



Payment Card Industry (PCI) **PTS PIN Security Requirements**

Technical FAQs for use with Version 2

December 2015

Table of Contents

PIN Security Requirements: Frequently Asked Questions	1
General	1
PIN Security Requirement 1	1
PIN Security Requirement 6	2
PIN Security Requirement 13	2
PIN Security Requirement 18	3
PIN Security Requirement 21	3
PIN Security Requirement 23	3
PIN Security Requirement 29	4
Normative Annex A – Symmetric Key Distribution Using Asymmetric Techniques	4
Normative Annex A-2 – Certification and Registration Authority Operations	5
PIN Security Requirement 28	5
PIN Security Requirement 32	5
Normative Annex B – Key-Injection Facilities	5
PIN Security Requirement 1	6
PIN Security Requirement 13	7
PIN Security Requirement 29	7
PIN Security Requirement 32	7

PIN Security Requirements: Frequently Asked Questions

These technical FAQs provide answers to questions regarding the application of PCI's (Payment Card Industry) PIN Security Requirements version 2. These FAQs provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered during the evaluation process.

Updates: New or questions modified for clarity are in **red**.

General

- Q 1** June 2015: Requirement 10 allows 2048 RSA keys to encrypt AES keys for transport. This is an exception to the general rule that key encryption keys must be of equal or greater strength to the keys they protect. Are there any other exceptions?
- A** *No. Entities implementing AES for the protection of PINs must protect any such keys at their host with keys of equal or greater strength when those keys are stored external to the HSM. For most entities, this will require that they migrate their host master file keys from TDES to AES keys that are of equal or greater strength than the keys they protect.*
- Q 2** June 2015: Logs are required in a number of requirements for activities in connection with key management. What are the minimum contents of any such log?
- A** *The minimum log contents includes date and time, object name/identifier, purpose, name and signature of individual(s) involved and if applicable, tamper-evident package number(s), if applicable serial number(s) of device(s) involved.*

PIN Security Requirement 1

- Q 3** June 2015: HSMs used for PIN acquiring must be either PCI approved or FIPS140-2 Level 3 or higher certified. Previously, in version 1 of the requirements, HSMs were not required to be specifically approved, but only to have representation that they met ISO requirements for a “physically secure device.”

PCI HSM is a relatively recent standard. As a result, most entities will not yet be operating in a PCI HSM compliant manner for a number of reasons, such as:

- Their HSM pre-dates PCI HSM.
- They may be using unapproved software (such as bespoke versions).
- The shipping requirements of PCI HSM were not met at the time they ordered the unit.
- They may not be able to deploy any “PCI mode” on their HSM.
- Their HSM vendor has not provided a PCI-approved version.

This means that many entities will have to fall back on FIPS 140-2 certification. However, the following issues exist:

- A strict definition of “firmware” would include all the HSM vendor’s embedded software (rather than just the bootstrap, low level drivers, etc.). This would mean that no FIPS 140-2 certificates for PIN processing HSMs meet the requirement.
- A number of the FIPS certificates cover only the crypto module rather than the whole HSM.
- Algorithms may be covered by other NIST/FIPS certifications rather than having been included in the FIPS 140-2 certificate.

For HSMs that were deployed prior to the PIN Security Requirements v2 stipulation of specific industry approvals, how can they demonstrate compliance??

- A** Where FIPS certifications is used in lieu of PCI approval, all of the following must be true:
- The HSM's FIPS 140-2 certificate must include at least the hardware where all cryptographic processes are executed and secret data is stored.
 - The HSM's FIPS 140-2 certificate must include at least the firmware required to load vendor-provided software components in a secure manner.
 - The implementation of cryptographic algorithms used in the HSM's FIPS 140-2-certified module must have appropriate NIST certifications.

PIN Security Requirement 6

Q 4 November 2015: Requirement 6-5 states that 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.**
- **Devices used for key generation or key injection are securely stored when not in use.**

Is this meant to be two separate requirements?

- A** *The first two bullets are options to each other. The third bullet is intended to be part of the second option. Further to this, additional information regarding management of key injection devices is contained in requirement 13-4.*

PIN Security Requirement 13

Q 5 June 2015: Some HSMs use laptop computers with terminal emulation software (e.g., VT-100) for loading clear-text secret or private key components/shares to the HSM due to the lack of availability of dumb terminals or secure cryptographic devices. What controls are required for this usage?

- A** *Only SCDs shall be used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility. An organization using a computer outside of a secure key loading facility is not in compliance with this requirement. Until such time as the organization comes into compliance, they must have the following controls, in addition to those stated in Control Objective 4:*
- *The computer is dedicated for the usage and is only operated under dual control*
 - *The computer must be used either locally via a dedicated physically connected cable or used in a controlled environment as defined in ISO 13491.*
 - *A minimal OS is used, and no applications other than the terminal emulation software is present*
 - *The computer is stored in a tamper evident authenticable (TEA) bag and logged when removed or placed back into storage*
 - *The computer must be further controlled via storage in either a dual control safe or a dual control compartment within a single control safe*
 - *The computer must be booted from a specially customized CD for boot up using a minimal OS image and the terminal emulation application and this CD stored in the same dual access controlled safe/compartment with the computer.*
 - *The computer must not possess a hard drive or any other storage mechanism.*

Q 6 November 2015: Requirement 13-4 requires that key-loading devices must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it. What would meet the requirement for securing the device when not in use?

A *Key loading/generation devices that are required to be securely stored when not in use require the use of a secure container(s) such as a safe or compartment therein, or a secure room. In either case, the equipment can only be physically accessed under dual control.*

PIN Security Requirement 18

Q 7 November 2015: Effective January 2018, encrypted symmetric keys must be managed in structures called key blocks. Does this apply to both when transported and when stored?

A *Yes it applies to the secure exchange of keys between two devices that share a symmetric key exchange key and for the storage of keys under a symmetric key. It is applicable to anytime an encrypted key exists outside of a SCD.*

This applies for both fixed and master/session key scenarios. It does not apply to DUKPT or similar unique key per transaction implementations where keys are stored inside a SCD.

Q 8 November 2015: Is the implementation of TR-31 the only method for meeting the requirement that encrypted symmetric keys must be managed in structures called key blocks?

A *No. TR-31 or any equivalent method can be used. Any equivalent method must include the cryptographic binding of the key-usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key must take place within the secure cryptographic boundary of the device.*

PIN Security Requirement 21

Q 9 June 2015: Can key components of different keys belonging to the same key custodian be stored in the same sealed in opaque, pre-numbered tamper-evident, authenticable packaging or must each component be in its own package?

A *Each key component must be in its own package. While they may be conveyed in a single TEA package, they must be uniquely identifiable packaging, e.g. individually within PIN Mailers.*

PIN Security Requirement 23

Q 10 March 2015: Requirement 23 stipulates that an MFK used by host processing systems for encipherment of keys for local storage—and variants of the MFK—must not be used external to the (logical) configuration that houses the MFK itself. A transaction processing organization uses the same MFK on both their transaction processing system and a stand-alone system used for key generation. The MFK is used as a KEK to transport keys from the key generation system to the transaction processing system. Is this allowed if these two systems are managed and controlled under a single operational and security policy?

A *No. A Master File Key is intended to encrypt other keys for local storage. It is not intended for key transport. The key generation system must have its own MFK and a separate KEK must be used for key transport between the key generation system and the transaction processing system.*

Q 11 June 2015: An entity is using the same MFK for both issuing and acquiring – does that violate any of the requirements?

A *The following scenarios apply:*

- *The issuing and acquiring platform(s) are part of the same logical configuration and the HSMs are either physically or logically (same partition) the same. This is allowed as long as the HSM(s) used do not support functions prohibited in requirement 29.*
- *The issuing and acquiring platform(s) are part of the same logical configuration and the HSMs are either physically or logically separate. This is allowed as long as the HSM(s) used for acquiring do not support functions prohibited in requirement 29.*
- *The issuing and acquiring platform(s) are not part of the same logical configuration. In this scenario the MFKs must be different for issuing vs. acquiring.*

PIN Security Requirement 29

Q 12 November 2015: PIN requirement 29 states that HSMs used for acquiring functions shall not be configured to output clear-text PINs. How is this to be achieved?

A *All commands and configuration options associated with the outputting of clear PINs must be disabled or removed from HSMs used for acquiring. HSMs temporarily used for PIN issuance may be reconfigured but must use a separate key hierarchy e.g., a different master file key.*

Q 13 November 2015: Requirement 29-2 stipulates the implementation of a documented chain of custody to ensure that all devices are controlled from receipt through to placement into service. It further states that the chain of custody must include records to identify responsible personnel for each interaction with the devices. What would constitute an effective and compliant chain of custody?

A *An effective and compliant chain of custody includes procedures, as stated in requirement 29-1, that ensures that access to all POI devices and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection.*

Q 14 November 2015: When do POI devices require direct oversight to prevent unauthorized access up to the point of deployment?

A *If a POI device is held in a secure location where access is restricted to individuals authorized for device access, e.g., a secure room or cabinet, it does not require direct oversight. If the POI device is in an unsecure area, without access restricted to individuals authorized for device access, it requires direct oversight, i.e., the devices must be under direct line of sight at all times of a person authorized for device access.*

Normative Annex A – Symmetric Key Distribution Using Asymmetric Techniques

Q 15 November 2015: Does the loading of secret or private keys to POI devices encrypted using asymmetric keys require compliance with Annex A?

A *Whenever 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, then Annex A does not apply. Remotely means whenever the key loading device and the POI device are not co-located and connected via a direct mechanism, such as a cable.*

Normative Annex A-2 – Certification and Registration Authority Operations

PIN Security Requirement 28

Q 16 June 2015: CAs may use several methods to validate the identity of certificate requestors and recipients before issuance of digital certificates. One of those methods is to use confirmation by telephone, confirmatory postal mail, and/or a comparable procedure. Does email constitute a comparable procedure?

A *Yes, email may be used in lieu of confirmation by telephone or confirmatory postal mail wherever those are specified as options.*

PIN Security Requirement 32

Q 17 November 2015: Requirement 32 of Annex A states that a physically secure, dedicated room must be used to house the CA and RA database and application servers and cryptographic devices and that this room not be used for any other business activities but certificate operations. This applies whenever a Public Key Infrastructure (PKI) is implemented to support remote key distribution using asymmetric techniques for use in connection with PIN encryption to transaction originating devices (POIs). Can this room ever be used for key injection to POI devices, e.g. injection of private or secret keys to the device?

A *If the intent is to use asymmetric keys to transport initial POI acquirer keys, such as initial DUKPT or Terminal Master Keys remotely using asymmetric techniques, then no. If private and/or secret keys are loaded in the CA room, and the intent is not to use asymmetric techniques for remote key loading, then this is not considered a CA operation as defined in Annex A, and thus Annex A does not apply.*

For example, if 1 occurs with the intent to deploy the IPEK encrypted with the POI device's public key after the POI device is deployed, then that would be considered remote key distribution as defined in Annex A and the injection could not be performed within the CA room. However, if both 1 and 2 are performed in the CA room, this is not considered remote key distribution as defined in Annex A and thus Annex A does not apply.

- 1. Injection of the POI device's asymmetric key pair*
- 2. Delivery of the IPEK under the POI device's public key.*

Normative Annex B – Key-Injection Facilities

Q 18 June 2015: Does Annex B - Key Injection Facilities apply to both acquirer and manufacturer keys?

A *The intent of Annex B is to apply to acquirer keys e.g., PIN keys, TMKs, etc. Manufacturer keys are separately addressed as part of the PTS POI Security Requirements and the PTS HSM Security Requirements.*

Acquirer keys includes those used by POI devices, HSMS, and those shared with other internal network nodes or with other organizations that are used for the conveyance of PIN data and associated messages. This also must include keys such as any asymmetric key pairs used for remote key-establishment and distribution as delineated in Annex A, and other keys used in the message flow such as MAC and keys associated with account data encryption. It includes acquirer-controlled private or secret keys used to sign payment applications that handle PIN data, display prompt control data, etc.

Q 19 December 2015: If a KIF uses a Base Derivation Key to derive initial PIN encryption keys (IPEK) used for DUKPT in POI devices, is that considered key generation?

A *Yes. As defined in ISO 11568, symmetric keys and their components are generated by one of the following:*

- *Non-repeatable key generation using*
 1. *a random process, or*
 2. *a pseudo-random process.*
- *Repeatable key generation using*
 1. *key transformation, or*
 2. *key derivation.*

IPEKs are generated by a key derivation process, and are therefore considered key generation.

PIN Security Requirement 1

Q 20 December 2015: Can an ESO perform key injections using either non-compliant keys and/or non-complaint SCDs and still be considered compliant?

A *ESOs that inject non-compliant keys into SCDs, or inject keys into non-compliant SCDs can still be considered compliant if the devices in this instance are not intended to acquire transactions of PCI payment brands or affiliates who require compliance to the PCI PIN Security Requirements. Such operations should be considered out of scope of the PCI PIN requirements. To ensure compliance; proof of confirmation from the non-compliant SCD/key owners, that the devices are intended for non-applicable transactions, must be retained for auditing purposes.*

Q 21 November 2015: Requirement 1-5 details the need for documentation detailing the distributed KIF architecture and key-management flows. Does this only apply to KIF platforms that have a distributed KIF architecture or does it apply to all KIF platforms regardless of architecture.

A *All KIF platforms are required to meet the requirements detailed in 1-5. Specifically the KIF Platform provider must:*

- *Maintain current documentation that describes or illustrates the architecture of the KIF, including all KIF functionality.*
- *Maintain documentation detailing the flow of keys from the key generation, through the functionality to the destination device. The documentation should indicate how personnel interaction and inventory management is integrated into the flow.*

PIN Security Requirement 13

Q 22 November 2015: PIN Entry Devices (PEDs), PCI approved or otherwise, may have their firmware modified to support usage for key injection. Are these devices considered Secure Cryptographic Devices (SCDs) for PCI purposes?

- A** *Modified PEDs, even if previously PCI approved, are not considered SCDs. As such, they are only approved for key injection when performed in conformance with requirement 13 of Annex B. In addition, they are not allowed to retain any clear text secret or private keys or components subsequent to key injection. Furthermore, modified PEDs are not allowed for conveyance of clear text secret or private keys or components.*

PIN Security Requirement 29

Q 23 December 2015: The introductory text to Requirement 29 in Annex B states that secure areas must be established for the inventory of PEDs that have not had keys injected. However these requirements are not detailed in the 'numbered' requirements or have associated testing procedures. How should these be assessed during an assessment?

- A** *As noted in the text, this area must have extended walls from the real floor to the real ceiling using sheetrock, wire mesh, or equivalent. The equivalence can be steel cages extending floor to real ceiling. The cages can have a steel cage top in lieu of the sides extending to the real ceiling. The cages must have locks (with logs) or badge control with logging for entry. An example of an acceptable area would be the secure room used for key injection.*

Test procedures include performing a physical inspection of the storage area to confirm walls go to the true ceiling and floor or an equivalence is achieved, and examination of how access is controlled to ensure that only authorized people have access e.g. who has the physical keys, who keeps copies of the keys, or checking the access control system to see who has badge access. Access logs must be inspected to determine who has entered and whether these times tally with times for receipt of devices or removing devices for key loading.

PIN Security Requirement 32

Q 24 November 2015: When does the injection of clear text secret or private keys or their components to POI devices require the use of a secure room in accordance with requirement 32-10 of Annex B?

- A** *A secure room must be used any time clear keys/components appear in unprotected memory during the process of loading/injecting keys into a SCD.*