demonstrably in use for all key-management processes.

Requirement 5A: Account data is processed using algorithms and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
5A-1.3.1 Maintain documentation of all cryptographic keys managed as part of the P2PE solution, including: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method	**5A-1.3.1.a** Examine key-management policies and procedures and verify documentation of all cryptographic keys managed as part of the P2PE solution is required, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method
	5A-1.3.1.b Observe documentation and interview personnel and confirm that documentation of all cryptographic keys managed as part of the P2PE solution exists, and includes: • Key type/description • Description of level in the key hierarchy • Purpose/function of the key (including type of devices using key) • Key-creation method • Key-distribution method (e.g., manually via courier, remote key distribution) • Type of media used for key storage • Key-destruction method

Requirement 5A: Account data is processed using algorithms and methodologies that ensure they are kept secure	
Domain 5 Requirements	**Testing Procedures**
5A-1.3.2 Maintain a list of all devices used to generate keys or key components managed as part of the P2PE solution, including: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **5A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per *NIST SP800-22*)	**5A-1.3.2.a** Examine key-management policies and procedures and verify a list of all devices used to generate keys managed as part of the P2PE solution is required, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **5A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per *NIST SP800-22*)
	5A-1.3.2.b Observe documentation and interview personnel and confirm that a list of all devices used to generate keys managed as part of the P2PE solution exists, and includes: • Device name/identifier • Device manufacturer/model • Type of keys generated (per **5A-1.3.1**) • Device location • Approved key-generation function (PTS, FIPS, or other approved per *NIST SP800-22*)

Requirement 5H: For hybrid decryption solutions: Implement secure hybrid key management	
Domain 5 Requirements	**Testing Procedures**
***5H-1** Hybrid decryption solutions securely manage the Data Decryption Keys (DDKs) that decrypt account data in software on a Host System.*	
***Note:** DDKs used to decrypt account data in a Host System are the ONLY keys that can ever be managed in software per these 5H Requirements; all other cryptographic keys used in hybrid decryption solutions are managed in HSMs and are never present or managed in software.*	
5H-1.1 The Data Decryption Keys (DDKs) used in software to decrypt account data must have defined usage limits. This can be achieved through the use of either one of the following approaches: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in *NIST SP800-57, ISO TR 14742,* and *NIST SP800-131*. The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the Host System. ***OR*** • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.	**5H-1.1.a** Examine documented key-management policies and procedures to verify that DDKs managed on the Host System meet one or both of the following: • Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in *NIST SP800-57, ISO TR 14742,* and *NIST SP800-131*. The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first). Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the host processing system. ***OR*** • DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.
	5H-1.1.b Observe the key-management methods used to manage DDKs on the Host System to verify they meet one, or both of the above options.
5H-1.2 DDKs must be erased from the Host System volatile memory via a mechanism that ensures the key cannot be recovered or reconstructed.	**5H-1.2.a** Examine documented key-management policies and procedures to verify that the mechanism used to erase a DDK from the Host System volatile memory is sufficient to ensure the key cannot be recovered or reconstructed.
	5H-1.2.b Test, through the use of forensic tools and/or methods, that the mechanism used to erase the DDK from the host volatile memory, is sufficient to ensure the key cannot be recovered or reconstructed.

Requirement 5H: For hybrid decryption solutions: Implement secure hybrid key management	
Domain 5 Requirements	**Testing Procedures**
5H-1.3 If the DDK is generated from a master key, the following conditions apply: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generate the DDK must be dedicated to generating DDKs.	**5H-1.3.a** Examine key-management policies and procedures to verify that the following is required for any DDKs generated from a master key: • A one-way derivation process must be used. • The DDK must never be generated as a variant of the HSM master file key. • The master key used to generate the DDK must be dedicated to generating DDKs.
	5H-1.3.b Observe key-generation processes for generating DDKs from a master key to verify: • A one-way derivation process is used. • The DDK is never generated as a variant of the HSM master file key. • The master key used to generate the DDK is dedicated to generating DDKs.
5H-1.4 The DDK must be encrypted between the HSM and the Host System, e.g., using a fixed transport key or a cryptographic protocol. The method of encryption used must maintain the security policy to which the HSM was approved (either *FIPS 140-2* or *140-3*, Level 3 or higher, or approved to the PCI HSM standard).	**5H-1.4.a** Examine key-management policies and procedures to verify that DDKs must be encrypted between the HSM and the Host System.
	5H-1.4.b Examine HSM and Host System configurations to verify that DDKs are encrypted between the HSM and the Host System.
	5H-1.4.c Examine the HSM security policies and observe HSM implementations to verify that the method of encryption used maintains the security policy to which the HSM was approved.
5H-1.5 The encryption mechanism used to protect the DDK between the HSM and the Host System:	**5H-1.5** Examine/observe the encryption mechanism used to protect the DDK between the HSM and the Host System, includes **5H-1.5.1** through **5H-1.5.4.** Perform the following:
5H-1.5.1 The encryption key must be equal or greater in strength than the key it protects.	**5H-1.5.1.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is equal or greater in strength than the key it protects.
	5H-1.5.1.b Observe key-management processes to verify the encryption mechanism used to protect the DDK between the HSM and the Host System uses an encryption key that is equal or greater in strength than the key it protects.

Requirement 5H: For hybrid decryption solutions: Implement secure hybrid key management	
Domain 5 Requirements	**Testing Procedures**
5H-1.5.2 The encryption key must be unique for each Host System.	**5H-1.5.2.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is unique for each Host System.
	5H-1.5.2.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is unique for each Host System.
5H-1.5.3 The encryption key must only be used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.	**5H-1.5.3.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.
	5H-1.5.3.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that is only used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.
5H-1.5.4 The encryption key must have a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.	**5H-1.5.4.a** Examine documented key-management policies and procedures to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.
	5H-1.5.4.b Observe key-management processes to verify that the encryption mechanism uses an encryption key that has a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.

Requirement 5l: Component providers ONLY: report status to solution providers	
Domain 5 Requirements	**Testing Procedures**
Note: *This section is ONLY applicable for P2PE component providers undergoing an assessment of this domain for subsequent PCI listing of the component provider's services. This section is not applicable to, and does not need to be completed by, P2PE solution providers (or merchants as solution providers).*	
5l-1 For component providers performing key management, maintain and monitor critical P2PE controls and provide reporting to the responsible solution provider.	
5l-1.1 Track status of the deployed key-management services for PTS POI devices and HSMs, and provide reports to solution provider annually and upon significant changes, including at least the following: • Types/models of PTS POIs and/or HSMs for which keys have been injected • For each type/model of PTS POI devices and/or HSM: – Number of devices – Type of key(s) injected – Key-distribution method • Details of any known or suspected compromised keys, per **22-1** ***Note:*** *Adding, changing, or removing PTS POI devices and/or HSM types, or critical key-management methods may require a Delta Change. Please refer to the PCI P2PE Program Guide for details about obligations when adding, changing, or removing elements of a Listed P2PE Product.*	**5l-1.1.a** Examine the component provider's documented procedures for providing required reporting to applicable solution providers, and interview responsible component-provider personnel to confirm that the following processes are documented and implemented: • Types/models of POIs and/or HSMs for which keys have been injected • For each type/model of POI and/or HSM: – Number of devices – Type of key injected – Key-distribution method • Details of any known or suspected compromised keys, per **22-1**
	5l-1.1.b Observe reports provided to applicable solution providers annually and upon significant changes to the solution, and confirm they include at least the following: • Types/models of POIs for which keys have been injected • For each type/model of POI: – Number of POI devices – Type of key injected – Key-distribution method • Details of any known or suspected compromised keys, per **22-1**

Domain 5 Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms

Approved Algorithms in connection with the requirements in this document are based on the approved algorithms listed in NIST SP 800-57 Part 1 Rev. 4, Section 4;

- Hash functions: only algorithms from the SHA2 and SHA3 family are allowed on POI v3 and higher devices, with output size >255[2]
- Symmetric-Key Algorithms used for encryption and decryption: AES must be used, with key size >= 128 bits or TDEA with key size >= 168 bits
- Message Authentication Codes (MACs): CMAC or GMAC can be used with AES, as well as HMAC with an approved hash function and a key size >=128
- Signature algorithms: DSA, RSA (with PKCS1-v1.5 or PSS) and ECDSA with key sizes specified below.
- Approved key establishment schemes are described in NIST SP800-56A (ECC/FCC[3]-based key agreement), NIST SP800-56B (IFC-based key agreement) and NIST SP800-38F (AES-based key encryption/wrapping).

[2] Except as noted, the use of SHA-1 is prohibited for all digital signatures used on the device that are used in connection with meeting PCI security requirements. This includes certificates used by the device that are non-device-specific that are part of a vendor PKI, up to and including a vendor root certificate. The only exception to this is that the initial code on ROM that initiates upon the device start may authenticate itself using SHA-1, but all subsequent code must be authenticated using SHA-2.

SHA-2 or higher is recommended for other usages, but SHA-1 may be used in conjunction with the generation of HMAC values and surrogate PANs (with salt), for deriving keys using key derivation functions (i.e., KDFs) and random number generation. Where applicable, appropriate key length minimums as delineated in the Derived Test Requirements are also required.

[3] IFC: Integer Factorization Cryptography; ECC: Elliptic Curve Cryptography; FFC: Finite Field Cryptography

The following are the **minimum key sizes**[4] and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange, or establishment, and for key or data protection:

Algorithm	TDEA	(IFC) RSA	ECC (ECDSA, ECDH, ECMQV)	FFC (DSA, DH, MQV)	AES
Minimum key size in number of bits [5]	168	2048	224	2048/224	128

TDEA refers to TDEA (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. Key-encipherment keys shall be at least of equal or greater strength than any key that they are protecting.[6] This applies to any key-encipherment keys used for the protection of secret or private keys that are stored or for keys used to encrypt any secret or private keys for loading or transport. For purposes of this requirement, the following algorithms and keys sizes by row are considered equivalent.

[4] Additional key sizes and algorithms may be supported for non-PCI payment brand relevant transactions.

[5] PTS POI version 3.x devices and above are **ONLY** permitted to use 2-key TDEA for account-data encryption with an industry recognized unique-key-per-transaction algorithm as defined in *ISO 11568* for key derivation or transformation (i.e., UKPT, DUKPT), including the use of a double-length BDK for key generation of data encryption/decryption keys.

[6] Notwithstanding the statement, 2048 RSA keys may be used to transport 128 AES keys when performing remote key distribution using asymmetric techniques.

Bits of Security *(not to be confused with minimum key size)*	Symmetric encryption algorithms	IFC (RSA)	ECC (ECDSA, ECDH, ECMQV)	FFC (DSA, DH, MQV)
112	Triple-length TDEA	2048	224	2048/224
128	AES-128	3072	256	3072/256
192	AES-192	7680	384	7680/384
256	AES-256	15360	512	15360/512

For implementations using FFC or ECC:

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

IFC, FFC and ECC are vulnerable to attacks from large-scale quantum computers. In 2017, NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms, planned to end with a selection of new algorithms by 2023-2025.

Because of rapid progress in the field of quantum computing, it is advised to become informed/aware of this specific threat and its potential mitigations.

Appendix A: Merchant-Managed Solutions: Separation between Merchant Encryption and Decryption Environments

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

Target Audience: *This appendix, in addition to applicable Domains, applies only to merchants that manage their own P2PE solutions.*

Overview

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

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

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

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

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

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

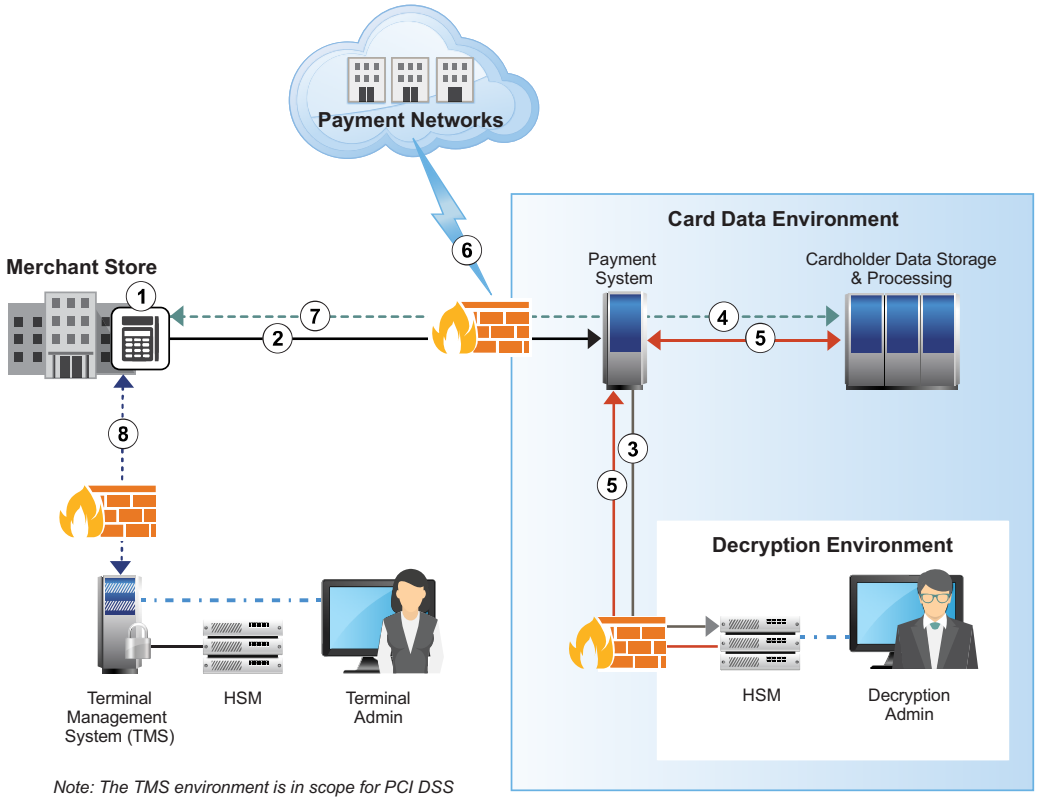
Eligibility Criteria

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

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

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

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



Example P2PE Transaction Steps

1 Transaction initiation
2 Transaction request with encrypted data
3 P2PE-encrypted transactions
4 Non-PCI branded transactions
5 Decrypted transaction data
6 Transactions sent to payment networks
7 Transaction response
8 Terminal Management System traffic

Legend

- P2PE Encrypted Data
- Clear Text Data
- Non-account Data
- Terminal Management Data (encrypted)
- HSM Console Management (encrypted)

Notes

Note: This diagram is for illustrative purposes only. Other implementations are acceptable as long as they meet the requirements specified in this appendix.

Note: This diagram focuses on traffic flows related to P2PE transaction processing and may not may not show all relevant payment transaction traffic.

Requirement MM-A: Restrict access between the merchant decryption environment and all other networks/systems	
Domain 4 Requirements	**Testing Procedures**
***MM-A-1** The merchant decryption environment must be dedicated to decryption operations.*	
MM-A-1.1 Current documentation must be maintained that describes, or illustrates, the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.	**MM-A-1.1.a** Interview responsible personnel and examine documentation to verify that procedures exist for maintaining documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs.
	MM-A-1.1.b Interview responsible personnel and examine merchant documentation that describes/illustrates the architecture of the merchant-managed P2PE solution, including the flow of data and cryptographic key exchanges, and interconnectivity between all systems within the encryption environment, the merchant decryption environment, and any other CDEs to verify that the document is kept current.
MM-A-1.2 Decryption systems must reside on a network that is dedicated to decryption operations. ***Note:** The decryption environment must exist within a cardholder data environment (CDE).*	**MM-A-1.2.a** Examine network diagrams to verify that decryption systems are located on a network that is dedicated to decryption operations.
	MM-A-1.2.b Examine network and system configurations to verify that decryption systems are located on a network that is dedicated to decryption operations.

Requirement MM-A: Restrict access between the merchant decryption environment and all other networks/systems	
Domain 4 Requirements	**Testing Procedures**
MM-A-1.3 Systems in the decryption environment must be dedicated to performing and/or supporting decryption and key-management operations: • Services, protocols, daemons, etc. necessary for performing and/or supporting decryption operations must be documented and justified. • Functions not required for performing or supporting decryption operations must be disabled or isolated (e.g., using logical partitions) from decryption operations. ***Note:*** *Security functions (e.g., logging and monitoring controls) are examples of functions supporting decryption operations. It is not required that supporting functions be present in the merchant decryption environment; these functions may be resident in the CDE. However, any supporting functions that are present in the decryption environment must be wholly dedicated to the decryption environment.*	**MM-A-1.3.a** Examine network and system configuration settings to verify that only necessary services, protocols, daemons, etc. are enabled, and any functions not required for performing or supporting decryption operations are disabled or isolated from decryption operations.
	MM-A-1.3.b Examine the documented record of services, protocols, daemons, etc. that are required by the decryption systems and verify that each service includes justification.
MM-A-1.4 Systems providing logical authentication services to system components within the decryption environment must: • Reside within the decryption environment • Be dedicated to supporting the decryption environment. ***Note:*** *Logical authentication services may be internal to the HSM management system.*	**MM-A-1.4.a** Examine documented policies and procedures, and interview responsible personnel to verify that systems providing logical authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.
	MM-A-1.4.b Examine system configurations and observe processes to verify that systems providing authentication services to system components within the decryption environment reside within the decryption environment and are dedicated to supporting the decryption environment.

Requirement MM-A: Restrict access between the merchant decryption environment and all other networks/systems	
Domain 4 Requirements	**Testing Procedures**
MM-A-1.5 Logical administrative/privileged access to systems within the decryption environment must be authorized and must originate from within the merchant decryption environment.	**MM-A-1.5.a** Examine documented policies and procedures, and interview responsible personnel to verify that logical administrative/privileged access to the systems within the decryption environment must be authorized and originate from within the merchant decryption environment.
	MM-A-1.5.b Examine firewall/router configurations to verify that logical administrative/privileged access to systems within the decryption environment is authorized and originates from within the merchant decryption environment.
MM-A-1.6 All remote access features on all systems in the merchant decryption environment must be permanently disabled and/or otherwise prevented from being used	**MM-A-1.6** Examine system configurations and observe processes to verify that all remote access features on all systems within the merchant decryption environment are permanently disabled and/or otherwise prevented from being used.
MM-A-1.7 Systems in the merchant decryption environment must not store account data.	**MM-A-1.7.a** Examine configurations of all devices and systems in the merchant decryption environment to confirm none of the systems store account data.
	MM-A-1.7.b Examine data flows and interview personnel to verify that account data is not stored in the merchant decryption environment.
MM-*A-2* *Restrict access between the merchant decryption environment and all other networks/systems.*	
MM-A-2.1 Firewalls must be in place to restrict connections between the merchant decryption environment and all other networks. Firewalls must be configured to restrict traffic as follows:	**MM-A-2.1** Examine documentation and observe network configurations to verify that firewalls are in place between the merchant decryption environment and all other networks.
MM-A-2.1.1 Inbound and outbound traffic to/from the decryption environment must be restricted to only IP addresses within the CDE.	**MM-A-2.1.1** Examine firewall and router configurations to verify that inbound and outbound traffic to/from the decryption environment is limited to only IP addresses within the CDE.
MM-A-2.1.2 Inbound and outbound traffic between the decryption environment and any CDE must be restricted to only that which is necessary for performing and/or supporting decryption operations, with all other traffic specifically denied (e.g., by using an explicit “deny all” or an implicit deny after an allow statement).	**MM-A-2.1.2.a** Examine firewall configuration standards to verify that inbound and outbound traffic necessary for performing and/or supporting decryption operations is identified and documented.
	MM-A-2.1.2.b Examine firewall configurations to verify that inbound and outbound traffic between the decryption environment and any CDE is limited to only that which is necessary for performing and/or supporting decryption operations, and all other traffic is specifically denied (e.g., by using an explicit “deny all” or an implicit deny after an allow statement).

Requirement MM-A: Restrict access between the merchant decryption environment and all other networks/systems	
Domain 4 Requirements	**Testing Procedures**
MM-A-2.2 Inbound and outbound traffic between the merchant CDE and the encryption environment must be restricted to approved POI devices located within the encryption environment.	**MM-A-2.2** Examine network and system configurations to verify that inbound and outbound traffic between the merchant CDE and the encryption environment is restricted to approved POI devices located within the encryption environment.
MM-A-2.3 Processes must be implemented to prevent unauthorized physical connections (e.g., wireless access) to the decryption environment as follows: • Wireless connections to the decryption environment are prohibited. • Processes are implemented to detect and immediately (as soon as possible) respond to physical connections (e.g., wireless connections) to the decryption environment.	**MM-A-2.3.a** Examine document policies and procedures to verify that wireless connections to the decryption environment are prohibited.
	MM-A-2.3.b Observe processes and interview personnel to verify a methodology is implemented to immediately (e.g., ASAP) detect, identify, and eliminate any unauthorized physical connections (e.g., wireless access points) that connect to the decryption environment.
	MM-A-2.3.c Examine firewall/router configurations to confirm that all wireless networks are prevented from connecting to the decryption environment.

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

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