



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

---

**Technical FAQs for use with Version 2**

June 2015

# Table of Contents

<b>PIN Security Requirements: Frequently Asked Questions .....</b>	<b>1</b>
General .....	1
PIN Security Requirement 1 .....	1
PIN Security Requirement 13 .....	2
PIN Security Requirement 21 .....	2
PIN Security Requirement 23 .....	3
Normative Annex A-2 – Certification and Registration Authority Operations .....	3
PIN Security Requirement 28 .....	3
Normative Annex B – Key-Injection Facilities .....	3

# 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 the 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 13**

**Q 4** **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 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 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.*

### **PIN Security Requirement 21**

**Q 5** **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 6** 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 7** 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.

## **Normative Annex A-2 – Certification and Registration Authority Operations**

### **PIN Security Requirement 28**

**Q 8** 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.

## **Normative Annex B – Key-Injection Facilities**

**Q 9** 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.

- A** *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.*