Payment Card Industry (PCI)

PTS PIN Security Requirements

Technical FAQs for use with Version 2

November 2018

Table of Contents

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 **July (update) 2017: 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 manual log contents include 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. Electronic logs contain similar information and must be protected from alteration by cryptographic mechanisms (e.g., digital signature or MACing)*

Q 3 **March 2017: Can a TDES key be used to encrypt an AES key for storage, for example, a host Master File Key (MFK)?**

A *No. A key of equal or greater strength must be used to encrypt AES keys for local storage. This requires the use of AES keys to encrypt other AES keys for local storage, either at a host using an HSM, or a POI device.*

Q 4 **March 2017: Can TDES keys be used to encrypt AES keys for conveyance into a POI device.**

A *Yes, but only for local key injection, i.e. directly cabled, and not over a network connection. Furthermore, because TDES keys are significantly weaker than AES keys, this must be treated as equivalent to clear text key injection and requires the use of a secure room as defined in requirement 32-10.*

Note that this specific restriction does not currently apply for the use of 2048 keys for conveyance of AES keys.

Q 5 **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.*

Q 6 **April 2016: Requirement 1 specifies that all hardware security modules (HSMs) are either FIPS140-2 Level 3 or higher certified, or PCI approved. If the using entity applies an update or patch to the HSM's firmware, there may temporarily be a discrepancy between the listed approved versions, and the actual version in place. How can this be addressed during an assessment?**

A *If the using entity has applied a vendor security patch resulting in an updated HSM firmware version, and the PCI SSC or NIST validation of that updated firmware version has not yet been completed (resulting in a mismatch between the HSM firmware version in use and the listed, validated one), the using entity must obtain documentation from the vendor regarding the update that includes confirmation the update has been submitted for evaluation per the process specified by either PCI SSC or NIST (as applicable to the HSM).*

This is not meant to infer that it would not be reported as a compliance issue, but rather that the using entity can take steps to facilitate the remediation process.

Q 7 **April 2016: Requirement 1 specifies the use of FIPS or PCI approved devices. How are PCI approved devices identified on the PCI website?**

A *These devices are identified by among other identifiers, with vendor name, model name/number, hardware version and firmware version – all of which are required to match the listing.*

As described in the PCI PTS Device Testing and Approval Program Guide, vendors may use a combination of fixed and variable alphanumeric characters in the version numbers. However, variable characters are not permitted for any physical or logical device characteristics that impact security. Device characteristics that impact security must be denoted using fixed characters.

The model name cannot contain any variable characters except as low order/suffix type identifiers for non-security relevant differentiators within the device family. All devices within a device family that are intended to be marketed under the same approval number must be explicitly named and pictures of those devices presented for display on the approval listing.

Q 8 **December 2016: Entities acquiring (e.g., the processor) PIN-based transactions are responsible for maintaining an inventory of POI Devices. How does this apply where the acquiring entity does not purchase the POS or ATM devices? For example, a merchant or other third-party purchases and owns the devices.**

A *Ultimately, the entity (typically a financial institution) sponsoring the usage of the devices into a payment network bears the responsibility for any non-compliance. However, the entity driving the devices must maintain an inventory of devices that contains the information stipulated in this requirement.*

Individual brand mandates stipulate which devices may be allowed for use and should be contacted for propriety of usage.

Q 9 **November 2018: In 2016, the NIST Cryptographic Module Validation Program adopted a five-year validation sunset program. This has resulted in a significant number of devices migrating from the Active Validation List to the Historical Validation List. Migration to this list reflects that the certificates and the documentation posted with them are more than 5 years old and have not been updated to reflect the latest NIST guidance and/or transitions, and may not accurately reflect how the module can be used in FIPS mode. It also includes more recently validated devices in accordance with NIST SP 800-131A Rev. 1, Transitioning the Use of Cryptographic Algorithms and Key Lengths whereby the devices use one or more of now disallowed items. For example, for previously allowed AES or TDEA key wrapping, Key Establishment Schemes using Public Key Cryptography, RNGs, etc.**
Can HSMs that have migrated to the CMVP Historical Validation List continue to be used?

A *Yes, FIPS 140-2 HSMs that have migrated to the CMVP Historical Validation List can continue to be used if approved at the time of deployment. However, new deployments (i.e., additional HSMs and not replacements of existing HSMs with like for like) of HSMs on the Historical Validation List are not allowed after December 2019.*

PIN Security Requirement 6

Q 10 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 10

Q 11 April 2016: Are PCI PTS POI v1 or v2 devices able to use RSA 1024-bit length keys to encrypt for transmittal or conveyance of other cryptographic keys as part of key distribution using asymmetric techniques?

A *If the PCI PTS POI v1 or v2 device is capable of supporting 2048 RSA keys, then they must be used. Where support for 2048-bit RSA keys is not possible, 1024-bit RSA keys are permissible.*

Q 12 **July (update) 2017: Requirement 10-1 states: Entities approved against version 3 or higher of the PCI POI Security Requirements—and thus have a mixed portfolio of devices—may use RSA key sizes less than 2048 and use SHA-1 to help facilitate the migration. However, in all cases, version 3 or higher devices must implement RSA using key sizes of 2048 or higher and SHA-2 within 24 months of the publication of these requirements when used for key distribution using asymmetric techniques in accordance with Annex A.**

Does this require that the entire certificate chain of the implementation meets this requirement effective January 2016 (24 months after publication)?

A *The minimum key size for an RSA based scheme on that date remains 2048 for v3 or higher POI devices. Other public key technologies require equivalent or greater strength. Additionally, certification authorities used already require the use of 2048 or higher.*

Implementations using SHA-1 may continue the use of SHA-1 past that date for only the top-level certificate (the Root Certification Authority), which is the trust anchor for the hierarchy of certificates used. The Root CA may be either vendor or acquirer based.

This deferment is due to the root certificate being self-signed, which protects the integrity of the data within the certificate, but does not guarantee the authenticity of the data. The authenticity of the root certificate is based on the use of secure procedures to distribute them. Specifically, they are directly installed into the PIN pad of the ATM or POS device and not remotely loaded to the device subsequent to manufacture.

However, all certificates expire, whether through forced expiration, or risk management considerations. Therefore, plans must exist to migrate the root CA to SHA-2 or higher. All lower level certificates used by the impacted devices must migrate by the effective date.

Q 13 **November 2018: PIN Security Requirement 10 states that RSA keys encrypting keys greater in strength than 80 bits (e.g. triple-length TDEA, AES) shall have a bit strength at least 112 bits (2048 RSA). Does this allow AES keys of any size to be encrypted with 2048 RSA keys?**

A *No. The intent of the allowance of using RSA keys that are weaker in strength than the keys they transport is to leverage the cryptographic algorithms and key strengths in existing POI devices to facilitate the migration to 128-bit AES keys. Other public key techniques such as Diffie Hellman or Elliptic Curve must be used to convey AES keys greater in strength than 128 bits.*

PIN Security Requirement 13

Q 14 **May (update) 2018: 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 *Effective 1 June 2019, 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 1 June 2019, any organization using a computer for loading cleartext keying material to an HSM 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 15 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 14

Q 16 December 2017: Asymmetric key pairs or symmetric keys are commonly used for authentication of applications and for display prompts or to facilitate management (e.g., enable functionality) of HSMs. The private or secret keys associated with these activities frequently reside on smartcards, USB sticks, or other devices which do not qualify as SCDs, but are termed Hardware Management Devices (HMDs). How must these HMDs be managed to compensate for their inherent limitations?

A *These limitations have associated security risks which must be addressed by restricted usage and additional controls. The following controls must be in place:*

- *The HMD must be maintained in a secure storage location, such as a safe or compartment therein, and accessible only under dual control to the authorized custodians.*
- *When removed from the secure storage location, the HMD must be in the physical possession of only the designated custodians and only for the minimum practical time necessary to complete the signing process.*
- *The HMD must be physically safeguarded at all times when removed from secure storage.*
- *If the HMD is decommissioned for any reason, all keying material within the HMD must be rendered irrecoverable in accordance with requirement 31*
- *If the HMD is required to generate keys, e.g., its own key pair, it must be capable of meeting requirement 5.*
- *If the HMD is conveyed between locations, the mechanisms (e.g., PINs) to become operational must not be conveyed using the same communication channel as the HMD. Both the HMD and the operational mechanisms must be conveyed using pre-numbered, tamper-evident, authenticable mailers. The HMD must be inspected for signs of tampering upon receipt.*

Any other usage where keys or multiple cleartext components or shares sufficient to form a key are stored or transported within a single device, requires that the SCD meets the tamper responsive requirements of PCI HSM Security Requirements or ISO 13491-1.

PIN Security Requirement 18

Q 17 December (update) 2016: When encrypted symmetric keys are managed in structures called key blocks, does this apply to both when the keys are 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 working keys for DUKPT or similar unique key per transaction implementations where these keys are stored inside a SCD. However, it does apply to related keys such as Base Derivation Keys and initial DUKPT keys.

Q 18 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.*

Q 19 November 2018: PIN Security Requirement 18 states that encrypted symmetric keys must be managed in structures called key blocks. This applies to both conveyance and storage. Does this only apply to only TDEA keys?

A *No. As stipulated in ANSI X9.24-1: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques, both AES and TDEA keys are required to be managed in key blocks.*

PIN Security Requirement 20

Q 20 December 2016: POI devices must implement unique per device secret and private keys for any function directly or indirectly related to PIN protection. This means not only the PIN-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. Does this apply to initial/start-up keys that are only used to download an initial DUKPT key or a unique terminal master key.

A *Yes. The intent of the requirement is that the compromise of a key in one transaction-originating device (e.g., an EPP or POS device) does not impact the security of another similar device. In that regard, any private or secret key present or otherwise used in a transaction originating device must be unique to that device except by chance.*

Q 21 **November 2018: Entities processing or injecting DUKPT or other key-derivation methodologies must incorporate a segmentation strategy in their environments based upon one or more of the following techniques:**

- **Different BDKs for each financial institution**
- **Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model**
- **Different BDKs by geographic region, market segment, processing platform, or sales unit**

How is this applied to a merchant host or a processor with a single sponsoring financial institution?

A *An entity may use the same BDK for its entire population of POI devices if there is only a single:*

- *Financial Institution (Sponsor), and*
- *Injection Vendor, and they are*
- *Within the same geographic region (e.g., within the US).*

PIN Security Requirement 21

Q 22 **June 2015: Can key components of different keys belonging to the same key custodian be stored in the same sealed 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 23 **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 24 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 25 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 26 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 27 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.*

PIN Security Requirement 31

Q 28 September 2016: Requirement 31 states that SCDs removed from service, even if only temporarily for repair, must render all keying material irrecoverable. Are there any exceptions to this?

A *Yes, PIN pads and integrated circuit card readers used in unattended devices that have anti-removal mechanisms to protect against unauthorized removal and/or unauthorized re-installation may not require zeroization of keys if the nature of the repair is such that it can be performed while all tamper response mechanisms other than the device anti-removal protection mechanisms are active. These mechanisms must be validated as part of the device's PCI POI approval and must be appropriately implemented in accordance with applicable POI requirements, including technical FAQs.*

Protection against removal may be implemented as detection of removal and procedures for authorized installation or re-installation. The procedures must:

- *Use dual-control techniques;*
- *Provide accountability and traceability including logging of user IDs, date and time stamp, and actions performed;*
- *Prevent replay of authorization data; and*
- *Cause the device to not process PIN data until authorized to do so.*

Normative Annex A – Symmetric Key Distribution Using Asymmetric Techniques

Q 29 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.*

Q 30 **November 2018: Two sets of RSA keys pairs, generated respectively by the POI device and the Key Distribution Host (KDH), are used for transport of an initial key to the POI device. Hashes of each public key are sent by a separate channel for loading to the other device (POI hash to KDH and vice versa) such that self-signed certificates are not used as the sole method of authentication. A certification authority is not used. Does this require validation under Annex A?**

A *No, this methodology does not qualify as remote key distribution using asymmetric techniques as described in Annex A. This type of implementation must be otherwise assessed.*

ANSI TR-34 illustrates a remote key methodology that would be compliant whereby both the Key Distribution Host, and the POI device have appropriate credentials in the form of certificates, and also must have a common relationship with a Certificate Authority (CA) as a trust anchor. Accordingly, in a methodology compliant to Annex A, the POI device must contain, at a minimum, its own public/private keypair, an X.509 certificate issued by the CA for the public key, and a certificate from the CA which can be used to verify certificates received from a KDH.

Further to this, in a valid remote key methodology, the KDH must generate a public/private keypair that will be used for signing messages sent to the POI. The public key must be contained in an X.509 certificate issued by the same CA which has issued the certificates for the POI devices. The KDH and the POI can use the credentials to form an automated, cryptographic relationship to transport a symmetric key from the KDH to the POI.

PIN Security Requirement 15

Q 31 **November 2018: Key-establishment and distribution procedures must be designed such that within an implementation design, there shall be no means available for "man-in-the-middle" attacks. What are acceptable methods for remote key distribution using asymmetric techniques methodologies to protect against man-in-the-middle attacks and the hijacking of PIN-acceptance devices?**

A *There are several techniques available, four of which are:*

- *For devices under a PKI hierarchy that facilitates more than one acquirer (e.g., a hierarchy under a PIN-acceptance device vendor's root), an acceptable technique is to force the PIN-acceptance device to bind to a specific transaction-processing host's certificate(s), and not accept commands digitally signed by any other hosts. This is frequently done at initialization of a new PIN-acceptance device, and subject to unbinding techniques as noted in another FAQ. Note: A third party may operate the KDH(s) on behalf of a specific processor. Once bound, POIs are permitted to accept commands from multiple KDHs, provided that each KDH has a certificate aligned to the same transaction-processing host.*
- *The acquirer KDH public key can be loaded only once and requires a factory return (preceded by a zeroization of acquirer keys function) to put the device back to ready state.*
- *An acquirer specific PKI hierarchy can be implemented. For this scenario, because of the rigor of criteria for operating a Certification Authority as stated in Annex A, it is best to have the PIN-acceptance device vendor operate the hierarchy, or else use a company that provides professional Certification Authority services.*
- *Certificate Revocation Lists can be distributed to the device to identify compromised key distribution hosts. This requires that device vendors maintain and distribute the CRLs for KDH keys that are part of their remote key distribution PKI. It further requires that the CRLs*

have a lifetime not to exceed one week to minimize the exposure window. Furthermore, it requires that the device cease processing if it does not possess a valid unexpired CRL.

Q 32 November 2018: ANSI TR-34 describes two protocols for implementing the distribution of symmetric keys using asymmetric techniques. The two techniques are described as the Two Pass method and the One Pass method and should be used as follows:

- **The Two Pass method is appropriate for where the POI and KDH can communicate in real time. It uses random nonces for the prevention of replay attacks.**
- **The One Pass method is appropriate for environments where the POI and KDH will not be able to communicate in real-time i.e. the POI cannot initiate the sequence of cryptographic protocol messages. In these environments, the KDH will generate the cryptographic message that can be transported to the POI over untrusted channels in non-real time. It includes the use of time-stamps in lieu of random nonces to prevent replay attacks.**

The malicious keying of a POI device by a second KDH under the same PKI is possible where the POI has already exchanged credentials with a first KDH. In order to prevent this attack, binding (or an equivalent method as noted in the immediately preceding FAQ) is necessary for all POI devices and is a pre-requisite for both the Two Pass and One Pass key exchange protocols.

If TR-34 is supported, are POI devices required to support both methods?

A *No, a device may support only one. Whether the device supports only one or both, the vendor must describe in the device's security policy that is posted to the PCI website the environments and circumstances under which it is appropriate to implement the supported method(s).*

Normative Annex A-2 – Certification and Registration Authority Operations

PIN Security Requirement 28

Q 33 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 34 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 initial DUKPT keys 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 initial DUKPT keys under the POI device's public key.*

Q 35 July (update) 2017: What is the minimum criteria for construct of Certification Authority room walls for offline CAs?

A *Offline CAs (those used to issue certificates to other CAs and/or KDHs) are typically stored in a large safe when not in use. Thus, construction of CA walls using two layers of 5/8 inch sheet rock attached to metal studs is the minimum requirement for CA room walls. This does not preclude the need for CCTV and alarmed access with motion sensors.*

If the CA room has a wall adjoining another company in a shared facility, the common wall must be reinforced and constructed of metal studded fire rated sheet rock (drywall) with expanded metal (security) mesh. The mesh must be constructed of steel or a stronger material and meet the ASTM F1267-12 or EMMA 557-12 standard. The construction must include vibration detectors to detect any attempts to cut through. The expanded metal (security) mesh shall meet the following minimum requirements:

- *16-gauge metal studs are used with 12inch (305mm) on center*
- *0.75inch #9 steel mesh or 3/4inch #9 or 19mm #9*
- *Thickness 0.120 inches (3mm) 0.01-inch tolerance (0.5mm)*
- *Expanded metal mesh is anchored to the stud with vendor supplied mesh anchors every 12 inches (305mm) and installed per the manufacturer's requirements.*

The installation must be double lined drywall, with expanded metal mesh on the attack side from true floor to true ceiling.

Q 36 July 2017: If a caged environment is used to meet requirement 32 for a CA room, what is the minimum criteria for the fencing materials used?

A *The fencing shall consist of the following minimums:*

- *Chain link, welded or expanded steel metal fencing.*
- *Minimum of 11-gauge wire used in the fencing.*
- *Have a gap no more than 2'' x 2" (50mm x 50mm).*
- *The fencing shall mount to steel fence posts, rails, or metal studs.*
- *Fencing will attach to the post and rails with a minimum 11-gauge tension band or fence brace and bolted together, or metal fencing will attach with vendor provided mounting bolts. Tie wires shall not be used at any time.*
- *Fencing will go from floor to true ceiling or fenced ceiling.*
- *The exterior side of the fencing must be kept clear to prevent the hiding of tamper evidence – e.g., boxes, whiteboards, or other covering materials must not be present. This does not alleviate the need to use blinds or similar materials during key injection activities to prevent observation from outside the secure area, however, this must be on the interior side of the fencing.*

Normative Annex B – Key-Injection Facilities

Q 37 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 38 December 2015: If a KIF uses a Base Derivation Key to derive initial DUKPT keys 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.*

Initial DUKPT keys are generated by a key derivation process, and are therefore considered key generation.

Q 39 July (update) 2017: Are there scenarios where a single key injection operator can perform key loading?

A *For injection in a secure KIF room, a single key injection operator may perform key injections under the following circumstances:*

- *Two authorized key injection operators log in and initialize the key loading device (KLD) so that it is ready to inject keys, i.e., load the Base Derivation Key.*
- *The initial DUKPT or TMK keys are encrypted from the KLD to the POI devices with a key of equal or greater strength.*
- *The KLD is secured in a dual locked cage, rack or cabinet that prevents a single key injection operator from performing any function other than injecting initial DUKPT into POI devices.*

For injection outside a secure room using a secure mobile cart to inject encryption keys on a manufacturing line or a repair line:

- *The KLD is in a secure mobile cart that uses dual locks that support dual control over access to the KLD inside the cart. When the mobile cart is not being used for injection it is stored in a secure room with access and CCTV controls similar to a secure KIF room.*
- *Two authorized custodians are required to unlock the door to the secure mobile cart. Then all controls are the same as for the secure KIF room.*
- *Two authorized key injection operators log in and initialize the key loading device so that it is ready to inject keys.*
- *The initial DUKPT or TMK keys are encrypted from the KLD to the POI devices with a key of equal or greater strength.*
- *The KLD is secured in a dual locked mobile cage that prevents a single key injection operator from performing any function other than injecting initial keys into POI devices.*

PIN Security Requirement 1

Q 40 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 41 **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 42 **July (update) 2017: 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 unless validated and approved to the KLD approval class. 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 18

Q 43 **December 2016: Symmetric keys must be managed in structures called key blocks when stored or transported. Does this apply to symmetric keys that are injected directly from a key loading device (KLD) to a POI or HSM device?**

A *No, the requirement only applies to encrypted symmetric keys that are stored at a transaction host or in a POI device, or are transported over a network connection. It is not intended to apply to keys, encrypted or cleartext, when injected by being directly cabled to a KLD.*

PIN Security Requirement 29

Q 44 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 45 November 2018: Only encrypted key loading is allowed for POI v3 or higher devices after 2020 for entities engaged in key injection on behalf of others. Does this apply to manufacturer's keys?

A *The PIN requirements are applicable to the keys used in the acquisition and protection of PIN data, and the keys associated with protection of those keys. This includes the following:*

- *Device-specific private keys for use in connection with remote key loading using asymmetric techniques*
- *Secret and private keys used for the protection of PIN data when conveyed between non-integrated components of a POI device—e.g., an SCR and a PIN pad.*

Q 46 July (update) 2017: 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 outside the tamper protected boundary of an SCD during the process of loading/injecting keys into a SCD.*

Q 47 **July (update) 2016: Requirement 32 stipulates that a secure area (room) is used for key injection where any secret or private keys or their components appear in unprotected memory during the process of loading/injecting keys into an SCD. The secure area must have walls made of solid materials, and additionally if the solid walls do not extend from the real floor to the real ceiling, the secure area must have extended walls from the real floor to the real ceiling using sheetrock or wire mesh. Can the secure room enclosure be made up of all metal wire mesh e.g., a cage?**

A *No, use of a wire mesh enclosure is not acceptable except as noted below. Wire mesh is only allowed as specified i.e., above false ceilings and below false floors. As stated in the requirement, the walls must at a minimum be made of solid materials between the visible floor and ceiling. If the walls are transparent, e.g., acrylic glass, then blinds or similar must be used during key injection activities to prevent observation from outside the secure area.*

In KIF environments where Level 1 and Level 2 physical barrier controls are in place and confirmed, the environment may be implemented within a "caged" environment. A caged environment is an enclosed secure room that meets the criteria of Requirement 32 but is not made of solid walls. Refer to Normative Annex A: A2 for additional information on Level 1 and Level 2 physical barrier controls. All other criteria stated in requirements 13-9 and 32-10 for when clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys applies.

If the metal screening cannot extend to the real ceiling because of (1) the presence of air-conditioning ducts, water pipes and/or cables, or (2) the height of the real ceiling (for example in a warehouse with a high ceiling), the metal screening can extend over the top of the KIF.

The intent of this requirement is to ensure the facility observes industry recognized requirements to allows only authorized access to the facility, facility access is managed appropriately and the KIF environment:

- *Restrict Access*
- *Restrict Observation*
- *Facilitate the effective use of motion activated CCTV systems*
- *Prevent the passing of restricted materials through openings.*

Q 48 July 2016: If a caged environment is used to meet requirement 32 for a KIF room, what is the minimum criteria for the fencing materials used?

A *The fencing shall consist of the following minimums:*

- *Chain link, welded or expanded steel metal fencing.*
- *Minimum of 11-gauge wire used in the fencing.*
- *Have a gap no more than 2'' x 2" (50mm x 50mm).*
- *The fencing shall mount to steel fence posts, rails, or metal studs.*
- *Fencing will attach to the post and rails with a minimum 11-gauge tension band or fence brace and bolted together, or metal fencing will attach with vendor provided mounting bolts. Tie wires shall not be used at any time.*
- *Fencing will go from floor to true ceiling or fenced ceiling.*
- *The exterior side of the fencing must be kept clear to prevent the hiding of tamper evidence – e.g., boxes, whiteboards, or other covering materials must not be present. This does not alleviate the need to use blinds or similar materials during key injection activities to prevent observation from outside the secure area, however, this must be on the interior side of the fencing.*