Payment Card Industry (PCI)

Point-to-Point Encryption

Solution Requirements:

Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware)

Initial Release: Version 1.0

September 2011

Document Changes

Date	Version	Description	Pages
14 September, 2011	1.0	Initial release of *PCI Point-to-Point Encryption: Solution Requirements – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware).*	

Table of Contents

Preface

Point-to-point encryption technology may assist merchants to reduce the scope of their cardholder data environment and annual PCI DSS assessments. As implementation of these technologies grows, the Council believes it is imperative to build, test and deploy solutions that provide strong support for PCI DSS compliance. With this aim the Council is launching the first set of validation requirements for point-to-point encryption solutions. The Council reminds stakeholders that forthcoming requirements for validating point-to-point encryption solutions do not supersede the PCI Data Security Standard or other PCI Standards. The Council will provide security requirements, testing procedures, assessor training and resources to support the deployment of secure point-to-point solutions. However the launch of these requirements does not constitute a recommendation from the Council nor does it 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.

This document contains the first set of validation requirements for point-to-point encryption solutions, and provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this document contains validation requirements for hardware-based encryption and decryption solutions, also called “hardware/hardware” requirements. Hardware solutions utilize secure cryptographic devices for both encryption and decryption including at the point of merchant acceptance for encryption, and within Hardware Security Modules (HSMs) for decryption. The Council will follow this initial release with related testing procedures before the end of 2011, and with requirements for solutions that utilize software decryption within hardware. This second category of solutions combine hardware based encryption and decryption through a secure cryptographic device, with software that may manage transaction-level cryptographic keys for decryption.

As part of the first phase of the launch, this document details the security requirements. Training to familiarize assessors with the program requirements and testing procedures is targeted for early 2012, with hardware-based solution listings following in the spring 2012.

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

This document requires the use of secure cryptographic devices, or SCDs, for the encryption and decryption of payment card data, as well as for the storage and management of cryptographic keys. The term ”secure cryptographic device” is defined in various standards, such as ISO13491 and ANSI X9.97. For the purposes of this P2PE standard, however, an SCD used for the acceptance and encryption of account data at the point of sale is required to be a PCI-approved POI device. A PCI-approved POI device is a device evaluated and approved via the PCI PTS program, with SRED (secure reading and exchange of data) listed as a “function provided,” and with the SRED capabilities enabled and active. *Note that within this document the terms “POI” and “PCI-Approved POI Device” are used interchangeably.* SCDs which are used for cryptographic key management functions and/or the decryption of account data are host/hardware security modules (HSMs), and must be either approved and configured to FIPS140-2 (level 3 or higher), or approved to the PCI HSM standard.

Definition of Account Data

"Account data," as referred to herein, consists of cardholder data plus sensitive authentication data, as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
Primary Account Number (PAN)	Full magnetic stripe data or equivalent on a chip
Cardholder Name	
Expiration Date	CAV2/CVC2/CVV2/CID
Service Code	PINs/PIN blocks

The following table, excerpted from the Payment Card Industry Data Security Standard (PCI DSS), illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited by PCI DSS, and whether each data element must be protected[1]. This table is not exhaustive, but is presented to illustrate the different types of PCI DSS requirements that apply to each data element.

		Data Element	Storage Permitted for PCI DSS [1]	Render Stored Account Data Unreadable per PCI DSS Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	Cannot store per Requirement PCI DSS 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement PCI DSS 3.2
		PIN/PIN Block	No	Cannot store per Requirement PCI DSS 3.2

[1] For merchants using a P2PE solution for PCI DSS scope reduction, storage of Primary Account Number is acceptable during the business process of finalizing the payment transaction if needed (for example, offline transactions). However, at all times, Sensitive Authentication Data is not stored after the completion of the authorization process.

[2] Senstive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Introduction: Solution Requirements for Point-to-Point Encryption

Purpose of this Document

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

Solutions with Encryption, Decryption, and Key Management within Secure Cryptographic Devices

Requirements for a P2PE solution will vary depending on the deployment environment and the technologies used for a specific implementation. This document presents requirements covering each domain for environments using SCDs for encryption, decryption, and cryptographic key management. This scenario addresses merchants who do not store or decrypt encrypted data within their P2PE environment, and who use validated solutions consisting of hardware-based encryption and third-party hardware-based decryption. Merchant characteristics include:

- Never store, process, or transmit any clear-text account data outside of an SCD within their P2PE environment. Account data must be entered directly into this SCD and encrypted with strong cryptography before being transmitted outside of the protected boundary of the device. To be eligible for PCI DSS scope reduction via use of a validated P2PE solution, merchants must ensure that any other payment channels within the merchant environment are adequately segmented (isolated) from the P2PE environment.
- Use a P2PE validated encryption/decryption solution provided or specified by acquirer, processor, or payment gateway (or "solution provider") that encompasses all of the following:
    - Validated encryption device at the point of interaction (POI) – Domain 1 of this document.
    - Validated application(s), for any applications on the POI that were not assessed as part of the PCI-approved POI device evaluation – Domain 2 of this document.
    - Solution-provider management of encryption devices and any applications, and merchant guidance from solution provider via the P2PE Instruction Manual – Domain 3 of this document.
    - Encrypted transmissions sent to the decryption environment for processing, such that account data is not decrypted until it reaches the secure cryptographic device of the solution provider – Domain 4 of this document.
    - Solution-provider management of decryption environment and all decrypted account data – Domain 5 of this document.
    - Solution-provider management of all cryptographic key operations, including the key-management requirements contained in - Domain 6 of this document.
- Use a third-party solution and services from a solution provider that has been validated compliant with P2PE solution requirements (including PCI DSS and PCI PIN Transaction Security (PTS) requirements).

- Receive reduced PCI DSS scope for environment using validated P2PE solution, as nearly all cardholder data environment (CDE) related operations are managed by the validated solution provider. For example, merchant validation may include physical environment controls (no altered POS terminals, etc.), third-party agreements, policies and procedures, etc.

P2PE Roles and Responsibilities

There are several stakeholders in the P2PE community. Some of these—payment device vendors, application vendors, QSAs, solution providers, and PCI SSC—have a more direct participation in the assessment process. The following sections define the roles and responsibilities of these P2PE stakeholders. Stakeholders that are involved in the assessment process have those related responsibilities listed.

Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards, including the PCI DSS, PA-DSS, PTS, and P2PE. In relation to P2PE, PCI SSC:

- Performs quality assurance (QA) reviews of P2PE reports to confirm report consistency and quality
- Lists P2PE validated solutions on the Website. *Note that this list will not be available on the Website until spring 2012.*
- Qualifies and trains P2PE QSAs to perform P2PE reviews. *Note that the P2PE QSA and P2PE PA-QSA qualification and training programs will be available in late 2011 and early 2012.*
- Maintains and updates the P2PE standard and related documentation according to a standards lifecycle management process.

Note that PCI SSC does not approve reports from a validation perspective. The role of the P2PE QSA is to document the solution provider's P2PE compliance as of the date of the assessment. Additionally, PCI SSC performs QA to assure that the P2PE QSAs accurately and thoroughly document results of P2PE assessments.

Payment Card Brands

American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the founding payment brands of the PCI SSC. These payment brands are responsible for developing and enforcing any compliance programs, including but not limited to any requirements, mandates, or due dates, and any fines or penalties.

P2PE Solution Provider

The P2PE solution provider is a third-party entity (for example, a processor, acquirer, or payment gateway). The solution provider designs and implements, and may also manage a P2PE solution for merchants. The solution provider may manage and perform all solution provider responsibilities or may outsource certain responsibilities. The solution provider has the overall responsibility for the design of an effective P2PE solution appropriate for a specific P2PE implementation. The solution provider is ultimately responsible for ensuring:

- Validation of encryption and decryption devices
- Secure device management

- Secure encryption and decryption operations and management of cryptographic keys
- Secure application management
- Maintenance of a PCI DSS compliant decryption environment
- Appropriate monitoring of controls
- Compliance of third-party organizations, such as Certification Authorities and key-injection facilities, to the requirements set in this standard
- Development, maintenance, and distribution of a P2PE Instruction Manual that covers all applicable requirements to all merchants deploying the solution

  Validated P2PE solution providers are required to provide a P2PE Instruction Manual to instruct merchants and, where applicable, resellers/integrators, on the secure implementation and management of the P2PE solution. The P2PE Instruction Manual must also document secure configuration specifics mentioned throughout this document and clearly delineate vendor, reseller/integrator, and customer responsibilities for maintaining the solution. When implemented and maintained according to the P2PE Instruction Manual, the P2PE solution should facilitate and support merchants' PCI DSS compliance.

Any security-related function that a solution provider implements or outsources in support of the P2PE solution must be assessed as part of the P2PE solution validation.

P2PE solution providers have their solutions assessed by a P2PE QSA, who has been specifically trained to perform P2PE solution assessments.

P2PE QSAs

P2PE QSAs are those companies and individuals that have been accredited by PCI SSC to evaluate Point-to-point Encryption solutions. *Note that not all QSAs are P2PE QSAs—there are additional qualification requirements that must be met for a QSA to become a P2PE QSA.*

P2PE QSAs are responsible for:

- Performing assessments on P2PE solutions in accordance with the P2PE solution requirements
- Providing an opinion regarding whether the P2PE solution and environment meets P2PE requirements
- Confirming that the P2PE Instruction Manual specific to a P2PE solution effectively documents secure configuration settings, merchant guidance, etc. for implementers, resellers/integrators, merchants, etc.
- Providing adequate documentation within the report to demonstrate the solution and environment's compliance to P2PE requirements
- Submitting the report to PCI SSC, along with the *Attestation of Validation* (signed by both P2PE QSA and solution provider)
- Maintaining an internal quality assurance process for their P2PE QSA efforts

It is the P2PE QSA's responsibility to state whether the P2PE solution has achieved compliance. PCI SSC does not approve reports from a technical compliance perspective, but performs QA reviews on the reports to assure that the reports adequately document the demonstration of compliance.

P2PE PA-QSAs

P2PEPA-QSAs are those companies and individuals that have been accredited by PCI SSC to evaluate applications on PCI-approved POI devices for Point-to-point Encryption solutions. *Note that not all PA-QSAs are P2PE PA-QSAs—there are additional qualification requirements that must be met for a PA-QSA to become a P2PE PA-QSA.*

PCI PTS Laboratories

PCI PTS security laboratories are responsible for the evaluation of POI devices against the PCI PTS requirements. Evaluation reports on devices found compliant to the requirements are submitted by the PCI PTS laboratories to PCI SSC for approval and listing. Note that this device evaluation per PCI PTS requirements is separate from the P2PE solution validation; the P2PE validation will confirm the device is listed on PCI SSC's PTS listing.

Payment Device (Hardware) Vendors

A POI vendor submits a POI device for evaluation to an independent PCI PTS security laboratory. Vendors must develop a supplement document describing the secure operation and administration of their equipment to assist merchants and solution providers.

Application (Software) Vendors

An application vendor that develops applications used on the POI device, where those applications were not reviewed as part of the PCI-approved POI device evaluation, must have that application assessed for secure operation within the POI device, and must provide guidance that describes secure installation and administration of the application on the POI device.

Resellers and Integrators

Resellers and integrators are those entities that may sell, install, and/or service P2PE solutions on behalf of device vendors, solution providers or others. Resellers and integrators performing services relating to P2PE validated solutions are responsible for:

- Implementing validated P2PE solutions in compliance with all applicable requirements in this document
- Configuring P2PE solutions (where configuration options are provided) according to the validated processes provided by the P2PE solution provider, as documented in the P2PE Instruction Manual
- Servicing P2PE devices (for example, troubleshooting, delivering remote updates, and providing remote support) according to the validated processes provided by the P2PE solution provider.

Resellers and integrators do not submit P2PE solutions for assessment—this is done by the solution provider.

Certification Authorities

A Certification Authority (CA) is a trusted third party that is responsible for managing security credentials and public keys for message encryption and for the issuance of digital certificates. For purposes of these requirements, a certificate is any digitally signed value containing a public key.

Enhanced key-management requirements are set in Annex A of this document and are exclusively applicable to CAs. Certification Authority requirements apply to all entities signing public keys, whether in X.509 certificate-based schemes or other designs. These requirements apply equally to third-party CAs or a CA that is hosted by the solution provider.

Ultimately, it remains the solution provider's responsibility to ensure that the CA is in compliance with the requirements set out in Annex A.

Key-Injection Facilities

The term key-injection facility (KIF) describes those entities that perform key injection of POI devices. Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer or vendor. Environmental and key-management requirements are defined in Domains 5 and 6 of this document; however, Annex B contains additional requirements for KIFs.

Ultimately, it remains the solution provider's responsibility to ensure that the KIF is in compliance with the requirements set out in this document.

Merchants

Merchants are those who use a payment device (point-of-sale (POS) device or terminal) that is part of a P2PE solution, with the objective of receiving reduced scope for their PCI DSS assessment. Merchants who use a P2PE solution to receive reduced PCI DSS scope are responsible for:

- Coordinating with the acquirer (merchant bank) to determine which payment device (as part of a validated P2PE solution) the merchant should implement
- Reviewing the P2PE Instruction Manual provided by the solution provider, and implementing the device and in-store processes in accordance with the P2PE Instruction Manual
- Coordinating with the acquirer and validating applicable PCI DSS requirements (if required to do so by the acquirer) in accordance with payment brand validation requirements (for example, an applicable Self-Assessment Questionnaire or the PCI DSS Security Assessment Procedures)

Once the list of P2PE validated solutions is posted by PCI SSC, merchants can find a listing of validated P2PE solutions including associated payment devices, along with other reference materials, on the PCI SSC Website.

In a hardware/hardware scenario, the PTS-approved POI device is part of the P2PE solution and provides the required level of segmentation between the merchant's CDE (contained within the device) and the rest of the merchant environment, such that the merchant is not obliged to segment their environment further.

Table 1: At-a-Glance – Domains and Requirements for P2PE Validation – Solutions with SCD Encryption/Decryption and Key Management

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

The following table provides an overview of each domain, including a description of the scope for the current scenario and the high-level requirements for each domain. Additionally, the table identifies the responsible parties for validation of each domain and for ultimately ensuring protection of account data in a P2PE solution. Each requirement identified here has corresponding sub-requirements and validation procedures, which are presented in detail beginning on page 15.

	Scenario 1: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 1: Encryption Device Build secure devices and protect devices from tampering during manufacture and delivery.	▪ POI device managed by solution provider. ▪ Hardware encryption performed by device. ▪ POI is PTS SRED validated.	1A Build PCI-approved POI devices. 1B Securely manage equipment used to protect account data, up to point of deployment.	▪ POI Device Manufacturer ▪ P2PE Solution Provider
Domain 2: Application Security Secure applications in P2PE environment.	▪ Application within secure controller of PCI-approved POI device. ▪ All applications with access to account data have been assessed and are listed as approved P2PE applications.	2A Protect PAN and SAD. 2B Develop and maintain secure applications. 2C Implement secure application-management processes.	▪ Application Vendor ▪ P2PE Solution Provider

	Scenario 1: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 3: Encryption Environment Secure environments where POI devices are present.	▪ No storage of CHD after payment transaction is finalized. ▪ Within the segmented P2PE environment, no CHD processed through channels or methods external from an approved SCD. ▪ All device and key-management functions are performed by solution provider. ▪ POI devices are implemented and maintained in accordance with the P2PE Instruction Manual.	3A Secure POI devices throughout the device lifecycle. 3B Implement secure device-management processes.	▪ P2PE Solution Provider
Domain 4: Transmissions between Encryption and Decryption Environments Secure operations between encryption and decryption environments.	▪ All operations managed by solution provider. ▪ Merchant has no access to the encryption environment (within POI device) or decryption environment. ▪ Merchant has no involvement in encryption or decryption operations. ***Note that this domain in not applicable for this hardware/hardware scenario.***	4A Control traffic between encryption and decryption environments. 4B Prevent exposure of decryption keys.	▪ P2PE Solution Provider
Domain 5: Decryption Environment Secure environments where decryption devices are present.	▪ Decryption environment implemented at and managed by solution provider ▪ Merchant has no access to the decryption environment. ▪ Decryption environment must be PCI DSS compliant	5A Secure all decryption systems and devices. 5B Implement secure device-management processes. 5C Implement monitoring and response procedures.	▪ P2PE Solution Provider

	Scenario 1: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 6: Cryptographic Key Operations Use strong cryptographic keys and secure key-management functions.	▪ All key-management functions implemented and managed by solution provider ▪ Merchant has no involvement in key-management operations.	6A Use secure encryption methodologies. 6B Use secure key-generation methodologies. 6C Distribute cryptographic keys in a secure manner. 6D Load cryptographic keys in a secure manner. 6E Ensure secure usage of cryptographic keys. 6F Ensure secure administration of cryptographic keys.	▪ P2PE Solution Provider

Figure 1: At-a-Glance - Steps Required to Create and Validate a P2PE Solution

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

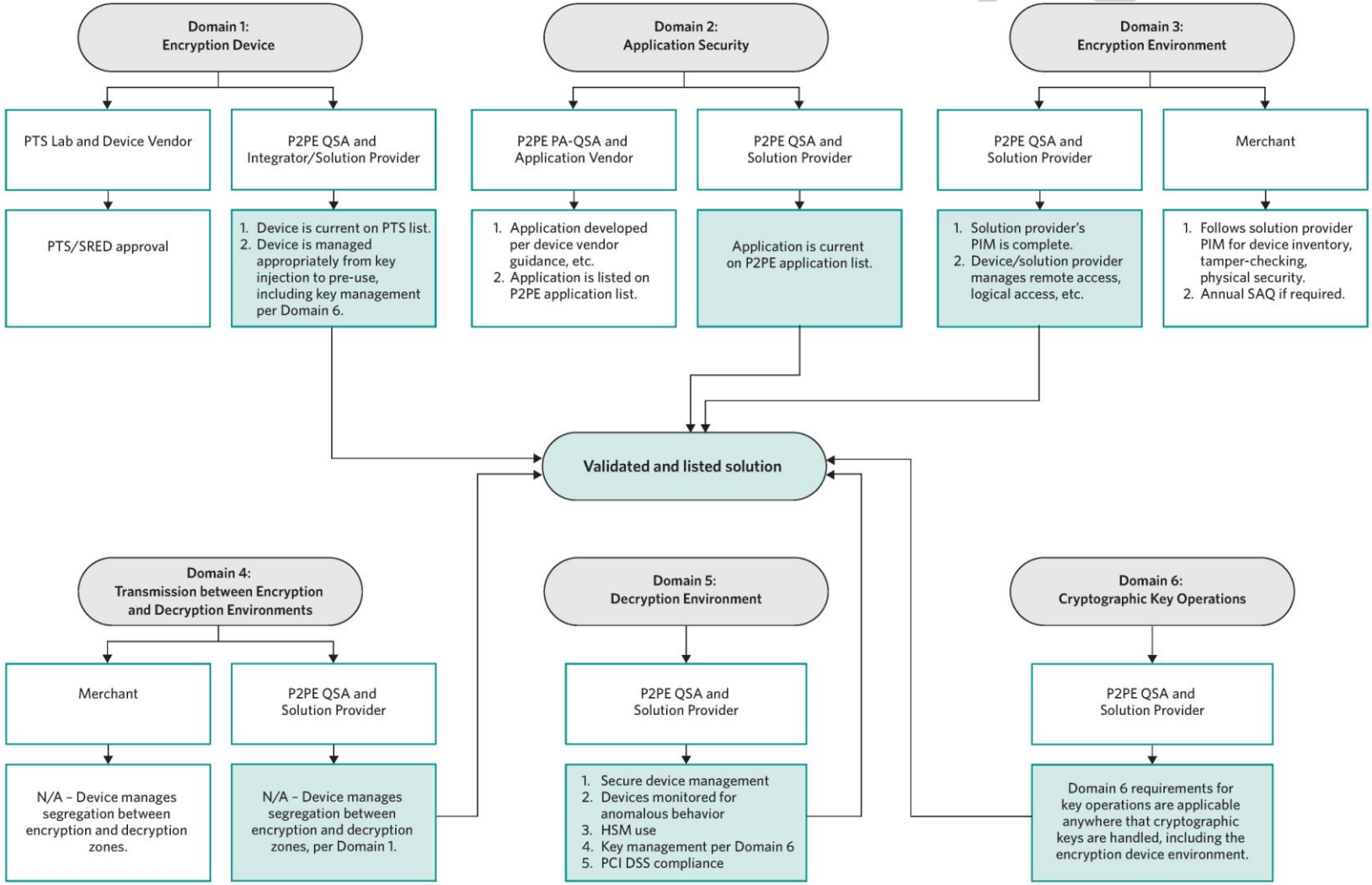


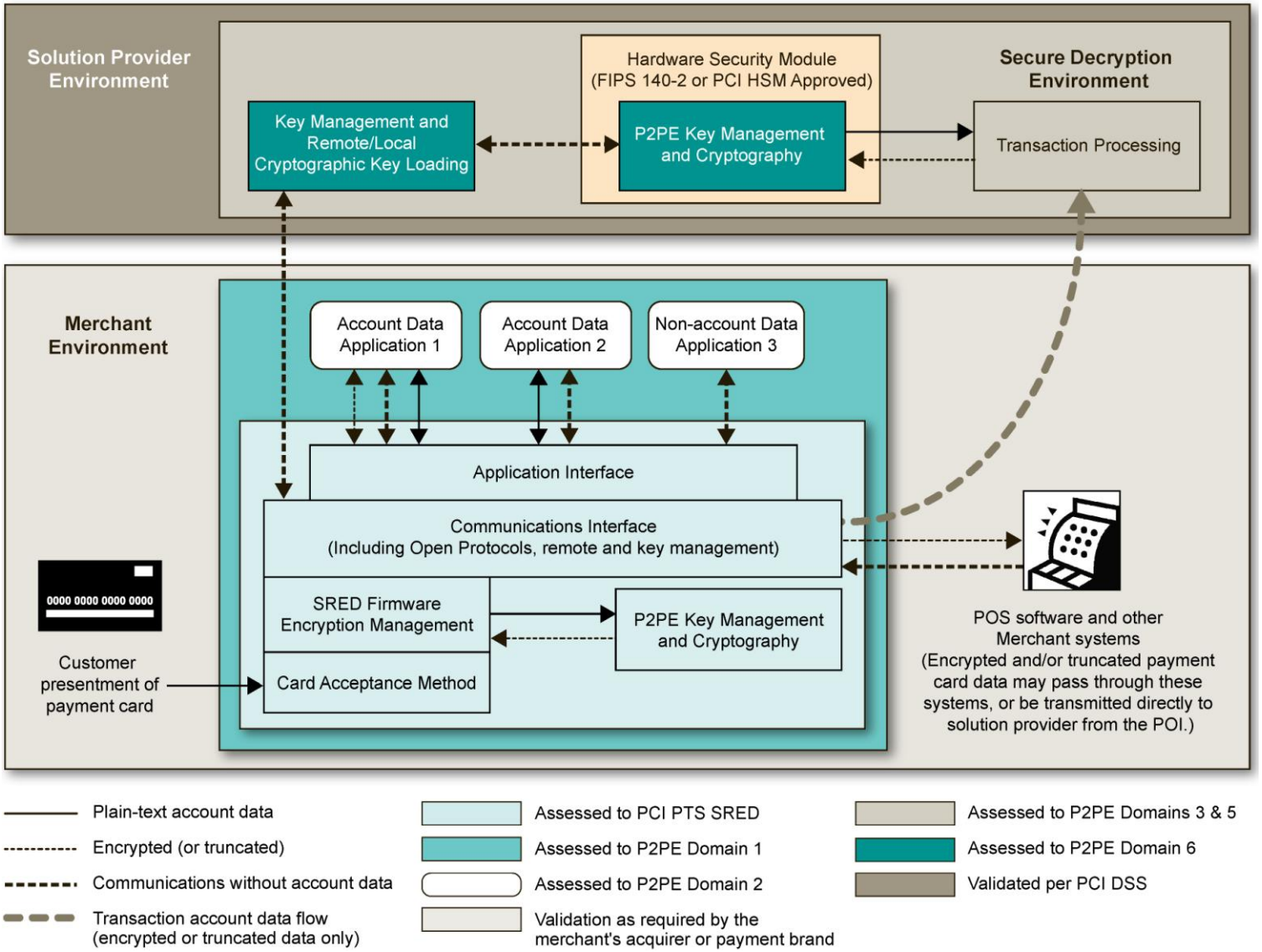
Table 2: At a Glance - Requirements and Processes for P2PE Solution Validation

Validation Requirements and Process for P2PE Solution Developers and Providers				
Stakeholder	**Step**	**Validation Process**	**Validation Requirements**	**Approval**
POI Manufacturer	Design and build a PCI-approved POI device.	PCI PTS lab evaluates all account data entry methods to ensure that they protect account data entry, and provide for encryption.	PCI PTS SRED/ PCI P2PE Domain 1	**PCI PTS listed**
	Securely manufacture and distribute POIs.	Compliance to PCI PTS attested by manufacturer. See first step below for solution provider.	PCI PTS	
Application Developer	Produce secure applications for POI.	P2PE PA-QSA evaluates all applications in SCD. This includes all applications that may have access to account data but have not been previously evaluated as part of the PCI-approved POI device approval process.	PCI P2PE Domain 2	**PCI P2PE listed**
Solution Provider	Secure environments where encryption devices are present.	P2PE QSA ensures solution provider securely manages devices in their possession, and provides merchant instructions for security of devices in the merchant's possession.	PCI P2PE Domain 1, Domain 3	**PCI P2PE listed**
	Ensure that traffic between POI and decryption environment (HSM) is controlled and secure.	P2PE QSA evaluates the integration of the SCD and decryption environment to ensure that it ensures secure account data encryption.	PCI P2PE Domain 4	
	Provide a secure decryption environment for the HSM.	P2PE QSA evaluates the decryption environment of the solution provider to ensure it secures any decrypted account data.	PCI P2PE Domain 5	
	Provide secure key management for all SCDs (POIs and HSMs).	P2PE QSA evaluates the ways in which keys are generated, distributed, loaded, and managed. This includes the loading of any root public keys.	PCI P2PE Domain 6	
	Provide integrated P2PE solution to merchants.	P2PE QSA ensures that the overall solution provided to the merchants complies with the above requirements, and provides instructions for secure deployment.	PCI P2PE All Domains	

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

- As shown in the above table, a P2PE merchant is able to reduce PCI DSS scope by implementing a validated P2PE solution, and validates compliance as required by their acquirer or payment brands. However, this scope reduction does not entirely remove or replace all of a merchant's PCI DSS compliance or validation obligations. For example, applicable requirements covering the education of staff handling account data, security policies, third-party relationships, and physical security of media will still apply to merchants that have implemented a validated P2PE solution. Merchants with account data channels external to the validated P2PE solution will also need to verify that the scope of their PCI DSS assessment is appropriate for their overall validation, and to be eligible for PCI DSS scope reduction due to use of a validated P2PE solution, must ensure that any other payment channels within the merchant environment are adequately segmented (isolated) from the P2PE environment.

Figure 2: At a Glance - Illustration of a typical P2PE Implementation and Associated Requirements



The above diagram shows an example of a generic P2PE implementation and illustrates which domains apply to each of the areas involved. In this example, we have an approved SRED POI device being used by the merchant for all account data acceptance and processing. This SRED device provides within its boundary of approval—that is, the systems tested to the PCI PTS SRED requirements by the PTS laboratory—the hardware and firmware that perform all card acceptance, encryption, key management, and communications.

In this example, the POI also has three applications resident within the boundary of the SRED approval, but which have not been evaluated to the SRED requirements. These applications are:

- Application 1 accesses both plain-text account data as well as account data encrypted by the SRED functions of the POI device.
- Application 2 accesses only plain-text account data. This may be a loyalty application that tracks the use of payment cards co-branded with some loyalty scheme. As this application does not retrieve any account data encrypted by the SRED functions of the POI, it must not communicate any account data (plain text or encrypted) outside of the POI.
- Application 3 does not access account data at all (Applications 1 and 2 also implement some modes of operation where account data is not communicated). An example of this type of application may be a loyalty application which tracks the use of non-PCI branded loyalty cards.

The diagram shows that these applications do not communicate directly; any communications between the applications occurs through the APIs provided by the SRED firmware of the POI device. Note that this does not mean that the applications cannot communicate together; the requirements allow for the applications to communicate where necessary *through the firmware APIs*, and part of the evaluation of the applications to Domain 2 of this standard will be to ensure that any such communication does not compromise the security of account data (for example, by passing plain-text account data from Application 1 to Application 3).

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

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

1) All key-management and key-loading functions must be implemented within the SRED-approved firmware. Applications must not bypass these functions, or provide key-management or key-loading functions themselves.
2) All applications that *may* be able to access plain-text account data are in scope of the requirements of P2PE Domain 2, or must have been assessed as part of the PCI PTS SRED approval. This may include traditional payment applications, non-payment applications that may require access to payment data (for example, loyalty applications), as well as applications that are not used for any payment functions and do not access account data. This last group of applications must be evaluated only to verify that they do not access account data in any way, and do not do anything to compromise the security of the device (for example, provide non-approved remote management functions).
3) The POI device only outputs account data that has been encrypted by the approved SRED functions. Applications must not implement their own encryption functions, algorithms, or modes of operation.

4) Within the P2PE environment, the merchant does not allow for any other method of acceptance of payment card information, except through the PCI-approved POI device. The merchant ensures that any other payment channels within the merchant environment are adequately segmented (isolated) from the P2PE environment. All processing and transmission of account data is performed by the P2PE solution provided by the solution provider.

5) The secure decryption environment is external to the merchant, provided by a P2PE solution provider that also provides the key-management functions for the SCDs. Data sent to the solution provider for decryption may pass through other merchant systems (such as cash registers or internal networks) but there is no possibility that this data may be decrypted within the merchant environment.

6) Although specific message formats can be implemented within an application, all external communications are provided through the communications options provided by the combination of PCI-approved POI device hardware and firmware.

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

Domain 1: Encryption Device

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 1: Encryption Device Build secure devices and protect devices from tampering during manufacture and delivery.	▪ POI device managed by solution provider. ▪ Hardware encryption performed by device. ▪ POI is a PCI-approved POI device.	1A Build PCI-approved POI devices 1B Securely manage equipment used to protect account data up to point of deployment	▪ POI Device Manufacturer ▪ P2PE Solution Provider (for example, acquirer or processor)

Domain 1 requirements encompass building secure point-of-interaction (POI) devices and securely managing and protecting those POI devices during manufacture and delivery. Requirement 1A is met by using a PCI-approved POI device, whereas the device-management requirements in 1B are met by the party(ies) that manage and secure POI devices during manufacture and delivery.

P2PE Requirements for Domain 1

Requirement 1A: Build PCI-approved POI devices.

Account data must be encrypted in equipment that is resistant to physical and logical compromise.

1A-1 The security characteristics of secure cryptographic devices provide tamper-resistance, detection, and response features to help prevent successful attacks involving penetration, monitoring, manipulation, modification, or substitution of the devices to recover protected data.

1A-1.1 Encryption operations must be performed using a device approved per the PCI PTS program, with SRED (secure reading and exchange of data) listed as a "function provided," and with the SRED capabilities enabled and active, and the approval must match the deployed device in the following characteristics:

a) Model name/number
b) Hardware version number
c) Firmware number
d) SRED as a function provided by the device
e) Any applications resident within the device (including any applications that may not use but could access account data)

P2PE Requirements for Domain 1

Requirement 1B: Securely manage equipment used to protect account data up to point of deployment.

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

1B-1 Employ POI device management at initial key-loading facility and pre-use until placed into service, and for any POI devices returned to the key-management facility or the vendor or their agent for repair or other disposition.

1B-1.1 Secure cryptographic devices (SCDs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the loading of cryptographic keys.

1B-1.1.1 Controls exist and are implemented to protect SCDs from unauthorized access up to point of deployment.

a) Access to all cryptographic devices is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any secure cryptographic device

b) SCDs do not use default keys (such as keys that are pre-installed for testing purposes), passwords, or data.

c) All personnel with authorized access to SCDs are documented in a formal list and authorized by management.

1B-1.2 Unauthorized individuals must not be able to access, modify, or substitute any SCD.

a) A documented “chain of custody” process is in place to ensure that all SCDs are controlled from receipt through installation and use.

b) Controls, including the following, must ensure that all installed hardware components are from a legitimate source:

- Compare the device serial number to the serial number on the purchase order, shipping waybill, or manufacturer’s invoice or similar document to ensure device substitution has not occurred.
- Documentation used for this process must not be received with the shipment).

1B-1.3 Dual-control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or backup devices. Procedural controls may exist to support the prevention and detection of substituted cryptographic devices, which may be a combination of physical barriers and logical controls, but cannot supplant the implementation of dual control mechanisms.

P2PE Requirements for Domain 1

1B-1.4 Physical protection of the SCD from receipt up to the point of key-insertion or inspection is in place. For example, one or more of the following controls (or alternatives that achieve the same protection) may be implemented:

a) Transportation from the manufacturer's facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.

b) Shipping from the manufacturer's facility to the place of key-insertion in physically secure and/or trackable packaging (for example, pre-serialized, counterfeit-resistant, or tamper-evident packaging). The devices are then stored is such packaging, or in secure storage, until key-insertion occurs.

c) A secret, device-unique "transport-protection token" is loaded into each SCD at the manufacturer's facility. Before key-insertion, the SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key.

1B-1.5 Each secure cryptographic device is inspected and tested immediately prior to key-insertion to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized modifications. Maintain records of the tests and inspections. Tests should include:

a) Running self-tests to ensure the correct operation of the cryptographic device.

b) Re-installing devices only after confirming that the device has not been tampered with or compromised.

c) Confirming that physical and logical controls and anti-tamper mechanisms are not modified or removed.

1B-1.6 Documented inventory control and monitoring procedures exist and are implemented to accurately track device locations from receipt of the device until ready to ship, including devices used for key loading or signing authenticated applications (such as "whitelists"). The documented inventory must provide for the following:

a) Upon receipt or no later than key loading, a device serial number is entered into an asset registry. The device is protected against unauthorized substitution or modification until a secret key has been loaded into it.

b) Detection of lost or stolen equipment.

1B-1.7 When the SCD is shipped from the key-loading facility to the initial point of use, procedures are in place and implemented to ensure that the device that is shipped arrives unaltered at the initial point of use, including the following:

a) If the device is stored en route, it must be under auditable controls that account for the location of every cryptographic module at any point in time.

b) Documented procedures are in place and implemented to transfer accountability for the SCD from the key-loading facility.

1B-2 Procedures must be in place and implemented to ensure the destruction of any cryptographic keys or key material within any HSMs, POI or key-loading devices that are removed from service, retired at the end of the deployment lifecycle, or returned for repair.

P2PE Requirements for Domain 1

1B-2.1 Procedures including the following are in place and implemented to destroy cryptographic keys or key material within any HSMs or POI or key-loading devices that are removed from service, retired at the end of the deployment lifecycle, or returned for repair:

a) Devices are tracked during the return process to prevent unauthorized use of such devices.

b) Once received, all cryptographic keys and all account data are destroyed.

Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.

1B-2.2 Procedures are in place to ensure that any secure cryptographic devices to be removed from service, retired, or returned for repair are not intercepted and used in an unauthorized manner, as follows:

a) The entity is notified that device is being returned.

b) Devices are transported via trusted carrier service—for example, bonded carrier.

c) Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.

d) Once received, devices remain in their original packaging until ready for destruction.

1B-2.3 If a secure cryptographic device has been removed from service, all keys stored within the device must be securely destroyed.

a) Dual control is implemented for all critical decommissioning processes.

b) Key and data storage are rendered irrecoverable (for example, zeroized) when a device is decommissioned.

c) If necessary, the device must be physically destroyed so it can neither be placed into service again or allow the disclosure of any secret data or keys.

d) SCDs being decommissioned are tested and inspected to ensure keys and account data have been destroyed, and records of the tests and inspections are maintained.

1B-3 Any secure cryptographic device capable of generating or loading cryptographic keys or for signing applications to be loaded onto a POI device, is protected against unauthorized use.

1B-3.1 For HSMs and other secure cryptographic devices used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into a POI device, procedures must be in place and implemented to protect against unauthorized access and use. Examples of these secure cryptographic devices include HSMs or key-injection/loading devices (KLD). Note that POIs are not examples of the specific cryptographic devices to which this requirement applies. Required procedures and processes include the following:

P2PE Requirements for Domain 1

	1B-3.1.1	The device has logical or physical characteristics (for example, passwords or physical high-security keys) that prevent the device being authorized for use except under the dual control of at least two authorized people. For example, dual control may be implemented for logical access via two individuals with two different passwords, or for physical access via a physical lock that requires two individuals with two different keys. ▪ Passwords used for dual control must each be of at least five decimal digits (or of an equivalent size).
	1B-3.1.2	Dual control must be implemented, and the device must be under continuous supervision for the following: a) To enable the key-encryption or signing functions (via dual control for logical access) and/or to provide physical protection of the equipment (via dual control for physical access); b) To place the device into a state that allows for the input or output of plain-text key components; c) For all access to key-loading devices (KLDs) and authenticated application-signing devices; and d) To detect unauthorized access when in a useable state.
	1B-3.1.3	HSMs, key-loading devices (KLDs) and authenticated application-signing devices do not use default passwords.
	1B-3.1.4	To detect any unauthorized use, devices are at all times are either: a) Locked in a secure cabinet, and/or sealed in tamper-evident packaging, or b) Under the continuous supervision of at least two authorized people.
1B-4		Documented procedures exist and are demonstrably in use to ensure the security and integrity of cryptographic devices placed into service, initialized, deployed, used, and decommissioned.
	1B-4.1	Written procedures exist governing the secure return and decommissioning of cryptographic devices, including the following: a) All affected parties are aware of required processes and provided suitable guidance on the secure return and decommissioning of cryptographic devices. b) Records are maintained of all tests and inspections given to cryptographic devices before they are placed into service, as well as devices being decommissioned.

P2PE Requirements for Domain 1

1B-4.2 Procedures that govern access to HSMs must be in place, implemented, and known to data center staff and any others involved with the physical security of such devices. HSM protections must include at least the following:

a) Any physical keys needed to activate the HSM are stored securely.

b) If multiple physical keys are needed to activate the HSM:

   i. They are assigned to separate designated custodians.

   ii. Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.

c) Anti-tamper sensors are enabled as required by the security policy of the HSM.

d) When HSMs are connected to online systems, they are not enabled in a sensitive state, which is a state that allows for executing functions or services that are not available during normal use. Examples of functions or services not available during normal use include but are not limited to: loading an HSM master key, deleting stored transactions, altering device configuration, and outputting clear-text keying material.

Domain 2: Application Security

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 2: Application Security Secure applications in P2PE environment.	▪ Application within secure controller of a PCI-approved POI device. ▪ All applications have been assessed and are listed as approved P2PE applications.	2A Protect PAN and SAD. 2B Develop and maintain secure applications. 2C Implement secure application management processes.	▪ Application Vendor ▪ P2PE Solution Provider

Although secure cryptographic devices are often considered as "hardware" devices, many SCDs will allow for the loading and execution of software applications that may have been developed after the evaluation and approval of that SCD. It is vital to the security of these devices—and the systems that rely on the operation of these devices—that any such applications have been assessed to confirm their secure operation. To this end, these requirements require both the confirmation that a PCI-approved POI device is in use, as well as the independent assessment of any software applications that may be resident within the SCD. However, it should be understood by those using this standard to assess merchant environments that some "simple" secure cryptographic devices may exist that do not provide for any applications, and implement all functionality within the PCI-approved POI device hardware and firmware combination .

All software implemented on an SCD must be assessed and confirmed to be secure. The evaluation of a PCI-approved POI device includes all firmware in the device, and may include some (but may not include all) applications. Applications are often developed specifically for each solution provider, and therefore are not included in the scope of the PCI-approved POI device evaluation. For example, the PCI-approved firmware may release plain-text account data to an authenticated application within the device for the purposes of formatting the payment message for the specific solution provider being used, but where this authenticated application was not included in the evaluation of the PCI-approved POI device. In this example, the application with access to plain-text account data should undergo validation by a P2PE PA-QSA per Domain 2 requirements and become listed on the List of PA-DSS Validated Payment Applications. Requirements in Domain 2 entail protecting PAN and SAD, developing and maintaining secure applications, and incorporating secure application management processes.

Note that for this hardware/hardware scenario, these "applications" *may* not be "payment applications" as traditionally defined by PA-DSS since they may not store, process, or transmit account data as part of authorization or settlement. Rather, these are applications that are installed on the PCI-approved POI device according to device vendor guidance (including but not limited to communication only with the secure controller of the device). These applications may have the ability to access clear-text account data prior to that data being encrypted by the device (for example, such access may be necessary for routing purposes). Once the application completes its designated business function, the account data is returned to the secure controller of the device for encryption or secure deletion.

Of course, "traditional" payment applications as defined by PA-DSS would also still require validation against Domain 2, as these applications would also have the ability to access plain-text cardholder data. Also, applications that do not access account data but are managed and authenticated in the same way as applications which do access account data—that is, they use the same authentication mechanisms, and they

are executed within the boundary of approval of the SRED device—require validation against Domain 2. This will validate that these applications are not accessing account data, and are not bypassing or overriding any security features provided by the other approved components of the device.

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

P2PE Requirements for Domain 2

Requirement 2A: Protect PAN and SAD.

	The application protects PAN and SAD.
2A-1	The application does not retain PAN or SAD after completion of the application's business processing.
2A-1.1	The application does not store PAN or SAD data after the business process of the application is completed (even if encrypted). Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (for example, offline transactions). However, at all times, SAD is not stored after the completion of the authorization process.
2A-1.2	A process is in place to securely delete any PAN or SAD stored during the application's business processing.
2A-2	The application does not transmit plain-text PAN or SAD outside the secure boundaries of the device, and only uses communications methods included in the scope of the PCI-approved POI device evaluation.
2A-2.1	The application only exports PAN or SAD data that has been encrypted by the firmware of the PCI-approved POI device. Where plain-text data is passed from the application to other applications—to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI—the handling of this data is examined to confirm its compliance with the requirements of this section. Output of plain-text account data that is verified to not be related to any of the PCI payment brands is acceptable. The security of this process is evaluated under Requirement 2A-2.4.

P2PE Requirements for Domain 2

2A-2.2	The application only uses external communication methods that have been included in the PCI-approved POI device evaluation.. *For example, the POI may provide an IP stack approved per the PTS Open Protocols module that allows for the use of the SSL/TLS protocol, or the device may communicate transaction data encrypted by its PCI PTS SRED functions using a serial port or modem included in the POI. It would be a non-compliance to this requirement if the application implemented its own IP stack, or utilized its own SSL implementation.*
2A-2.3	Securely delete any PAN or SAD used for debugging or troubleshooting purposes. These data sources must be collected in limited amounts and only collected when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.
2A-2.4	Ensure that any methods used to allow for the output of plain-text (non-PCI payment accounts/cards only) account data are cryptographically authenticated by the PCI-approved POI device's firmware, and implemented to provide for accountability and auditing.

Requirement 2B: Develop and maintain secure applications.

The application is developed securely and in accordance with industry standards.

2B-1	The application developer uses industry-standard software development life cycle practices that incorporate information security.
2B-1.1	The software vendor develops applications based on industry best practices, and incorporates information security throughout the software development life cycle. These processes must include the following:
2B-1.1.1	Live PANs are not used for testing or development.
2B-1.1.2	Test data and accounts are removed before release to customer.
2B-1.1.3	Custom application accounts, user IDs, and passwords are removed before applications are released to customers
2B-1.1.4	Application code, and any non-code configuration options such as "whitelists," are reviewed prior to release after any significant change, to identify any potential vulnerabilities or security flaws.
2B-1.2	Develop applications based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes.
2B-1.3	Software developer must follow change control procedures for all product software configuration changes. The procedures must include the following:
2B-1.3.1	Documentation of impact
2B-1.3.2	Documented approval of change by appropriate authorized parties
2B-1.3.3	Functionality testing to verify that the change does not adversely impact the security of the device

2B-1.3.4	Back-out or application de-installation procedures
2B-2	The application is implemented securely, including the secure use of any resources shared between different applications.
2B-2.1	The application is developed in accordance with the security guidelines provided by the device's platform vendor. These security guidelines are intended for application developers, system integrators, and end-users of the platform to meet requirements in the PCI PTS Open Protocols module as part of a PCI-approved POI device evaluation. The user guidance the vendor includes with their PTS evaluation materials ensures the secure use of, and integration with, the device platform components: • IP and link layer (where implemented by the POI) • IP Protocols (where implemented by the POI) • Security protocols, including specific mention if specific security protocols or specific configurations of security protocols are not to be used for financial applications and/or platform management • IP services, including specific mention if specific IP services or specific configurations of IP services are not to be used for financial applications and/or platform management (where implemented by the POI) • Security and configuration management • For each platform component listed above, coverage of, including but not limited to, the following as it relates to the application's specific business processing: o Vulnerability assessment o Configuration and updates o Key management o Data integrity and confidentiality o Server authentication
2B-2.2	The application development process includes secure integration with any shared resources.
2B-2.3	The application does not bypass or render ineffective any application segregation that is enforced by the POI.
2B-2.4	The application does not bypass or render ineffective any OS hardening implemented by the POI.
2B-2.5	The application does not bypass or render ineffective any encryption or account data-security methods implemented by the POI.
2B-3	The application vendor uses secure protocols, provides guidance on their use, and has performed integration testing on the final application.

2B-3.1	The application developer's process includes full documentation, and integration testing of the application and intended platforms, including that: a) The application developer provides key-management security guidance describing how keys and certificates have to be used. Examples of guidance includes what SSL certificates to load, how to load account data keys (through the firmware of the device), when to roll keys, etc. The application does not perform account data encryption since that is performed only in the firmware of the PCI-approved POI device.) b) The protocol used to communicate with the solution provider uses the communications functions provided by the PCI-approved POI device as follows: i. Provides the confidentiality of data sent over a network connection ii. Authenticates the server of the solution provider iii. Detects replay of messages, and enables the secure handling of exceptions iv. Utilizes a unique value during each transaction to prevent replay attacks c) The application developer has performed final integration testing on the device, which has included identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform.
2B-4	The application does not implement any encryption or key-management functions. All such functions are performed by the approved SRED firmware of the device.
2B-4.1	The application does not bypass or render ineffective any encryption or key-management functions implemented by the approved SRED functions of the device. At no time should plain-text keys be passed through an application that has not undergone SRED evaluation.

Requirement 2C: Implement secure application management processes.

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

2C-1	New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.
2C-1.1	Software developers must establish and implement a process to identify newly discovered security vulnerabilities and to test their applications for vulnerabilities.
2C-1.2	Software vendors must establish and implement a process to develop and deploy updates to address discovered security vulnerabilities in a timely manner.
2C-2	The application implements only trusted, signed, authenticated updates using an approved security protocol evaluated for the PCI-approved POI device.

P2PE Requirements for Domain 2

2C-2.1 Ensure that the application only accepts authenticated changes as follows:

- The application only allows for updates using an approved security protocol of the POI.
- Unauthenticated changes are not allowed (for example, all changes to whitelists must be authenticated).
- If the application may be accessed remotely, remote access to the application must be authenticated using either cryptographic means (which use keys managed under dual control and split knowledge) or two-factor authentication.
- The application developer includes guidance for whoever signs the application (including for whiitelists), which includes requirements for dual control over the application-signing process.

The application developer provides documentation and training.

2C-3 Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.

2C-3.1 Develop, maintain, and disseminate a P2PE Instruction Manual for the application's installation, maintenance and upgrades, and general use that accomplishes the following:

2C-3.1.1 Addresses all requirements in this P2PE Domain 2 document wherever the P2PE Instruction Manual is referenced.

2C-3.1.2 Includes a review at least annually and updates to keep the documentation current with all device upgrades and major and minor software changes.

2C-3.2 Develop and implement training and communication programs to ensure application installers (for example, resellers/ integrators) know how to implement the application and according to the P2PE Instruction Manual.

2C-3.2.1 Update the training materials on an annual basis and whenever new application versions are released.

Domain 3: Encryption Environment

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 3: Encryption Environment Secure environments where POI devices are present.	▪ No storage of CHD after payment transaction is finalized. ▪ Within the segmented P2PE environment, no CHD processed through channels or methods external from an approved SCD. ▪ All device and key-management functions are performed by solution provider. ▪ POI devices are implemented and maintained in accordance with the P2PE Instruction Manual.	**3A** Secure POI devices throughout the device lifecycle. **3B** Implement secure device-management processes.	▪ P2PE Solution Provider

In this scenario for hardware/hardware, the only merchant system that stores, processes, or transmits account data is the PCI-approved POI device, which also isolates all account data from the merchant environment. Because all account data operations are managed by the validated solution provider, the merchant has reduced responsibility for validating PCI DSS compliance.

POI encrypting devices must be a PCI-approved POI device, and the customer PAN may be inputted from the card's magnetic stripe or chip. Alternatively, the PAN may enter the POI by manual input. Requirements in Domain 3 include physically securing SCDs throughout the device lifecycle and implementing secure device-management processes.

For the hardware/hardware scenario, all requirements in Domain 3 are the responsibility of the P2PE solution provider, who must also provide detailed instructions for the merchant in the P2PE Instruction Manual. As part of any validation required by the merchant's acquirer or payment brand, the merchant would submit an annual attestation that their environment meets the eligibility criteria for the hardware/hardware scenario, and that they have implemented procedures for securing and managing their P2PE devices in accordance with the P2PE Instruction Manual. If so directed by a merchant's acquirer or payment brand, merchants using P2PE solutions may be eligible to complete an annual SAQ that specifically addresses both their P2PE requirements and PCI DSS compliance validation. A proposed validation approach for P2PE merchants is included in Appendix A of this document.

P2PE Requirements for Domain 3

Requirement 3A: Physically secure POI devices throughout the device lifecycle.

Secure POI devices throughout the device lifecycle.

3A-1 Solution provider maintains a device-tracking and inventory system for devices in their possession, and provides related instructions to merchants.

3A-1.1.a Maintain a device-tracking system and procedures to identify and locate all POI devices, including those devices:

- Deployed
- Awaiting deployment
- Undergoing repair or otherwise not in use
- In transit

3A-1.1.b Provide instructions via the P2PE Instruction Manual for the merchant to maintain a device-tracking system and procedures, including those devices:

- Deployed
- Awaiting deployment
- Undergoing repair or otherwise not in use
- In transit

3A-1.2.a Perform device inventories at least annually to detect removal or substitution of devices.

3A-1.2.b Provide instructions via the P2PE Instruction Manual for the merchant to perform device inventories at least annually.

3A-1.3.a Maintain an inventory of all devices to include at least the following:

- Make, model of device
- Location (site/facility)
- Serial number
- General description
- Security seals, labels, hidden markings, etc.
- Number and type of physical connections to device
- Date of last inspection
- Firmware version
- Hardware version
- Any application versions

P2PE Requirements for Domain 3

3A-1.3.b	Provide instructions via the P2PE Instruction Manual for the merchant to maintain an inventory of all PCI-approved POI devices, to include at least those items described in 3A-1.3.a.
3A-1.3.1.a	Secure the device inventory from unauthorized access.
3A-1.3.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to secure the device from unauthorized access.
3A-1.4.a	Implement procedures for responding to missing or substituted devices as part of the incident response plan (refer 5C-4).
3A-1.4.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures for responding to missing or substituted devices as part of the incident response plan.
3A-2	Solution provider physically secures devices when not deployed or being used while in their possession, and provides related instructions to merchants.
3A-2.1.a	Physically secure the storage of devices awaiting deployment.
3A-2.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to secure the storage of devices awaiting deployment.
3A-2.2.a	Physically secure the storage of devices undergoing repair or otherwise not in use.
3A-2.2.b	Provide instructions via the P2PE Instruction Manual for the merchant to physically secure the storage of devices undergoing repair or otherwise not in use.
3A-2.3.b	Physically secure the storage of devices awaiting transport between sites/locations.
3A-2.3.b	Provide instructions via the P2PE Instruction Manual for the merchant to physically secure the storage of devices awaiting transport between sites/locations.
3A-2.4.a	Physically secure devices in transit, including: • Packing the device using tamper-evident packaging prior to transit. • Procedures for determining whether a device packaging has been tampered with. • Defined secure transport method, such as bonded carrier or secure courier.
3A-2.4.b	Provide instructions to the merchant via the P2PE Instruction Manual for the merchant physically secure devices in transit, to include at least those items described in 3A-2.4.a.
3A-2.5.a	Ensure devices are transported only between trusted/predefined sites/locations : • Only devices received from trusted sites/locations are accepted for use. • Devices received from untrusted or unknown locations are not used unless and until the source location is verified as trusted. • Devices are sent only to trusted sites/locations.

P2PE Requirements for Domain 3

	3A-2.5.b	Provide instructions via the P2PE Instruction Manual for the merchant to only transport devices between trusted/predefined sites/locations, as described in 3A-2.5.a.
3A-3		Solution provider has procedures to prevent and detect the unauthorized alteration or replacement of devices in their possession prior to and during deployment, and provides related instructions to merchants.
	3A-3.1.a	Implement procedures to prevent and detect unauthorized modification, substitution, or tampering of devices prior to deployment. Procedures must include the following: • Validate that serial numbers of received devices match sender records. • Transport documents used for validating device via a separate communication channel. • Perform pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify integrity of device. • Maintain device in original, tamper-evident packaging or store it physically secured, until ready for deployment. • Record device in inventory-tracking system as soon as possible.
	3A-3.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures, including those items described in 3A-3.1.a, to prevent and detect unauthorized alteration or replacement of the device.
	3A-3.2.a	Implement procedures to control and document all physical access to devices prior to deployment. Procedures to include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out
	3A-3.2.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures to control and document all physical access to devices prior to deployment. Procedures to include those items described in 3A-3.2.a.
	3A-3.3.a	Implement a documented audit trail to demonstrate that a device is controlled, and is not left unprotected, at all times from receipt through to installation.
	3A-3.3.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement an audit trail, to demonstrate that a device is controlled, and not left unprotected, at all times from receipt through to installation
3A-4		Solution provider provides instructions to merchants to physically secure devices by preventing unauthorized access, modification, or substitution while devices are deployed for use. This includes both attended and unattended devices (for example, kiosks, “pay at the pump” etc.).

P2PE Requirements for Domain 3

3A-4.1	Provide instructions via the P2PE Instruction Manual for the merchant to select appropriate locations for deployed devices, for example: • Control public access to devices such that device access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locate devices so they can be observed/monitored by authorized personnel—for example, during daily store checks of the devices performed by store/security staff. • Locate devices in an environment that deters compromise attempts—for example, through lighting, access paths, visible security measures, etc..
3A-4.2	Provide instructions via the P2PE Instruction Manual for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution.
3A-4.3	If devices—for example, wireless, handheld, line-busters etc.—cannot be physically secured, provide instructions via the P2PE Instruction Manual, for the merchant to implement procedures to prevent unauthorized removal or substitution of devices—for example, secure room when not in use, assign responsibility to individual when in use, observe at all times, sign in/out.
3A-5	Solution provider prevents unauthorized physical access to devices undergoing repair or maintenance while in their possession, and provides related instructions to merchants..
3A-5.1.a	Implement procedures for identification and authorization of repair /maintenance personnel and other third parties prior to granting access, to include the following: • Procedures to verify the identity and authorization of repair personnel. • All repair personnel must be verified and authorized prior to granting access. • Unexpected personnel must be denied access unless fully validated and authorized. • Escort and monitor authorized personnel at all times.
3A-5.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures for identification and authorization of repair/maintenance personnel and other third parties prior to granting access. Procedures to include those items described in 3A-5.1.a

Requirement 3B: Implement secure device-management processes.

3B-1	Solution provider securely maintains devices being returned, replaced, or disposed of, and provides related instructions to merchants.
3B-1.1.a	Implement process for securing devices being returned or replaced.
3B-1.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to implement a process for secure devices being returned or replaced.

P2PE Requirements for Domain 3

3B-1.2.a Implement procedures for secure disposal of devices.

- Return devices to authorized vendor for destruction.
- Wipe memory / clear devices prior to destruction

3B-1.2.b Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures for the secure disposal of devices.

3B-2 Solution provider configures devices to fail closed if encryption mechanism fails.

3B-2.1.a Upon failure of the encryption mechanism, the device must immediately fail closed and/or be immediately removed/shut down/taken offline until the P2PE encryption is restored.

3B-2.1.b The device cannot be re-enabled until it is confirmed that either:

- The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or
- All applicable PCI DSS controls are enabled and enforced within the environment to protect account data, since the P2PE solution can no longer be used to reduce PCI DSS scope.

3B-2.1.c Provide instructions via the P2PE Instruction Manual for the merchant outlining processes to be implemented upon device failure.

Domain 5 requires that solution providers actively monitor traffic that is received into the decryption environment, to confirm that the POI equipment in the merchant's encryption environment is not outputting clear-text CHD, through some error or misconfiguration. Refer to 5C-3.1.

Secure logical access to POI devices.

3B-3 Solution provider restricts access to devices to authorized personnel.

3B-3.1 Merchant has no administrative access to the device (cannot change anything on the device that can impact the security settings of the device, has no access to keys, has read-only access to transaction data—not full PAN nor SAD, no access to device settings or configuration). Merchant access, if needed, must meet the following:

- Be read-only.
- Only view transaction-related data.
- Cannot view or access encryption keys.
- Cannot view or access full PAN.
- Cannot view or access SAD.
- Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD.

P2PE Requirements for Domain 3

3B-3.2	Only authorized solution provider personnel have access to devices.
3B-3.3	Access and permissions on devices are granted based on least privilege and need to know.
3B-4	Solution provider provides features for secure remote access to devices deployed at merchant locations.
3B-4.1	Solution provider's authorized personnel use two-factor or cryptographic authentication for all remote access to merchant POIs over a public network (Internet).
3B-4.2	Remote access to merchant devices is only from the solution provider's authorized systems and only from the solution provider's PCI DSS compliant environment/network.
3B-4.4	Merchants do not have remote access to the merchant POIs.
3B-5	Solution provider implements secure identification and authentication procedures for remote access to devices deployed at merchant locations, including:
3B-5.1	Authentication credentials for solution provider personnel that are unique for each merchant site
3B-5.2	Tracing all logical access to devices by solution provider personnel to an individual user.
3B-5.3	Maintaining audit logs of all logical access to devices.
3B-6	The solution provider implements procedures for secure updates to devices deployed at merchant locations.
3B-6.1	Documented process to ensure secure updates is implemented, including: • Integrity checks • Source authentication
3B-6.2	Develop and deploy patches and other device updates in a timely manner.
3B-6.3	Deliver updates in a secure manner with a known chain-of-trust.
3B-6.4	Maintain the integrity of patch and update code during delivery and deployment.
3B-6.5	If a solution provider obtains PAN or SAD to help troubleshoot merchant transaction problems, the solution provider securely deletes any PAN or SAD used for debugging or troubleshooting purposes. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.

P2PE Requirements for Domain 3

The P2PE solution provides logging of critical processes.

3B-7 The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).

3B-7.1 Ensure that any changes to the critical functions of the POI are logged—either on the device or within the remote-management systems of the P2PE solution provider. Critical functions include application and firmware updates, as well as changes to security-sensitive configuration options, such as whitelists or debug modes.

Monitor and inspect POI devices.

3B-8 Solution provider implements tamper-detection mechanisms for devices in their possession, and provides related instructions to merchants.

3B-8.1.a Perform periodic physical inspections of devices to detect tampering or modification of devices.

3B-8.1.b Provide instructions via the P2PE Instruction Manual for the merchant to perform periodic physical inspections of devices to detect tampering or modification of devices. Detailed procedures for performing periodic physical inspections to include:

- Description of tamper-detection mechanisms
- Guidance for physical inspections including photographs or drawings of the device illustrating what the merchant is to inspect, for example:
  - Missing or altered seals or screws, extraneous wiring, holes in the device or the addition of labels or other covering material that could be used to mask damage from device tampering).
  - If the device is a PTS POI v3 device, weigh the POI equipment for comparison with vendor specification weight to identify potential insertion of tapping mechanisms within devices.
- Recommendations for frequency of inspections (variable per device specifics).

3B-8.2.a Implement tamper-detection processes for devices deployed in remote or unattended locations—for example, use cameras or other physical mechanisms to alert personnel to physical breach.

3B-8.2.b Provide instructions via the P2PE Instruction Manual for the merchant to implement tamper-detection processes for devices deployed in remote or unattended locations—for example, the use cameras or other physical mechanism to alert personnel to physical breach.

3B-8.3.a Implement procedures for responding to tampered devices.

3B-8.3.b Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures for responding to tampered devices.

P2PE Requirements for Domain 3

3B-9	Solution provider implements mechanisms to monitor and respond to suspicious activity on POI devices deployed at merchant locations.
3B-9.1.a	Implement controls to provide immediate notification of suspicious activity, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of encryption mechanism • Failure of any device security control
3B-29.1.b	Provide instructions via the P2PE Instruction Manual for the merchant to notify the solution provider of suspicious activity.
3B-9.2	Prepare incident-response procedures to respond to detection of potential security breaches, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device failure of any device security control

Domain 4: Transmissions between Encryption and Decryption Environments

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 4: Transmissions between Encryption and Decryption Environments Segregate operations between encryption and decryption environments.	▪ All decryption operations managed by solution provider. ▪ Merchant has no access to the encryption environment (within POI device) or decryption environment. ▪ Merchant has no involvement in encryption or decryption operations. ***Note that this domain in not applicable for this hardware/hardware scenario.***	4A Segregate duties and functions between encryption and decryption environments. 4B Prevent use of decryption keys.	▪ P2PE Solution Provider

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

Note that for the above reason, this domain is not applicable for Solutions with Encryption, Decryption, and Key Management within Secure Cryptographic Devices—or "hardware/hardware," scenario.

Requirements in Domain 4 are intended to be applicable for scenarios such as the following:

1. When the encryption and decryption environments are part of the same network;
2. Where encrypted account data is being passed between the two environments; and
3. Where the desire is for PCI DSS scope reduction for the parts of the network though which encrypted account data is transmitted and within which there is no ability to decrypt encrypted data or access cryptographic keys.

Requirements in this domain will include those for:

- Segregating duties and functions between encryption and decryption environments; and
- Preventing potential use of decryption keys in the encryption environment, or any network where encrypted data is present, before it reaches the secure SCD in the decryption environment.

Domain 5: Decryption Environment

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 5: Decryption Environment Secure environments where decryption devices are present.	▪ Decryption environment implemented at and managed by solution provider. ▪ Merchant has no access to the decryption environment. ▪ Decryption environment must be PCI DSS compliant.	5A Secure all decryption systems and devices. 5B Implement secure device-management processes. 5C Implement monitoring and response procedures.	▪ P2PE Solution Provider

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

References to “devices” within this section are always to be interpreted as referencing decryption devices, such as HSMs, unless specifically noted. This section is not intended to include requirements to be assessed against encrypting devices, such as POI devices.

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

P2PE Requirements for Domain 5

Requirement 5A: Secure all decryption systems and devices.

Secure decryption devices throughout the device lifecycle.

5A-1 Maintain a decryption device-tracking and inventory system.

5A-1.1 Maintain a device-tracking system and procedures to identify and locate all decryption devices, including those devices:

- Deployed
- Awaiting deployment
- Undergoing repair or otherwise not in use
- In transit

5A-1.2 Perform device inventories to detect removal / substitution of devices at least annually.

5A-1.3 Maintain an inventory of all devices to include at least the following:

- Make, model, and hardware version of device.
- Firmware and any application version(s) of device
- Location
- Serial number
- General description
- Security seals, labels, hidden markings etc.
- Number and type of physical connections to device
- Date of last inspection

5A-1.3.1 Secure the device inventory from unauthorized access.

5A-1.4 Implement procedures for responding to missing or substituted devices as part of the incident response plan.

5A-2 Physically secure decryption devices when not in use.

5A-2.1 Physically secure the storage of devices awaiting deployment.

5A-2.2 Physically secure the storage of devices undergoing repair or otherwise not in use.

5A-2.3 Physically secure the storage of devices awaiting transport between sites /locations.

P2PE Requirements for Domain 5

5A-2.4 Physically secure devices in transit, including:

- Packing the device using tamper-evident packaging prior to transit
- Procedures for determining if a device packaging has been tampered with
- Defined secure transport method, such as bonded carrier or secure courier

5A-2.5 Ensure devices are only transported between trusted sites/locations:

- Only devices received from trusted sites/locations are accepted for use.
- Devices received from untrusted or unknown locations are not used unless and until the source location is verified as trusted.
- Devices are sent only to trusted sites/locations.

5A-3 Prevent and detect the unauthorized alteration or replacement of the device prior to and during deployment.

5A-3.1 Implement procedures to ensure devices are placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering. This requires physical protection of the device up to the point of key-insertion or inspection.

- Validate serial number of received devices match sender records.
- Transport documents used for validating device via a separate communication channel.
- Perform pre-installation inspection procedures including physical and functional tests and visual inspection to verify integrity of device.
- Maintain device in original, tamper-evident packaging until ready for deployment.
- Record device in inventory-tracking system as soon as possible.

5A-3.2 Implement a documented “chain of custody” to ensure that all devices are controlled from receipt through to installation.

5A-4 Physically secure decryption devices by preventing unauthorized access, modification, or substitution while devices are in production.

5A-4.1 Physically secure deployed devices to prevent unauthorized removal or substitution.

5A-5 Prevent unauthorized physical access to devices.

5A-5.1 Physical access to decryption devices is restricted to minimum required personnel.

5A-5.2 Implement procedures to control and document all physical access to devices. Procedures to include:

- Identifying personnel authorized to access devices.
- Restricting access to authorized personnel.
- Maintaining a log of all access including personnel name, company, reason for access, time in/out.

5A-5.3	Implement procedures for identification and authorization of repair /maintenance personnel prior to granting access, to include the following: • Procedures to verify the identity and authorization of repair personnel. • All repair personnel must be verified and authorized prior to granting access. • Unexpected personnel must be denied access unless fully validated and authorized. • Escort and monitor authorized personnel at all times. • Maintain a log of all access including personnel name, company, reason for access, time in/out.
5A-6	Implement tamper-detection for decryption devices.
5A-6.1	Ensure that the hardware security module is at least FIPS140-2 Level 3 or higher certified and configured at FIPS140-2 Level 3 or higher, or a PCI-approved HSM.
5A-6.2	The decryption device is deployed according to the security policy to which it has been approved.

Approval to both FIPS140-2 and PCI HSM requires that the decryption-device manufacturer makes available a security policy document to end users, which provides information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.

Requirement 5B: Implement secure device-management processes.

5B-1	Securely maintain devices.
5B1.1	Document operational security procedures for physical security controls and operational activities throughout device lifecycle, including but not limited to: • Installation procedures • Maintenance and repair procedures • Production procedures • Replacement procedures • Destruction procedures
5B-1.2	Implement process for securing devices being returned or replaced.
5B-1.3	Implement procedures to ensure that all operational keys are zeroized from the hardware security module when removed from service permanently or for repair.
5B-1.4	Implement procedures to document and log the removal process for the repair or decommissioning of the security module.

P2PE Requirements for Domain 5

5B-1.5 Implement procedures for secure disposal of devices.

- Return devices to authorized vendor for destruction.
- Wipe memory / clear devices prior to destruction

Logically secure decryption equipment.

5B-2 Implement administration procedures for logically securing decryption equipment.

5B-2.1 Implement procedures to provide secure administration of decryption devices including but not limited to:

- Management of user interface
- Password/smart card management
- Console/remote administration
- Access to physical keys
- Use of HSM commands

5B-2.2 Implement a process/mechanism to protect the HSM's Application Program Interfaces (APIs) from misuse.

For example, require authentication between the API and the HSM and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate access to the API, the process should limit the exposure of the HSM to a host via connection by a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (for example high speed serial or dedicated Ethernet).

5B-3 Restrict access to authorized personnel.

5B-3.1 Only authorized personnel have access to the device.

5B-3.2 Access and permissions granted based on least privilege and need to know.

5B-4 Provide a mechanism for POI device authentication.

5B-4.1 Devices are authenticated upon connection to the decryption environment and upon request by the solution provider (for example, this authentication can occur via use of cryptographic keys or certificates, uniquely associated with each POI device and decryption system).

P2PE Requirements for Domain 5

Requirement 5C: Implement monitoring and response procedures.

Monitor decryption devices.

5C-1 Implement tamper-detection mechanisms.

5C-1.1 Perform periodic physical inspections of devices to detect tampering or modification of devices. Inspections to include:

- The device itself
- Cabling/connection points
- Physically connected devices

5C-2 Log and monitor suspicious activity.

5C-2.1 Implement mechanisms to provide immediate notification of potential security breaches, including but not limited to:

- Physical breach
- Logical alterations (configuration, access controls)
- Disconnect / reconnect of devices
- Failure of any device security control
- Misuse of the HSM API.

5C-3 Detect encryption failures.

5C-3.1 Implement controls to detect presence of clear-text data and provide immediate notification

Controls must include at least the following:

- Checking for clear-text "track" data.
- Reviewing any decryption errors reported by the HSM, which may be caused by inputting clear-text data when only encrypted data is expected.
- Reviewing any transaction data received without an authentication data block (such as a MAC or signature).
- Reviewing the data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.

Although Domain 5 is concerned with the decryption environment, not the encryption environment, it is the duty of the solution provider to actively monitor traffic received into the decryption environment to confirm that the POI equipment in the merchant environment is not outputting clear-text CHD through some error or misconfiguration.

P2PE Requirements for Domain 5

5C-3.2	Identify source of encryption failure (device, function).
5C-3.3	Implement documented response procedures.
5C-4	Implement incident response procedures.
5C-4.1	Implement procedures for responding to tampered devices.
5C-4.2	Implement procedures for responding to missing or substituted devices.
5C-4.3	Implement procedures for responding to unauthorized key-management procedures or configuration changes.
5C-4.4	Implement procedures for responding to disconnect/reconnect of devices.
5C-4.5	Implement procedures for responding to failure of any device security control.
5C-4.6	Implement procedures for responding to decryption failure.
	Protecting the decryption environment.
5C-5	PCI DSS compliance of decryption environment.
5C-5.1	Decryption environment subject to full PCI DSS compliance

Domain 6: Cryptographic Key Operations

	Scenario: Environments with Encryption, Decryption, and Key Management within Secure Cryptographic Devices		
Domain	**Scope**	**Requirements**	**Responsibility**
Domain 6: Enhanced Cryptographic Key Operations Use strong cryptographic keys and secure key-management functions.	▪ All key-management functions implemented and managed by solution provider. ▪ Merchant has no involvement in key-management operations.	6A Use secure encryption methodologies. 6B Use secure key-generation methodologies. 6C Distribute cryptographic keys in a secure manner. 6D Load cryptographic keys in a secure manner. 6E Ensure secure usage of cryptographic keys. 6F Ensure secure administration of cryptographic keys.	▪ P2PE Solution Provider

Domain 6 covers the use of strong cryptographic keys and secure key-management functions. Implementation of these procedures is fundamental to the security of a P2PE solution. An exploit of a single POI device should not compromise the security of all encrypted data originating from a merchant environment. An example of a secure key-management function is that cryptographic keys used to protect account data cannot be used to verify the authenticity of a software update.

Domain 6 includes enhanced key-management procedures derived from existing industry standards for PIN key management. These procedures include criteria for managing keys and performing decryption functions including but not limited to encryption methodologies, key generation, key loading, key usage, and key administration. These requirements do not assume any specific use case; they can be applied to systems where CHD is encrypted using TDES, AES, or directly with asymmetric keys.

Similarly, these requirements do not assume any specific key-management method. However it should be understood that 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. For example, even if a system does not load externally generated secret or private keys into a POI device and instead relies on asymmetric encryption methods to provide security to account data, the loading and use of the asymmetric public key (and any other keys generated, used, or transferred by such a system) must comply with the requirements set forth in this section of the document—including procedures to ensure the integrity and authenticity of the root public key.

Note that, for hardware/hardware, this domain applies to key management within the solution-provider environment (for example, within their approved HSM), required in Domain 5. It also applies to key management as needed within the POI device (for example, key injection), required in Domain 1.

All requirements relevant to clear-text secret or private-key components/shares apply to all key types (including keys used to secure the components of other keys through encryption). To clarify this, any keys used to secure account data, any key-encrypting keys used to encrypt these keys, or keys that have a direct bearing on the security of the P2PE solution (for example, keys used to protect the integrity of a whitelist), must comply with the requirements of this domain. If a system is used where there are multiple key-encrypting keys, forming a multi-tier "key hierarchy," all keys up to and including the top level "master key" must be assessed to meet these requirements.

For the purposes of this document:

- Secret Key = symmetric key (aka shared secret),
- Private Key = asymmetric key used for signature-generation and decryption operations (this would never be the public key, and no one private key should be used for both operations).)
- Public Key = asymmetric key used for signature-verification and encryption operations (this would never be the private key, and no one public key should be used for both of these operations).

Annexes A and B contain enhanced key management requirements that should be considered by the solution provider, to determine their applicability to their P2PE solution. These Annexes must be applied in the following circumstances:

- **Annex A - Symmetric Key Distribution using Asymmetric Techniques**
  This Annex contains specific requirements pertaining to acquiring entities involved in the implementation of symmetric key distribution using asymmetric keys (remote key distribution) or those entities involved in the operation of Certification Authorities for such purposes. Acquiring entities involved in remote key distribution are subject both to the requirements stipulated in Domain 6 of this document and the additional criteria stipulated in Annex A.
- **Annex B – Key Injection Facilities**
  This Annex contains specific requirements pertaining to those entities that perform key injection of POI devices. Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer, or vendor. This Annex provides additional requirements to those set out in in all other Domains of this document.

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

P2PE Requirements for Domain 6

Requirement 6A: Use secure encryption methodologies.

Account data must be processed using cryptographic methodologies that ensure account data is kept secure.

6A-1 Key management, cryptographic algorithms and cryptographic key lengths must be consistent with international and/or regional standards.

6A-1.1 Cryptographic keys must be managed in accordance with internationally recognized key-management standards (for example, ISO 11568 (all parts) or ANSI X9.24 (all parts) or equivalent).

6A-1.2.a Account data, cryptographic keys, and components must be encrypted using only ISO or ANSI approved encryption algorithms (for example, AES, TDES) and modes of operation.

6A-1.2.b Cryptographic key changes for keys that have reached the end of their crypto-period (for example, after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, *NIST Special Publication 800-57*).

See *Appendix C: Minimum Key Sizes and Equivalent Key Strengths* for minimum required key lengths for commonly used algorithms.

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

6A-1.3 Ensure that any key-management requirements of the mode of operation used for encryption of account data are enforced.

For example, if a stream-cipher mode of operation is used, ensure that the same key stream cannot be re-used for different sets of data.

6A-1.4 Documentation describing the architecture (including all participating devices in cryptographic protocols), set-up and operation of the key-management solution must exist and must be demonstrably in use for all key-management processes).

P2PE Requirements for Domain 6

Requirement 6B: Use secure key-generation methodologies.

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

6B-1 All keys and key components are generated using an approved random or pseudo-random process to ensure the integrity and security of cryptographic systems.

6B-1.1 Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Cryptographic keys or key components must be generated by one of the following:

a) An approved key-generation function of a PCI–approved HSM.

b) An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM.

c) A process that has been certified by an independent laboratory to comply with *NIST SP800-22*.

Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values

6B-2 Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.

6B-2.1.a Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation secure cryptographic device and the device or medium receiving the key or key component.

6B-2.1.b There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.

6B-2.1.c Key-generation devices must be logged off when not in use (except when an HSM is being used to generate key components/key pairs).

6B-2.1.d Key-generation equipment must not show any signs of tampering, such as unnecessary cables.

6B-2.1.e Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area and observing the key component/key generation-process.

6B-2.2 Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret key or private key, or key component thereof, appears in unprotected memory.

For example, it is not permitted for the cryptographic key to be passed through the memory of a computer that has not been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed for key loading and are not used for any other purpose are permitted for use if all other requirements can be met. Additionally, this requirement is not intended to include in its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.

6B-2.3 Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that:

- Only approved key custodians can observe their own key.
- Tampering can be detected.

6B-2.4 Any residue which may contain clear-text keys or components must be destroyed immediately after processing that key to prevent disclosure of a key or key component.

Examples of where such key residue may exist includes (but may not be 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, for example, manually written down*
- *Recorded on any media*

6B-2.5 Procedures must ensure the following is not performed:

- Dictate keys or components over the telephone
- Record key or component values on voicemail
- Fax, e-mail, or otherwise convey clear-text keys or components
- Write key or component values into startup instructions
- Tape key or component values to or inside devices
- Write key or component values in procedure manuals

P2PE Requirements for Domain 6

6B-3	Documented procedures must exist and must be demonstrably in use for all key-generation processing.
6B-3.1	Written key-generation procedures must exist and be known by all affected parties (key custodians, supervisory staff, technical management, etc.).
6B-3.2	All key-generation events must be documented.
6B-3.3	Key-generation processes include logs for events for device master keys (HSMs and POIs). key-encrypting keys, data-encrypting keys, public/private key pairs, etc.

Keys that are generated on the POI device do not need to generate an audit-log entry, but the creation of any keys to decrypt data sent from such a POI must be logged at the solution provider.

Requirement 6C: Distribute cryptographic keys in a secure manner.

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

6C-1	Cryptographic keys must be conveyed or transmitted securely.
6C-1.1	Secret or private keys are only transmitted in one of the approved forms listed in requirement 6F-1.
6C-1.2	Specific techniques (and supporting documentation) must exist detailing how keys are transferred as specified above while maintaining their integrity and/or confidentiality.
6C-1.3	Keys used to protect the transfer of other keys or key components are managed securely according to requirement 6F-1.
6C-1.4	No single person can ever have access to more than one component of a particular cryptographic key: A person with access to one component/share of a key, or to the media conveying this component/share, must not have access to any other component/share of this key or to any other medium conveying any other component of this key.
6C-1.5.a	Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.
6C-1.5.b	Ensure that the method used does not allow for unauthorized personnel to have access to all components at any one point in time, for example, mail room and courier staff.
6C-1.6	Where key components are transmitted in clear-text using tamper-evident mailers, ensure that details of the serial number of the package are transmitted separately from the package itself.

6C-1.7	Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of a key check value and other control vectors that can be verified using a separate channel • Use of public-key certificates created by a trusted CA. • A hash of the public key sent by a separate channel (for example, mail or phone) • A new public-key certificate signed by an existing authenticated key ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.*
6C-2	A key component must be protected at all times during its transmission, conveyance, or movement between any two organizational entities.
6C-2.1	Any single clear-text key component must at all times be either: • Under the continuous supervision of a person with authorized access to this component • In one of the approved forms listed in 6F-1
6C-2.3	Packaging or mailers containing clear-text key components are examined for evidence of tampering before being used. Any sign of package tampering must result in the destruction and replacement of: • The set of components • Any keys encrypted under this (combined) key
6C-2.4	No one but the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.
6C-2.5	Mechanisms must exist to ensure that only authorized custodians: • Place key components into tamper-evident packaging for transmittal. • Open tamper-evident packaging containing key components upon receipt. • Check the serial number of the tamper-evident packing upon receipt of a component package.

P2PE Requirements for Domain 6

6C-3 All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key they transmit or convey.

6C-3.1 Cryptographic algorithms used for key transport, exchange, or establishment must use acceptable key lengths for the algorithm being used. (For the minimum key lengths please refer to *Appendix C: Minimum Key Sizes and Equivalent Key Strengths* in this document.)

6C-3.2 Verify that the key-encryption key (KEK) is at least as strong as the key(s) it is protecting, per *Appendix C: Minimum Key Sizes and Equivalent Key Strengths* in this document. For example, 168-bit ("three-key") key triple-DES keys must not be encrypted by 112-bit ("two key") triple DES keys, and AES keys must not be encrypted by triple-DES keys of any length.

6C-4 Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.

6C-4.1 Written procedures must exist and be known to all affected parties.

6C-4.2 Methods used for the conveyance or receipt of keys must be documented.

Requirement 6D: Load cryptographic keys in a secure manner.

Key loading to cryptographic devices must be handled in a secure manner, using the principles of dual control and split knowledge.

6D-1 Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.

6D-1.1 The loading of clear-text cryptographic keys, including public keys, requires dual control to authorize any key-loading session.

Dual control can be implemented using two or more passwords of five characters or more, multiple cryptographic tokens (such as smartcards), or physical keys.

6D-1.2 For loading of secret or private cryptographic keys, split knowledge is enforced by:

a) Manual entry of the key as multiple-key components, using a different custodian for each component

b) The use of a key-loading device managed under dual control

Manual key loading may involve the use of media such as paper, magnetic stripe or smart cards, or other physical tokens.

6D-1.4 For any given set of components each device shall compose the same final key from the reverse of the process used to create the components.

Secret and private cryptographic keys must be unique per POI device, but may be shared between a POI device and a decrypting HSM. It is important that any cryptographic keys loaded into the different devices are combined such that they produce the same cryptographic key.

P2PE Requirements for Domain 6

6D-1.5	If key-establishment protocols using public-key cryptography are used to distribute secret keys, these must meet the requirements detailed in Annex A of this document, or meet requirements of ANSI TR34.
6D-2	The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.
6D-2.1	Plain-text secret and private keys and key components must be transferred into a cryptographic device only when it can be ensured that: • There is no unauthorized mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. • The device has not been subject to any prior tampering that could lead to the disclosure of keys or account data.
6D-2.2	The injection of secret or private key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) results in either of the following: • The medium is placed into secure storage, managed under dual control, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device; or • All traces of the component are erased or otherwise destroyed from the electronic medium.
6D-2.3	For secret or private keys transferred from the cryptographic device that generated the key to an electronic key-loading device, the following must be in place: • 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; *and* • 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; *and* • The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs; *and* • The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.
6D-2.4	Any media (electronic, or otherwise) containing secret or private key components used in loading encryption keys must be maintained in a secure location and accessible only to authorized custodian(s).

P2PE Requirements for Domain 6

6D-2.5 When removed from secure storage, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s) and only for the minimum practical time necessary to complete the key-loading process

Key components that can be read/displayed (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are visible only at one point in time to only one designated key custodian. Component documents must not be opened until immediately prior to entry, and non-paper media must be managed so that a custodian cannot, through accident or mismanagement, expose the component beyond the key-loading facility.

6D-3 All hardware and access/authentication mechanisms used for key loading or the signing of authenticated applications (for example, for "whitelists") must be managed under dual control.

6D-3.1.a Any hardware and passwords used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control.

6D-3.1.b Dual-control practices must be specified in emergency procedures and in place during emergency situations.

6D-3.1.c Default dual-control mechanisms must be changed.

6D-3.2 All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.

6D-3.3 Any physical tokens used to enable key loading or the signing of authenticated applications (for example, physical (brass) keys, or smartcards) must not be in the control or possession of any one individual who could use those tokens to load secret cryptographic keys or sign applications under single control.

6D-3.4 Use of the equipment must be monitored and a log of all key-loading and application-signing activities maintained for audit purposes.

6D-4 The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.

6D-4.1.a A cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and components (for example, testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded).

6D-4.1.b Methods used for key validation are consistent with ISO 11568, and prevent exposure of the actual key values.

P2PE Requirements for Domain 6

6D-4.2.a Public keys must only be stored in the following approved forms:

- Within a certificate,
- Within a secure cryptographic device,
- Encrypted using strong cryptography, or
- Authenticated with strong cryptography using one of the following methods:
  - ISO16608-2004 compliant MAC
  - *NIST SP800-38B* CMAC
  - PKCS #7 compliant public-key signature

6D-4.2.b Procedures exist to ensure the integrity and authenticity of public keys prior to storage (for example, during transmission as part of a certificate request operation).

6D-5 Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.

6D-5.1 Procedures must be documented and demonstrably in use for all key-loading operations.

6D-5.2 Audit trails must be in place for all key-loading events.

Requirement 6E: Ensure secure usage of cryptographic keys.

Keys must be used in a manner that prevents or detects their unauthorized usage.

6E-1 Unique secret cryptographic keys must be in use for each identifiable link between encryption and decryption points.

6E-1.1 Where two organizations share a key to encrypt account data (including a key-encryption key used to encrypt a data-encryption key) communicated between them, that key must meet the following:

- Be unique to those two entities and
- Not be given to, or used by, any other entity.
- Where symmetric keys are used to encrypt account data, the keys must be unique per transaction-originating SCD.

(Continued on next page.)

This technique of using unique keys for communication between two organizations is often referred to as "zone encryption" and may be required. For example, keys may exist at more than one pair of locations for disaster recovery or load balancing (for example, dual processing sites). However, at all times cryptographic keys must be protected in-line with all other requirements specified in this document.

This requirement is not intended to require that any keys that are used only as part of the key-loading process but are not directly involved in key generation must be unique per device. For example, if a key-loading device first loads a "transport" key into the device before loading the device master key, the transport key is not required to be unique per device on the condition that it is erased from the device before that device leaves the key-loading facility.

Key-generation keys, such as a base derivation key used in DUKPT, which is a fixed key that is used to derive multiple keys for many different devices, must never be output from a secure cryptographic device.

6E-2 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.

6E-2.1.a The unauthorized replacement or substitution of one stored key for another or the replacement or substitution of any portion of a key, whether encrypted or unencrypted, must be prevented or detected.

6E-2.1.b Secret cryptographic keys must be managed as key bundles at all times.

6E-2.2 Documented procedures must exist and be demonstrably in use describing how the replacement and/or substitution of one key for another is prevented. These procedures must specifically include the following:

- HSMs (including CA's HSMs) must not remain in the "authorized" state when connected to online production systems.
- Keys no longer needed are destroyed, especially those keys used to encipher other keys for distribution.
- Procedures for monitoring/alerting to the presence of multiple cryptographic synchronization errors, including the following:
  - Specific actions that determine whether the legitimate value of the cryptographic key has changed, such as encryption of a known value to determine whether the resulting cryptogram matches the expected result.
  - That proactive safeguards are in place that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.
- Physical and logical controls exist over the access to and use of devices used to create cryptograms to prevent misuse

6E-2.3 Key-component documents and their packaging that show signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.

P2PE Requirements for Domain 6

6E-3	Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems.
6E-3.1	To limit the magnitude of exposure should any key(s) be compromised and to significantly strengthen the security of the underlying system, the device must enforce the following practices:
6E-3.1.a	Encryption keys must only be used for the purpose they were intended (for example, key-encryption keys must not be used as data-encryption keys, PIN keys must not be used for account-data encryption, and these keys must not be used to encrypt any arbitrary data (data that is not account data).
6E-3.1.b	Master keys (and any variants or keys derived from master keys) used by host processing systems for encipherment of keys for local storage are not used for other purposes—for example, key conveyance between platforms that are not part of the same logical configuration.
6E-3.1.c	Account data keys, key-encipherment keys, and PIN-encryption keys have different values.

Ensuring key purpose is an essential part of key management, and compromise of key purpose can render even strong cryptography invalid. Review of HSM commands used to access keys for decryption of data will often show if keys are being misused, for example where a key that is designed for account-data encryption is used to decrypt other data as well.

6E-3.2	To limit the magnitude of exposure should any key(s) be compromised and to significantly strengthen the security of the underlying system, the following practices must be enforced for private/public keys:
6E-3.2.a	Private keys must only be used as follows: • To create digital signatures ***or*** to perform decryption operations. • For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating SCDs).
6E-3.2.b	Public keys must only be used for either encryption ***or*** for verifying digital signatures, but not both (except for transaction-originating devices).
6E-3.3	Keys must never be shared or substituted between a processor's production and test systems. • Production keys must never be present or used in a test system, and • Test keys must never be present or used in a production system.
6E-4	All secret and private keys must be unique (except by chance) to that device.

P2PE Requirements for Domain 6

6E-4.1 All cryptographic keys ever present and used to encrypt account data or to protect account-data keys through encryption, in a transaction-originating POI device must be:

- Known only in that device and, and
- In one or more HSMs in the audited decryption domain of the solution provider for that device, at the minimum number of facilities consistent with effective system operations.
- Unique to each separate decryption end-point.

Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.

The requirement for unique private and secret keys includes all keys that are used to secure account data or to provide security to account-data keys. This includes not only the account-data keys themselves, but also any KEKs, master keys, or any secret and private keys used to sign firmware updates or for other device-management operations.

POI devices used for account-data decryption may be used to send encrypted data to more than one end point. Where a device is used in this way, the secret and private cryptographic keys within the device must be unique to each end point.

6E-4.2 These unique keys, or set of keys, must be totally independent and produced using a reversible process, such as that used to produce "key variants."

There are two commonly used methods of generating new keys from existing keys: key calculation and key derivation.

***Key calculation** uses a reversible process, such as the binary addition of a static value with an existing key. The result of this process is often called a "key variant" and can be trivially used to determine the value of the key from which it was derived.*

***Key derivation** is a process that is not easily reversible, and determination of the derivation key from any generated key must be at least as difficult as reversing an encryption operation performed with that key.*

6E-4.3 Emergency procedures must support requirements for unique device keys and not circumvent uniqueness controls

6E-4.4 Master keys that are generated by a derivation process and derived from the same base derivation key must be as follows:

- Use unique data for the derivation process such that all transaction-originating SCDs receive unique secret keys.
- Key derivation must be performed prior to a key being loaded/sent to the recipient transaction-originating POI.

This requirement refers to the use of a single "base" key to derive master keys for many different POI devices, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys, once loaded.

P2PE Requirements for Domain 6

Requirement 6F: Ensure secure administration of cryptographic keys.

Keys must be administered in a secure manner.

6F-1 Secret keys used for encrypting account-data encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of a secure cryptographic device, except when encrypted or managed using the principles of dual control and split knowledge.

6F-1.1 Secret or private keys must only exist in one or more of the following forms at all times—including during generation, transmission, storage, and use:

a) At least two separate key shares or full-length components.

b) Encrypted with a key of equal or greater strength. If asymmetric remote key distribution is used, mutual authentication of the sending and receiving devices shall be performed, and compliance to the asymmetric key-distribution requirements of this document are met.

c) Contained within a secure cryptographic device, approved to FIPS140-2 L3, PCI HSM, or PCI PTS.

d) Clear-text cryptographic keys can be transferred through an unprotected physical media (such as a cable, or the memory of a single-purpose key-loading computer) during key loading only, and only when such key loading is performed in a secure environment.

6F-1.2 Wherever key components are used, they have the following properties:

a) Knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key.

b) Construction of the cryptographic key requires the use of at least two key components.

c) Each key component has one or more specified custodians.

d) Procedures exist to ensure any custodian never has access to sufficient key components to reconstruct a cryptographic key.

e) Components only exist in approved forms listed in requirement 6F-1.1 (b) or (c) above or in opaque, tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging.

f) Key components must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components. For example via XOR'ing. Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two eight hexadecimal character halves to form a sixteen hexadecimal secret key. The resulting key must only exist within the SCD.

(Continued on next page)

For example, in an M of N *scheme, where only two of any three components are required to reconstruct the cryptographic key, a custodian cannot have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian cannot then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.*

In an M of N *scheme where all three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (for example, component A and component B), as a second custodian (with component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*

Tamper-evident packaging used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.

6F-1.3 If key components are stored on tokens (for example, integrated circuit cards), these tokens must be stored as follows:

6F-1.3.a In a secure manner to prevent unauthorized access of the key components (for example, by using tamper-evident envelopes) to enable the token's owner to determine whether a token was used by another person.

6F-1.3.b Key components for each specific custodian must be stored in a separate secure repository that is accessible only by the custodian or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys are not sufficient to meet this requirement.*

6F-1.3.c If a key is stored on a token, and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup(s)) must have possession of both the token and its corresponding PIN.

6F-1.4 If secret keys are encrypted using public-key cryptography for distribution to transaction originating POIs, as part of a key-establishment protocol, the requirements detailed in Annex A of this document must be met.

6F-2 Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key) and keys derived from the compromised key, to a value not feasibly related to the original key.

6F-2.1 Procedures for known or suspected compromised keys must include the following:

6F-2.1.a Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.

P2PE Requirements for Domain 6

	6F-2.1.b	If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.
	6F-2.1.c	If compromise of the cryptographic key is suspected, processing with that key is halted, and the key is replaced with a new unique key. This process includes any systems, devices, or processing that involves subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.
	6F-2.1.d	For each key in the solution provider's key suite, including any subordinate keys that are generated, protected, or transported under other keys, the purpose of that key is listed.
	6F-2.1.e	The names and/or functions of each staff member assigned to the recovery effort, as well as phone numbers and the place where the team is to assemble
	6F-2.1.f	A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: • A damage assessment • Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.
	6F-2.1.g	Identification of specific events that would indicate a compromise may have occurred. Such events may include but are not limited to: • Missing SCDs • Tamper-evident seals or package numbers or dates and times not agreeing with log entries • Tamper-evident seals or packages that have been opened without authorization or show signs of attempts to open or penetrate
	6F-2.1.h	Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.
	6F-2.1.i	If attempts to load a secret key or key component into an SCD fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original SCD.
6F-3	Keys generated using reversible key-calculation methods, such as key variants, must only be used in devices that possess the original key. Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange cannot be used as a working key or as a master file key for local storage.	

6F-3.1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner—that is, under the principles of dual control and split knowledge. Reversible transformations of a key must not be exposed outside of the secure cryptographic device that generated those transforms.

6F-3.2 Reversible key transformations are not used to generate working keys from master keys, or key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or different working keys from an initial working key.

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.

Additionally, using transforms of keys across different levels of a key hierarchy—for example, generating an account-data key from a key-encrypting key—increases the risk of exposure of each of those keys.

It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as a PIN key, MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.

Key generation that uses a non-reversible process, such as key derivation with a base key using an encipherment process, is not subject to these requirements.

6F-4 Secret keys and key components that are no longer used or have been replaced must be securely destroyed.

6F-4.1 Instances of secret or private keys, or key components, that are no longer used or that have been replaced by a new key must be destroyed.

6F-4.2 The procedures for destroying keys or key components that are no longer used or that have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered.

Keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.

Keys on other storage media types and in other permissible forms of a key instance (physically secured, enciphered, or components) must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.

In all cases, a third party—other than the custodian—must observe the destruction and sign an affidavit of destruction.

For keys on paper, consider having the affidavit of destruction as a part of the same piece of paper that contains the key component value itself. To destroy the key, tear off the section of the sheet that contains the value, destroy it, sign and witness the affidavit and log it. Affidavits of destruction can also be digitally signed if considered legally acceptable in the locale.

6F-4.3 Any residues of key-encryption keys used for the conveyance of working keys (such as components used to create the key) must be destroyed after successful loading and validation as being operational.

6F-5 Access to material which can be used to construct secret and private keys (such as key components) must be:

a) Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and

b) Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.

6F-5.1 To reduce the opportunity for key compromise, limit the number of key custodians to a minimum as follows:

- Designate a primary and a backup key custodian for each component, such that the fewest number of key custodians is necessary to enable effective key management.
- Document this designation by having each custodian and backup custodian sign a key-custodian form in some legally binding way.
- Each key-custodian form does the following:
  - Specifically authorizes the custodian
  - Identifies the custodian's responsibilities for safeguarding key components or other keying material entrusted to them
  - Specifies an effective date and time for the custodian's access
  - Is signed by management authorizing the access
- Key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual. For example, for a key managed as three components, at least two individuals report to different individuals. In an *m-of-n* scheme, such as 3 of 5 key shares, no more than two key custodians can report to the same individual. In all cases, neither the direct reports nor the direct reports in combination with their immediate supervisor shall possess a quorum of key components sufficient to form any given key.

P2PE Requirements for Domain 6

6F-6 Logs are kept for any time that keys, key components, or related materials are exposed as clear text outside of a secure cryptographic device, or removed from secure storage (such as used to store tamper-evident packaging), or loaded to an SCD.

6F-6.1 At a minimum, logs must include the following:

- Date and time in/out,
- Component identifier,
- Purpose of access,
- Name and signature of custodian accessing the component,
- Tamper-evident package number (if applicable).

Note that key components must NOT be stored in insecure locations, such as desk drawers (even if locked), and that multiple components must NOT be stored in the same physical area within a safe or lockbox such that access can be gained by one person to all necessary components to reconstruct a cryptographic key.

6F-7 Backup copies of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.

6F-7.1 The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as operational keys in line with all requirements specified in this document

6F-7.2 If backup copies are created, the following must be in place:

- Creation (including cloning) must require a minimum of two authorized individuals to enable the process.
- All requirements applicable for the original keys also apply to any backup copies of keys and their components.

It is not a requirement to have backup copies of key components or keys, but it is acceptable to maintain such backup copies for the purposes of business continuity if they are secured and maintained in approved forms.

6F-7.3 If backup copies of secret and/or private keys exist, confirm that they are maintained in one of the approved forms noted in Requirement 6F-1.1 and are managed under dual control and split knowledge.

P2PE Requirements for Domain 6

6F-8	Documented procedures must exist and must be demonstrably in use for all key administration operations.

6F-8.1	Written procedures must exist as follows:
	• All affected parties must be aware of those procedures.
	• All aspects of and activities related to key administration must be documented, including:
	  ○ A defined cryptographic-key change policy for each key layer defined in the key hierarchy (this applies to both symmetric and asymmetric key types)
	  ○ Security-awareness training
	  ○ Role definition—nominated individual with overall responsibility
	  ○ Background checks for personnel
	  ○ Management of personnel changes, including revocation of access control and other privileges when personnel move

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

This annex contains detailed requirements that apply to remote key establishment and distribution applications and are in addition to key and equipment-management criteria stated in the main body of this document. Remote key-distribution schemes should be used for initial key loading only—for example the establishment of a TDES or AES key hierarchy, such as a terminal master key. Standard symmetric key-exchange mechanisms should be used for subsequent symmetric key exchanges, except where a device requires a new key initialization due to unforeseen loss of the existing terminal master key.

Certification Authority requirements apply to all entities (acquirers, manufacturers, key-distribution hosts (KDH), and other third parties) signing public keys to be used for remote distribution of cryptographic keys, whether in X.509 certificate-based schemes or other designs, to allow for the required authentication of these signed public keys. For purposes of these requirements, a certificate is any digitally signed value containing a public key, where the term "digitally signed" refers to any cryptographic method used to enforce the integrity and authenticity of a block of data through the encryption of a whole or digest of that block of data with a private key. The CA requirements only apply to methods that allow for the distribution and use of such signed keys to multiple systems, and as such do not apply to systems that apply symmetric cryptography to keys for authentication (such as through the use of MACs or CMACs).

The Certificate 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.

Requirements for Remote Key Establishment and Distribution – Logical Security

	Compromise must not be possible without collusion.
RD-1	Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals (Reference 6B-2)
RD-1.1	Asymmetric key pairs must either be generated by the device that will use the key pair or, if generated externally, the key pair and all related critical security parameters (for example, secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair occurs.
	Cryptographic keys must be conveyed or transmitted securely.
RD-2	Cryptographic keys must be conveyed or transmitted securely. (Reference 6C-1)
RD-2.1	Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used (refer to Appendix C for guidance).

Requirements for Remote Key Establishment and Distribution – Logical Security

	Authenticity of keys must be validated.
RD-3	The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised. (Reference 6D)
RD-3.1.a	SCDs and key-distribution hosts (KDHs) involved in using public-key schemes must check the validity of other such devices involved in the communication prior to any key transport, exchange, or establishment. Validation of authentication credentials must occur immediately prior to any key establishment. (Examples of this kind of validation include checking current certificate revocation lists or embedding valid authorized KDH certificates in devices and disallowing communication with unauthorized KDHs.)
RD-3.1.b	Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange or key establishment with transaction originating POIs. An example of this kind of mechanism is through limiting communication between the transaction-originating POI and KDH to only those KDHs contained in a list of valid KDHs managed by the transaction originating POI.
RD-3.1.c	Within an implementation design, there shall be no means available for "man in middle" attacks. System implementations must be designed and implemented to prevent replay attacks.
RD-3.1.d	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.
RD-3.1.e	Once asymmetric keys are loaded for a specific service provider, changing of those keys must not be possible without the authorization of that service provider.
	Procedures must prevent or detect unauthorized key substitution.
RD-4	Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. (Reference 6E-2)
RD-4.1.a	Encryption devices shall only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate issuing authority generates the key pair on behalf of the SCD); and with KDHs for key management, normal transaction processing, and certificate (entity) status checking.
RD-4.1.b	KDHs shall only communicate with transaction-originating SCDs for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.

Requirements for Remote Key Establishment and Distribution – Logical Security

Keys must be used only for their intended purpose and may never be shared between systems.

RD-5 Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems. (Reference 6E-3)

RD-5.1.a Only one certificate shall be issued per key pair. Certificates for a key pair shall not be renewed using the same keys.

RD-5.1.b Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose (for example. keys are 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.)

- CA certificate/certificate (entity) status checking (for example, using Certificate Revocation Lists), signature keys, or signature keys for updating valid/authorized host lists in encryption devices cannot be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates. 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. CAs that issue certificates to other CAs cannot be used to issue certificates to encryption devices.
- Public keys are only used for either encryption or for verifying digital signatures, but not both (except for EPPs/PEDs).
- Private keys can only be used for decryption or for creating digital signatures, but not both (except for EPPs/PEDs).

RD-5.1.c Public-key-based implementations must provide mechanisms for restricting and controlling the use of public and private keys. For example, this can be accomplished through the use of X.509 compliant certificate extensions.

RD-5.1.d CA and KDH private keys cannot be shared between devices except for load balancing and disaster recovery. EPP and POS PED private keys cannot be shared.

All secret keys must be unique to their devices.

RD-6 All secret keys must be unique (except by chance) to that device. (Reference 6C-4)

RD-6.1 Private keys must be uniquely identifiable in all hosts and encryption devices. Keys must be identifiable via cryptographically verifiable means (for example, through the use of digital signatures, “fingerprints,” or key check values).

Keys Known or suspected to be compromised must be replaced.

RD-7 Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) to a value not feasibly related to the original key. (Reference 6F-2)

RD-7.1.a To provide for continuity of service in the event of the loss of a root key (for example, through compromise or expiration), a key-distribution management system and the associated end entities (KDHs, encryption devices) should provide support for more than one root (although this is not a requirement).

Requirements for Remote Key Establishment and Distribution – Logical Security

RD-7.1.b	Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.
RD-7.1.c	Mechanisms must be in place to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke subordinate certificates and notify affected entities.
RD-7.1.d	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. In the event of the issuance of phony certificates with the compromised key, the CA should determine whether to recall and reissue all signed certificates with a newly generated signing key. Mechanisms (for example, time stamping) must exist to ensure that fake certificates cannot be successfully used.
RD-7.1.e	The compromised CA must notify any superior or subordinate CAs of the compromise. Subordinate CAs and KDHs should have their certificates reissued and distributed to them or be notified to apply for new certificates.
	Access to key-construct material must be limited and protected.
RD-8	Access to material that can be used to construct secret and private keys (such as key components) must be: 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. (Reference 6F-5)
RD-8.1.a	All user access shall be directly attributable to an individual user, for example through the use of unique IDs, and be restricted to actions authorized for that role through the use of a combination of CA software, operating-system, and procedural controls.

Requirements for Remote Key Establishment and Distribution – Logical Security

RD-8.1.b The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include that:

- The network is used only for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access shall exist only for the purposes of "pushing" certificate status information to relying parties (for example, KDHs, encryption devices).
- No CA or Registration Authority (RA) software updates are done over the network (local console access must be used for CA or RA software updates).
- Non-console access requires two-factor authentication. This also applies to the use of remote console access.
- Remote user access to the CA or RA system environments shall be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.
- CA certificate (for SCD/KDH authentication and validity status checking) signing keys must be enabled under multilevel controls.
- Certificate requests may be vetted (approved) using single user logical access to the RA application.

RD-8.1.c The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as "split knowledge and dual control." At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).

RD-8.1.d For systems accessible via non-local console access, the operating system(s) utilized must be hardened. Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, etc., commands in Unix) must be removed or disabled. Unnecessary ports must also be disabled. Documentation must exist to support the enablement of all active services and ports.

RD-8.1.e Vendor-default IDs that are required only as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason. Vendor-default IDs such as "Guest" must be removed or disabled. Default passwords must be changed during initial installation.

RD-8.2.a Audit trails must include, but not be limited to all key-management operations, such as key generation, backup, recovery, compromise, and destruction and certificate generation or revocation, together with the identity of the person authorizing the operation and persons handling any key material (such as key components or keys stored in portable devices or media). The logs must be protected from alteration and destruction, and archived in accordance with all regulatory and legal requirements.

RD-8.2.b Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.

Requirements for Remote Key Establishment and Distribution – Logical Security

RD-8.2.c Logical events are divided into operating-system and CA application events. For both events the following will be recorded in the form of an audit record:

- Date and time of the event,
- Identity of the entity and/or user that caused the event,
- Type of event, and
- Success or failure of the event.

RD-8.2.d CA application logs must deploy a mechanism to prevent and detect attempted tampering of application logs.

RD-8.3.a The on-line certificate-processing system components must be protected by a firewall(s) and intrusion-detection systems from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to:

- Deny all services not explicitly permitted.
- Disable or remove all unnecessary services, protocols, and ports.
- Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure.
- Disable source routing on the firewall and external router.
- Not accept traffic on its external interfaces that appears to be coming from internal network addresses.
- Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken.
- Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc. must be deleted or disabled.

RD-8.3.b Online systems must employ individually or in combination network and host-based intrusion detection systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments, must be covered.

RD-8.4 The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as “dual control.” At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).

RD-8.5 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

RD-8.6 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system-hardening standards.

Requirements for Remote Key Establishment and Distribution – Logical Security

RD-8.7	Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
RD-8.8	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
RD-8.9	Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
RD-8.10	Do not use group, shared, or generic accounts and passwords, or other authentication methods.
RD-8.11	Change user passwords at least every 30 days.
RD-8.12	Require a minimum password length of at least eight characters.
RD-8.13	Use passwords containing numeric, alphabetic, and special characters.
RD-8.14	Limit repeated access attempts by locking out the user ID after not more than five attempts.
RD-8.15	Pass phrases are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.
RD-8.16	The embedding of pass phrases in shell scripts, command files, communication scripts, etc., is strictly prohibited.
RD-8.17	Log-on security tokens (for example, smart cards) and encryption devices are not subject to the pass-phrase management requirements for maximum and minimum timelines as stated above. Security tokens must have associated PINs/pass phrases to enable their usage. The PINs/pass phrases must provide a security equivalent to or greater than eight decimal digits (that is, there must be at least 100,000,000 possible PINs/passphrases, of which all are equally likely to be used.
RD-8.18	Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations, including any physical access to the CA environment. If the process is manual, ensure that it occurs at least quarterly.

Requirements for Remote Key Establishment and Distribution – Logical Security

Procedures must be in place for all key-administration operations.

RD-9	Documented procedures must exist and must be demonstrably in use for all key-administration operations (Reference 6F-8)	
	RD-9.1.a	CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.
	RD-9.1.b	The certificate issuing and management authority may consist of one or more devices that are used for the issuance, revocation, and overall management of certificates and certificate status information.
	RD-9.1.c	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). This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific single document or a collection of specific documents. The CPS must be consistent with the requirements described within this document. The CA shall operate in accordance with its CPS.
	RD-9.1.d	Documented procedures exist and are demonstrably in use by CAs to validate the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.
	RD-9.1.e	For CA and KDH certificate-signing requests, including certificate or key-validity status changes (for example, revocation. suspension, replacement), verification must include validation that: • The entity submitting the request is who it claims to be. • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. • The entity submitting the request has a valid business relationship with the issuing authority (for example, the vendor) consistent with the certificate being requested. • The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner. • 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

Physical Security Requirements for CAs and RAs

Certificate and Registration Authorities must implement physical security to reduce the risk of compromise of their systems. Physical security must be implemented to provide three tiers of physical security, as indicated below.

Level One Barrier

This level consists of the entrance to the facility. The building or secure facility entrance will only allow the entrance of authorized personnel to the facility. A guarded entrance or foyer with a receptionist requires the use of a logbook to register authorized visitors (guests) to the facility.

Level Two Barrier

This level secures the entrance beyond the foyer/reception area to the CA facility. This entrance must be monitored by a video-recording system and require secure entry of authorized personnel only. All entry through this barrier must be logged. Single entry into this barrier is allowed. Authorized visitors must be escorted at all times when within this barrier and beyond.

Level Three Barrier

This level provides access to the dedicated room housing the CA and signing engines. This entrance requires dual access. Personnel with access must be divided into an "A" group and a "B" group, such that access requires at least one member from each group. The A and B groups should correlate to separate organizational units.

Doors must have locks, and all authorized personnel having access through this barrier must have successfully completed a background security check and are assigned resources (staff, dedicated personnel) of the CA operator. Other personnel that require entry to this level must be accompanied by two (2) authorized and assigned resources at all times.

Additionally, certificate-processing operations must meet the following requirements.

Requirements for Remote Key Establishment and Distribution – Physical Security

	The certificate-processing operations center must implement a physical security boundary.
RD-10.1	The certificate-processing operations center must implement a three-tier physical security boundary, as noted above.
RD-10.2	The Level 3 environment must consist of a physically secure dedicated room not used for any other business activities but certificate operations (stand-alone).
RD-10.3	The Level 3 environment must have true floor to ceiling (slab to slab) walls, or use solid materials (such as steel mesh or bars) below floors and above ceilings to protect against intrusions. For example, the Level 3 environment may be implemented within a 'caged' environment.
RD-10.4	CA and RA systems must provide for the documentation of all access granting, revocation, and review procedures and of specific access authorizations, whether logical or physical.

Requirements for Remote Key Establishment and Distribution – Physical Security

RD-10.5.a	Access to CA and RA systems requires dual control. The room hosting the certificate-signing equipment (Level 3 environment) must never be occupied by a single individual for more than thirty (30) seconds.
RD-10.5.b	The enforcement mechanism must be automated. The system must enforce anti-pass-back. Dual occupancy requirements are managed using electronic (for example, badge and/or biometric) systems.
RD-10.6	Access to CA and RA systems is permitted only to pre-designated staff with defined business needs and duties. Visitors must be authorized and escorted at all times within the Level 2 and Level 3 environments.
RD-10.7	The Level 2 entrance and Level 3 environment must be monitored by CCTV system, recording to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds (motion-activated systems that are separate from the intrusion-detection system may be used). Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, etc.
RD-10.8	Personnel with access to the Level 3 environment must not have access to the media (for example, VCR tapes, digital-recording systems, etc.) with the recorded surveillance data. Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. Systems using digital-recording mechanisms must have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.
RD-10.9	Continuous, or motion activated, appropriate lighting for any cameras is provided.
RD-10.10.a	Permanent (24/7) intrusion-detection systems are implemented for the Level 3 environment, which protect the secure area by motion detectors when unoccupied. Any windows in the secure area must be locked, protected by alarmed sensors, or otherwise similarly secured.
RD-10.10.b	These intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have exited the secure area.
RD-10.11	Access logs record all personnel entering the Level 2 and Level 3 environments. The logs may be electronic, manual, or both. Visitors must sign an access log detailing name, organization, date and time in and out, and purpose of visit. The person escorting the visitor must also initial the log.
RD-10.12	Access logs for the Level 3 environment include documented reasons for the access.
RD-10.13	All access-control and monitoring systems are powered through an uninterruptible power source (UPS).
RD-10.14	Document all alarm events. Under no circumstances shall an individual sign off on an alarm event in which they were involved.
RD-10.15	The use of any emergency entry or exit mechanism must cause an alarm event.
RD-10.16	All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.

Requirements for Remote Key Establishment and Distribution – Physical Security

RD-10.17	A process is implemented for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs. This may be done by either automated or manual mechanisms. If a manual process is utilized, synchronization must occur at least quarterly. Documentation of the synchronization must be retained for at least a one-year period.

Cryptographic Key Operations – Annex B: Key-Injection Facilities

The term key-injection facility (KIF) describes those entities that perform key injection of POI devices. Key injection may be performed by the solution provider or by a third party such as a POI terminal manufacturer or vendor. This annex contains the specific requirements that apply to key-injection facilities, and are in addition to those set out in all other Domains of this document.

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

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

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

Requirements for Key-Injection Facilities

Account data must be in equipment resistant to compromise.

KF-1 Account data must be encrypted in equipment that is resistant to physical and logical compromise (Reference 1A-1)

KF-1.1 Key-injection facilities must only inject keys into PCI-approved POI devices that are managed in accordance with Domain 1 of this document.

KF-1.2 Key-injection platforms and systems that include hardware devices for managing (for example, generating and storing) cryptographic keys must ensure those hardware devices are certified and configured to FIPS140-2 Level 3 or higher, or are a PCI-approved HSM. These devices must be managed in accordance with Domain 5 of this document.

Keys must be entered using dual control and split knowledge.

KF-2 Unencrypted secret or private keys must be entered into encryption devices using the principles of dual control and split knowledge. (Reference 6D-1)

KF-2.1 Key-injection facilities must implement dual control and split knowledge controls for the loading of keys into equipment. Such controls can include (but are not limited to):

a) 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.

b) 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.

c) 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.

d) Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry.

Requirements for Key-Injection Facilities

Procedures must prevent or detect unauthorized substitution.

KF3 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. (Reference 6E-2)

KF-3.1 Key-injection facilities must implement controls to protect against unauthorized substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to:

a) All key loading must be performed using dual control and split knowledge. Controls must be in place to prevent and detect the loading of keys by any one single person. 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.

b) All devices loaded with keys must be tracked at each key-loading session by serial number.

c) Key-injection facilities must use something unique about the transaction-originating secure cryptographic device (for example, serial number) when deriving the key (for example, DUKPT, TMK) injected into it.

All keys must be unique to their devices.

KF-4 All secret and private keys must be unique (except by chance) to that device. (Reference 6E-4)

KF-4.1.a Key-injection facilities must ensure that keys established on a device are unique, except by chance. The same key(s) must not be loaded into multiple devices.

KF-4.1.b Key-injection facilities that load DUKPT keys must use separate BDKs for different entities.

KF-4.1.c Key-injection facilities that load DUKPT keys for various terminal 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.

Physical protection of Key-Injection Facilities.

Physical security requirements for Key-Injection Facilities will be included in the next release of this document, when the testing procedures are also added, before the end of 2011. These requirements will be aligned with those detailed in the PCI PIN Security Requirements – Version 1.0 (see Requirement 31, Normative Annex: Key-Injection Facilities), which were released in September 2011.

Appendix A: PCI DSS Validation for P2PE Merchants

This appendix outlines the proposed validation that P2PE merchants with validated hardware/hardware P2PE solutions may be eligible to complete.

PCI DSS validation requirements are determined by the individual payment card brands. The information in this appendix is provided for illustrative purposes only and should not be used for PCI DSS validation. Entities should consult with their acquirer (merchant bank), and/or the individual payment brands directly to verify their PCI DSS compliance validation requirements.

PCI DSS Scoping and Assessment Considerations

Considerations for PCI DSS scoping and assessment requirements for merchants using a validated P2PE solution include the following:

- Is all account data within the P2PE environment accepted using a secure POI device that is listed on the PCI PTS Approval List, and does this listing show that it provides SRED functionality?
- Have all other payment channels within the merchant environment been adequately segmented (isolated) from the P2PE environment?
- Is the POI provided by an external solution provider—such as a payment gateway, processor, or acquirer—that manages all applicable POI functions, including management and loading of the cryptographic keys, installation, and any on-going maintenance?
- Is the P2PE solution listed by PCI SSC as an approved P2PE solution?
- Is there other account data not protected by the P2PE solution?

  Note that the P2PE solution and any resulting PCI DSS scope reduction is only applicable to account data that is protected by the P2PE solution; PCI DSS is applicable to any other channels or sources of clear-text account data.

Reduced PCI DSS Validation

Reduced PCI DSS validation for P2PE merchants is expected to consist of the following:

- Merchant completion of self-assessment or onsite assessment by a QSA
- Assessment-validation reporting according to payment brand compliance program—for example, completion of Self-Assessment Questionnaire (SAQ), Report on Compliance (ROC), and/or Attestation of Compliance (AOC).
- Merchant attestation of Eligibility to Complete Reduced PCI DSS Validation for P2PE Merchants using Hardware/Hardware P2PE Solutions
- Merchant attestation of adherence to P2PE Instruction Manual
- Merchant attestation of compliance to applicable PCI DSS requirements
- Merchant attestation of accuracy of PCI DSS compliance validation, including:
  - PCI DSS validation and attestation of compliance was completed according to applicable instructions.
  - All information in the attestation fairly represents the results of the PCI DSS assessment in all material respects.
  - No evidence of magnetic-stripe (track) data, CAV2, CVC2, CID, or CVV2 data, or PIN or PIN-block data storage after transaction authorization was found on ANY systems reviewed during the assessment.

Proposed Merchant Attestation of Eligibility to Complete Reduced PCI DSS Validation

Eligibility to Complete Reduced PCI DSS Validation for P2PE Merchants using Hardware/Hardware P2PE Solutions	
Merchant certifies eligibility for reduced PCI DSS validation and attests to all of the following:	
☐	All payment processing is via a validated P2PE solution listed by the PCI Security Standards Council ▪ Identify the solution: ▪ Identify the PCI-approved POI devices in use:
☐	If merchant receives or transmits account data electronically through other channels, those channels are adequately segmented (isolated) from the P2PE environment.
☐	Merchant does not store account data in electronic format after authorization, even if encrypted.
☐	Merchant retains only paper reports or paper copies of receipts, and such data is not received electronically.
☐	Merchant verifies there is no legacy storage of CHD in the environment,
☐	Merchant does not run any applications on the POI device (other than those approved for use with the validated P2PE solution).

Proposed Merchant Attestation of Adherence to P2PE Instruction Manual

Merchant Attestation: Adherence to P2PE Instruction Manual provided as part of validated P2PE solution.	YES	NO	P2PE Reference
Merchant has implemented the following in accordance with the instructions documented in the P2PE Instruction Manual:			
▪ A device-tracking system is in place for all encryption devices.	☐	☐	3A-1.1
▪ Device inventories to detect removal / substitution of devices are performed.	☐	☐	3A-1.2
▪ An inventory of all devices is maintained and secured.	☐	☐	3A-1.3
▪ Procedures are implemented for responding to missing or substituted devices.	☐	☐	3A-1.4
▪ Devices not in use are stored in a physically secure location.	☐	☐	3A-2.1 – 3A-2.3
▪ Devices in transit are secured.	☐	☐	3A-2.4
▪ Devices are only transported between trusted locations.	☐	☐	3A-2.5
▪ Procedures to prevent and detect unauthorized modification, substitution or tampering of devices prior to deployment are implemented.	☐	☐	3A-3.1
▪ Procedures are implemented to control and document all access to devices prior to deployment.	☐	☐	3A-3.2
▪ A documented audit trail is implemented to ensure that all devices are controlled from receipt through to installation.	☐	☐	3A-3.3
▪ Devices are deployed in appropriate locations and are physically secured to prevent unauthorized removal or substitution.	☐	☐	3A-4.1 – 3A-4.2
▪ Where devices cannot be physically secured—for example, wireless, handheld, line-busters etc.—procedures are implemented to prevent unauthorized removal or substitution of devices.	☐	☐	3A-4.3
▪ Procedures are implemented for identification and authorization of repair /maintenance personnel and other third parties prior to granting access.	☐	☐	3A-5.1
▪ Procedures are implemented for securing devices being returned or replaced.	☐	☐	3B-1.1
▪ Procedures are implemented for secure disposal of devices.	☐	☐	3B-1.2
▪ Periodic physical inspections of devices are performed to detect tampering or modification.	☐	☐	3B-7.1
▪ If applicable, mechanisms are in place to detect tampering of devices deployed in remote or unattended locations and alert appropriate personnel.	☐	☐	3B-7.2
▪ If applicable, procedures are implemented for responding to detection of tampered devices.	☐	☐	3B-7.3

Proposed Merchant Validation of Compliance to Applicable PCI DSS Requirements

Eligible merchants using PCI SSC-validated P2PE solutions will be able to validate to a reduced set of PCI DSS requirements. The particular PCI DSS requirements that will apply to eligible merchants will be included with the release of the P2PE validation program in 2012.

It is expected that PCI DSS controls that will be applicable to a merchant's validation will include (but may not be limited to):

- Protection of media and devices
- Maintaining information security policies and training for personnel
- Processes for management of third-party providers (including P2PE provider)
- Incident response and escalation procedures

Appendix B: Glossary

Term	Definition
Access Controls	Ensuring that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
Account Data	At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code. ***Note:*** *Truncated, masked, and hashed PAN data (with salt) is not considered account data. Encrypted data that satisfies the requirements stated in this guidance document is not considered to be account data.*
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
ANSI	American National Standards Institute. A U.S. standards accreditation organization.
Asymmetric cryptography (techniques)	See *Public key cryptography*.
ATM	An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks.
Authentication	The process for establishing unambiguously the identity of an entity, organization, or person at a specific point in time.
Authorization	The right granted to a user to access an object, resource, or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource, or function.
Base (master) derivation key (BDK)	See *Derivation key*.
Cardholder	An individual to whom a card is issued or who is authorized to use the card.
Cardholder data (CHD)	At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: ▪ Cardholder name ▪ Expiration date ▪ Service Code See *Sensitive authentication data (SAD)* for additional data elements that may be transmitted or processed as part of a payment transaction.
Certificate	The public key and identity of an entity, together with other information, rendered unforgeable by signing the certificate with the private key of the certifying authority that issued that certificate.
Certificate revocation	The process of revoking an otherwise valid certificate by the entity that issued that certificate. Revoked certificates are placed on a Certificate Revocation List (CRL) or the information is conveyed using Online Certificate Status Protocol (OCSP) as specified in the product/service specification.

Term	Definition
Certificate Revocation List (CRL)	A list of revoked certificates. For example, entities that generate, maintain and distribute CRLs can include the Root or subordinate CAs.
Check value	A computed value that is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible.
Cipher text	Data in its encrypted form.
Clear text	See *Plain text.*
Compromise	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plain-text cryptographic keys and other keying material).
Computationally infeasible	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it.
Credentials	Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key.
Critical Security Parameters (CSP)	Security-related information (for example, cryptographic keys, authentication data such as passwords and PINs) appearing in plain text or otherwise unprotected form and whose disclosure or modification can compromise the security of a SCD or the security of the information protected by the device.
Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic key	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of plain-text data into cipher-text data, ▪ The transformation of cipher-text data into plain-text data, ▪ A digital signature computed from data, ▪ The verification of a digital signature computed from data, ▪ An authentication code computed from data, or ▪ An exchange agreement of a shared secret.
Cryptographic key component	A parameter used in conjunction with other key components in an approved security function to form a plain-text cryptographic key or perform a cryptographic function.
Data Encryption Algorithm (DEA)	A published encryption algorithm used to protect critical information by encrypting data based upon a variable secret key. The Data Encryption Algorithm is defined in *ANSI X3.92: Data Encryption Algorithm* for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.

Term	Definition
Data-encryption (encipherment or exchange) key (DEK)	A cryptographic key that is used for the encryption or decryption of account data.
Decipher	See *Decrypt*.
Decrypt	A process of transforming cipher text (unreadable) into plain text (readable).
Derivation key	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the DUKPT key-management method. Derivation keys are normally used in a transaction-receiving (for example, acquirer) SCD in a one-to-many relationship to derive or decrypt the transaction keys (the derived keys) used by a large number of originating SCDs (for example, POIs).
DES	Data Encryption Standard (see Data Encryption Algorithm). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. Government *as Federal Information Processing Standard (FIPS) Publication 46,* which allows only hardware implementations of the data encryption algorithm.
Digital signature	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.
Double-length key	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDES cryptographic algorithm.
Dual control	A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (for example, cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see *Split knowledge.*
DUKPT	Derived Unique Key Per Transaction: a key-management method that uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction-originating POI. The unique transaction keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.
EEPROM	Electronically erasable programmable read-only memory.
Electronic key entry	The entry of cryptographic keys into a SCD in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.
Encipher	See *Encrypt*.
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.

Term	Definition
Encrypting PIN pad (EPP)	A device for secure PIN entry and encryption in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (for example, an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell.
EPROM	Erasable programmable read-only memory.
Exclusive-OR	Binary addition without carry, also known as "modulo 2 addition," symbolized as "XOR," and defined as: ▪ 0 + 0 = 0 ▪ 0 + 1 = 1 ▪ 1 + 0 = 1 ▪ 1 + 1 = 0
Fail closed	A state where the PCI-approved POI device discontinues operations for PCI-branded payment accounts/cards,
FIPS	Federal Information Processing Standard.
Firmware	The programs and data (i.e., software) permanently stored in hardware (for example, in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.
Host/Hardware security module (HSM)	A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key management functions and/or the decryption of account data. For P2PE, these devices must be 1) approved and configured to FIPS140-2 (level 3 or higher), or 2) approved to the PCI HSM standard. See also *Secure cryptographic device.*
Hash function	A (mathematical) function that takes any arbitrary length message as input and produces a fixed-length output. It must have the property that it is computationally infeasible to discover two different messages that produce the same hash result. It may be used to reduce a potentially long message into a "hash value" or "message digest" that is sufficiently compact to be input into a digital-signature algorithm.
Initialization vector	A binary vector used as the input to initialize the algorithm for the encryption of a plain-text block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Interface	A logical section of a SCD that defines a set of entry or exit points that provide access to the device, including information flow or physical access.
Irreversible transformation	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.

Term	Definition
ISO	International Organization for Standardization. An international standards accreditation organization.
Issuer	The institution holding the account identified by the primary account number (PAN).
Key	See *Cryptographic key.*
Key agreement	A key-establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
Key backup	Storage of a protected copy of a key during its operational use.
Key component	See *Cryptographic Key Component.*
Key-derivation process	A process that derives one or more session keys from a shared secret and (possibly) other public information.
Key destruction	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.
Key distribution host (KDH)	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to POIs and the financial processing platform communicating with those POIs. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys.
Key-encrypting (encipherment or exchange) key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys.
Key establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generation	Creation of a new key for subsequent use.
Key instance	The occurrence of a key in one of its permissible forms, i.e., plain-text key, key components, encrypted key.
Key loading	Process by which a key is manually or electronically transferred into a SCD.
Key-loading device	A self-contained unit that is capable of storing at least one plain-text or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
Key management	The activities involving the handling of cryptographic keys and other related security parameters (for example, initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving.
Key pair	A key pair comprises the two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is only known to the appropriate entities.

Term	Definition
Key replacement	Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.
Key (secret) share	Related to a cryptographic key generated such that a specified fraction of the total shares of such parameters can be combined to form the cryptographic key but such that less than a specified fraction does not provide any information about the key.
Key storage	Holding of the key in one of the permissible forms.
Key transport	A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
Key usage	Employment of a key for the cryptographic purpose for which it was intended.
Key variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Keying material	The data (for example, keys and initialization vectors) necessary to establish and maintain cryptographic-keying relationships.
Manual key loading	The entry of cryptographic keys into a SCD from a printed form, using devices such as buttons, thumb wheels, or a keyboard.
Master derivation key (MDK)	See *Derivation key.*
Master key	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a master key.
Message	A communication containing one or more transactions or related information.
Node	Any point in a network that does some form of processing of data, such as a terminal, acquirer, or switch.
Non-PCI-branded payment accounts/cards	Payment accounts/cards which are not PCI-branded payment accounts/cards. Examples of non-PCI-branded payment accounts/cards may include certain loyalty cards or non-PCI branded store cards. See *PCI-branded payment accounts/cards*.
Non-reversible transformation	See *Irreversible Transformation.*
OCSP	See *Online Certificate Status Protocol.*
Online Certificate Status Protocol	The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
Out-of-band notification	Notification using a communication means independent of the primary communications means.
PAN	Primary account number. See also *Cardholder data.*

Term	Definition
Password	A string of characters used to authenticate an identity or to verify access authorization.
Physical protection	The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.
PCI-approved POI device	Point of interaction (POI) device evaluated and approved via the PCI PTS program, with SRED (secure reading and exchange of data) listed as a "function provided," and with the SRED capabilities enabled and active.
PCI-branded payment accounts/cards	Payment accounts/cards that are associated with one of the five founding payment card brands of the Payment Card Industry (PCI). These accounts/cards are either issued by, or on behalf of, one of the founding payment card brands. The founding payment card brands are: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
PIN entry device (PED)	A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor, and storage for PIN processing sufficiently secure for the key-management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell.
Plain text	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as clear text.
Plain-text key	An unencrypted cryptographic key, which is used in its current form.
Point of Interaction (POI)	The initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions." See also *Secure cryptographic device.*
P2PE solution provider	The P2PE solution provider is a third-party entity (for example, a processor, acquirer, or payment gateway). The solution provider designs and implements, and may also manage a P2PE solution for merchants, The solution provider may manage and perform all solution provider responsibilities or may outsource certain responsibilities. The solution provider has the overall responsibility for the design of an effective P2PE solution appropriate for a specific P2PE implementation.
Private key	A cryptographic key, used with a public-key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encryption system, the private key defines the decryption transformation.
PROM	Programmable read-only memory.
Pseudo-random	A value that is statistically random and essentially random and unpredictable although generated by an algorithm.

Term	Definition
Public key	A cryptographic key, used with a public-key cryptographic algorithm, uniquely associated with an entity, and that may be made public In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encryption system, the public key defines the encryption transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to all members of a pre-specified group.
Public key (asymmetric) cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can be any of the following: – An encryption system, a signature system, – A combined encryption and signature system, or – A key agreement system. With asymmetric cryptographic techniques, there are four elementary transformations: sign and verify for signature systems, and encrypt and decrypt for encryption systems. The signature and the decryption transformation are kept private by the owning entity, whereas the corresponding verification and encryption transformations are published. There exist asymmetric cryptosystems (for example, RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation, and where used, the four elementary transformations and the corresponding keys should be kept separate.
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware based "noise" mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
ROM	Read-only memory.
Root Certification Authority (RCA)	The RCA is the top level Certification Authority in a public-key infrastructure. An RCA is a CA that signs it own public key with the associated private key. RCAs only issue certificates to subordinate CAs. Root CAs do not issue certificates directly to KDHs, EPPs or PEDs. RCAs may also issue certificate status lists for certificates within their hierarchy.
Secret key	A cryptographic key, used with a secret-key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.

Term	Definition
Secure cryptographic device (SCD)	A device used either for the acceptance and encryption of account data at the point of sale, or for cryptographic key management functions and/or the decryption of account data. SCDs used for acceptance or encryption of account data at the point of sale are also referred to at *POIs* or *PCI-approved POI devices*. SCDs used for cryptographic key management functions and/or the decryption of account data are also referred to as *HSMs* (host/hardware security modules). See also *Point of Interaction, PCI-approved POI device,* or *Host/hardware security module.*
Secure environment	An environment that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or purpose-built room with continuous access control, physical security protection, and monitoring.
Sensitive authentication data (SAD)	Security-related information (card-validation codes/values, full-track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain text or otherwise unprotected form.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration, or destruction—especially cardholder data, sensitive authentication data, and cryptographic keys—and includes design characteristics, status information, and so forth.
Session key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, for example, an encryption key and a MAC key.
Shared secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key-derivation function to derive session keys.
Single-length key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
Software	The programs and associated data that can be dynamically written and modified.
Solution provider	See *P2PE solution provider.*
Split knowledge	A condition under which two or more entities separately have key components, which individually convey no knowledge of the resultant cryptographic key.
Subordinate CA and Superior CA	If one CA issues a certificate for another CA, the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, SCDs. Subordinate CAs may also issue certificates to lower-level CAs and issue certificate status lists regarding certificates the subordinate CA has issued.
Symmetric key	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.

Term	Definition
System software	The special software (for example, operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.
Tamper-evident	A characteristic that provides evidence that an attack has been attempted.
Tamper-resistant	A characteristic that provides passive physical protection against an attack.
Tamper-responsive	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
Tampering	The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data.
TDEA	See *Triple Data Encryption Algorithm.*
Terminal	A device/system that initiates a transaction.
Transaction	A series of messages to perform a predefined function.
Triple Data Encryption Algorithm (TDEA)	The algorithm specified in *ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.*
Triple Data Encryption Standard (TDES)	See *Triple Data Encryption Algorithm.*
Triple-length key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.
Trustworthy system	Computer hardware and software which: ▪ Are reasonably secure from intrusion and misuse; ▪ Provide a reasonable level of availability, reliability, and correct operation; and ▪ Are reasonably suited to performing their intended functions.
Unattended acceptance terminal (UAT)	See *Unattended payment terminal.*
Unattended payment terminal (UPT)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment, including, but not limited to, the following: ▪ ATM ▪ Automated fuel dispenser ▪ Ticketing machine ▪ Vending machine
Unprotected memory	Components, devices, and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a SCD.
Variant of a key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Verification	The process of associating and/or checking a unique characteristic.

Term	Definition
Whitelist	A list used by a POI function or application to make processing decisions. For example, a whitelist could be a list and/or range of non-PCI-branded payment account/card numbers, approved by the solution provider, which are not required to be encrypted at the POI, or it could be used to make routing decisions that pertain to only a subset of accounts/cards processed. Unless explicitly authorized by the relevant payment brand, PCI-branded payment brand card/account numbers must not be on this list.
Working key	A key used to cryptographically process the transaction. A Working key is sometimes referred to as a data key, communications key, session key, or transaction key.
XOR	*See* Exclusive-Or.
Zeroize	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.

Appendix C: Minimum Key Sizes and Equivalent Key Strengths

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

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

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

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

DES refers to TDES keys with non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

For Diffie-Hellman implementations:

- Entities must securely generate and distribute the system-wide parameters: generator *g,* prime number *p* and parameter *q,* the large prime factor of (*p* - 1). Parameter *p* must be at least 2048 bits long, and parameter *q* must be at least 224 bits long. Each entity generates a private key *x* and a public key *y* using the domain parameters (*p, q, g*,). Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
- Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES—see *ISO 16609 – Banking –Requirements for message authentication using symmetric techniques;* Method 3 should be used).