Payment Card Industry (PCI)

PTS PIN Security Requirements

Technical FAQs for use with Version 3

December 2024

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 3. 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?**

Yes, but only for local key injection—i.e., directly cable—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 32-9.

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

Q 5 January 2020: Can an acquirer use third-party hosted HSM service—i.e., HSM in the cloud?

A *Yes, however the acquirer is responsible for ensuring that all applicable requirements regarding the management of the HSMs are met by the HSM cloud Provider.*

Q 6 January 2020: Can an HSM as a Service (cloud) provider use third-party hosted data center facilities to house the HSMs?

A *Yes, subject to the following:*

- *The cloud provider must control all logical access. Data center operations staff must not have any logical access rights (administrator or operator) to the HSMs.*
- *The cloud provider must have appropriately placed CCTV cameras that are implemented consistent with PIN Requirement Annex B 32-9.7 and send images to a server controlled by the cloud provider at a site other than that of the data center hosting the HSMs—e.g., the cloud provider's own site.*
- *Access to the cabinets housing the cloud provider's HSMs and/or peripheral equipment—e.g., firewalls—must either be:*
  - *Controlled directly by cloud provider staff under dual control via badge or equivalent mechanisms; or*
  - *Restricted to known pre-authorized data center staff under dual control via badge or equivalent mechanisms and where physical access is required, the cloud provider must:*
  - *Monitor access to the cabinets housing the equipment at all times during any access,*
    - *Authorizes the access for an approved purpose during a specific time window,*
    - *Verifies the identity of data center staff upon and during access, and*
    - *Monitors the activity during the maintenance window.*

Q 7 November 2020: Do the PIN Security Requirements apply to SPoC solutions?

A *SPoC solutions are tested and evaluated by PCI laboratories using the PCI Software-based PIN Entry on COTS (SPoC) Security Requirements, which is a separate and distinct standard from PCI PIN Requirements and Testing Procedures. The SPoC Security Requirements align with the PIN standard as it pertains to use of SCDs (SCRPs and HSMs) and requires the PIN processing environments and key injection facilities to be validated against the PCI PIN standard as enumerated in the SPoC Program Guide. Therefore, the PIN Security Requirements apply indirectly to SPoC solutions. Refer to the PCI SPoC Security Requirements and associated Testing Requirements available on the PCI Document Library at https://www.pcisecuritystandards.org/document_library, to understand all the requirements that are applicable to SPoC solutions.*

Q 8 November 2020: Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms stipulates that key-encipherment keys shall be at least of equal or greater strength than any key that they are protecting. And that this applies to any key-encipherment keys used for the protection of secret or private keys that are stored or for keys used to encrypt any secret or private keys for loading or transport. Does this apply to key conveyance in a secure environment?

A *Yes, unless otherwise stated it applies to all key storage, loading or conveyance.*

Q 9 December 2021: Are remote assessments permitted for PIN Security Requirements assessments?

A *While onsite assessments continue to be the expected method for PCI SSC assessments, the use of remote assessment methods may provide a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. Prior to the engagement of the QPA, entities must consult with the applicable compliance-accepting entity to confirm whether remote assessments are allowed and any requirements they may have around the submission of remote assessment reports.*

PCI SSC has developed a set of guidelines and procedures outlining the appropriate use of remote assessment methods when an onsite assessment is not feasible and where remote assessments are permitted by the compliance-accepting entity. The PCI SSC Remote Assessment Guidelines and Procedures can be found in the PCI SSC Document Library Remote Assessment (pcisecuritystandards.org).

If remote assessment methods are used in place of an onsite assessment, the Assessor may be required to complete the Addendum for ROC/ROV: Remote Assessments, provided in Appendix A of the PCI SSC Remote Assessment Guidelines and Procedures document, if requested by the compliance-accepting entity.

Contact the applicable payment brand(s) at https://www.pcisecuritystandards.org/faqs

Q 10 May 2024: Can a service provider providing multi-tenant (i.e., concurrent multi-organizational usage) HSM services share secret or private cryptographic keys between tenants?

A *No. Secret and private cryptographic keys that are managed or owned by the HSM Service Provider to support each of their HSM tenant (clients) must be unique per HSM tenant. This would not apply to keys used to support an HSM's Virtualization System (e.g., device authentication keys, firmware integrity keys, etc.).*

Q 11 May 2024: Can a service provider providing multi-tenant HSM services share the same master/storage ("Local Master Key" or "Master File Key") keys between HSMs?

A *No. Where multi-tenant HSM services are provided, master/storage keys that are not directly managed or owned by the HSM tenant must be unique per HSM instance, except in cases where a tenant instance pair/cluster has a designated purpose of load balancing or hot-spare backup.*

Q 12 May 2024: What additional requirements exist for multi-tenant HSMs?

A *An HSM Service Provider that provides cryptographic key storage and operations across multiple tenants must use both i) HSMs with multi-tenant features; and ii) procedural controls, that ensure:*

- *Compromise of any key within the hierarchy of any one tenant does not impact the security of cryptographic keys for another tenant.*
- *The cryptographic keys of any one tenant cannot be loaded, deleted, used for operational processing, or otherwise accessed in any way by another tenant.*
- *The HSM tenant must be able to query the HSM configuration to determine settings meet the PCI PIN requirements. Changes to settings which may Impact how any PCI PIN requirement is met must be communicated to the HSM tenants prior to the change being made.*
- *The multi-tenant HSM service provider must, at all times, meet all relevant PCI PIN requirements.*

Q 13 May 2024: Do different HSM Service Provider architectures impact how cryptographic key material used as part of the HSM Solution need to be protected?

A *Two possible solutions that a HSM Service Provider may use, but are not limited to:*

- *Implementation of two or more virtual HSMs within a single physical HSM instance, with each virtual HSM having its own tamper key e.g., the master/storage key ("Local Master Key" or "Master File Key"), controlled by the HSM tenant; or*
- *Implementation where the HSM Solution stores the master keys of the HSM tenants in an encrypted form under a higher-level tamper key, the same way the working keys themselves are stored encrypted under the HSM tenant's master key.*

In either implementation, the requirements for protecting the ownership and security of the user keys remains, and it is expected that any HSM tamper key regardless of whether it is directly managed by the user is unique per HSM and does not facilitate the exposure or unauthorized use of the user keys it protects.

Q 14 May 2024: What procedures must a HSM Service Provider have for the handover of a tenant's partition from the HSM service provider (HSM owner) to a tenant (client)?

A *For partition handovers to tenants, the HSM Service Provider must have and follow documented procedures that include:*

- *The use of functionality that provides for and entails cryptographic decoupling of HSM partition administration from the HSM Service Provider to the tenant organization.*
- *Ensuring the assigned partitions do not have any keys from or traces of the previous tenant of the HSM service provider other than default administrative keys that allow for tenant initialization which must be replaced during initialization.*
- *Ensuring the only HSM Service Provider operations permitted on a tenant partition are to suspend or terminate the tenant partition.*

Note the detail of the procedures may vary by HSM platform vendor and/or model, including firmware version.

Q 15 May 2024: What procedures must a HSM Service Provider have for the termination of a tenant partition?

A *For the termination of tenant partitions, the HSM as a Service Provider must have and follow documented procedures that include ensuring the complete erasure of key material, administrative access and configuration settings. These documented procedures must define how quickly key material is to be destroyed, either immediately or within a contractually defined destruction timeline; ensuring that a notification of destruction is communicated to the tenant.*

Additionally, when the tenant relationship is terminated, all instances of tenant owned keys (e.g., in backups or external storage) shall be securely destroyed/erased.

In all cases, the partition's secure log file shall be retained after termination. The entity responsible for maintaining the logs after termination is dependent on whom, per the service agreement, was responsible for key management activities within the partition. Tenants responsible for maintaining the logs may delegate this to the HSM as a Service Provider.

Q 16 December 2024: Are Hardware Management Devices (HMDs), e.g., smartcards, equivalent to Secure Cryptographic Devices (SCDs) for purposes of key management?

A *No. Consistent with ISO 13491, HMDs are not considered equivalent to SCDs, as HMDs are a "non-secure cryptographic device (SCD), typically a dedicated integrated circuit card (ICC), with security features similar to an SCD but lacking tamper-response characteristics".*

As stated in ISO 11568, cleartext key components and shares include both written form and those stored within an HMD, regardless of whether that component or share is encrypted within the HMD or similar device. PIN Security Requirements that reference cleartext key components and shares are applicable to those managed using HMDs.

PIN Security Requirement 1

Q 1 **January (update) 2020: HSMs used for PIN acquiring must be either PCI approved or FIPS140-2 Level 3 or higher certified. Under FIPS, the target of evaluation can be selected by the HSM vendor, and can vary widely. What are the minimum criteria that the scope of the FIPS certification must include?**

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.*
- *Effective 1 July 2020 for new deployments—i.e., additional HSMs and not replacements of existing HSMs with like for like—the HSM's FIPS 140-2 certification scope (the Target of Evaluation) must include the tamper responsive boundaries within which PIN translation occurs.*

Q 2 **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 3 **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 4 **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 5 **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.*

Q 6 **July (update) 2022: For PCI approved HSMs that have had their approvals expire, can they continue to be used?**

A *For clarification on the usage of PCI approved HSMs for which the approval has expired, contact the payment brand(s) of interest at: https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands*

Q 7 **November 2020: PCI approved HSMs may contain in the Additional Information field on the PCI website whether or not they must be deployed in a Controlled or the more robust Secure Environment as described in ISO 13491-2: Financial services — Secure cryptographic devices (retail) — Security compliance checklists for devices used in financial transactions. Does this impact their compliance to the PIN Security Requirements?**

A *Yes. PCI approved HSMs that are approved with the restriction must be deployed in environments that meets at least the ISO 13491-2 requirements for a Controlled Environment. Failure to do so invalidates the HSM's approval and thus its compliance to the PIN Security Requirements.*

Q 8 October 2024: Can PCI PTS approved EPPs, PEDs and SCRPs with expired approvals continue to be used?

A *Yes. EPPs, PEDs and SCRPs with expired approvals can continue to be used if approved at the time of deployment. However, new deployments, i.e., additional devices are not allowed, except as replacement of like for like of existing deployed devices.*

Q 9 October 2024: Are PIN acceptance devices including EPPs, PEDs and SCRPs with expired approvals considered as acceptable for PCI PIN assessment?

A *PIN acceptance devices deployed prior to their approval expiry are considered as acceptable for PCI PIN within a 10-year period after the approval expiry. Using PCI PTS approved PIN acceptance devices beyond that timeline may put an entity at risk of liability for any breach that can be tied to the use of a device post sunset of the approval expiry.*

PIN Security Requirement 2

Q 1 September 2021: PCI PIN Requirement 2-2 says "Online PIN translation must only occur using one of the allowed key-management methods: DUKPT, fixed key, master key/session key. Effective 1 January 2023: Fixed key for TDEA PIN encryption in POI devices is disallowed." What is fixed key management?

A *Fixed key is a transaction key-management method whereby the fixed transaction key is either physically loaded (from a KLD or using components or shares) or remotely loaded using asymmetric techniques. The fixed transaction key is used for transaction processing until a new key is similarly loaded. There is no ability to change this key except by using the same technique that originally loaded the key.*

Q 2 September 2021: What is master key/session key management?

A *Master key/session key management is a method for managing transaction keys using a key-encipherment key, called a master key, that is used to encrypt for distribution new or replacement key-encipherment keys, derivation keys and/or Session (e.g., PIN encryption keys) keys. This method is also known as the master key/transaction key method.*

Q 3 September 2021: For purposes of routing PIN transactions, organizations will share a key-encipherment key (KEK). The establishment of this key in most cases involves the manual loading of key components. Subsequently a PIN encipherment key (PEK) is generated by one organization and encrypted by this KEK to send to the other organization. If this PEK is infrequently or never changed, does that constitute a fixed key under the PIN Security Requirements?

A *No. The ability to replace the PEK over the network encrypted by the KEK is a master key/session key management method. Even if a PEK exists for an extended period of time without change, this is not considered fixed key management.*

Q 4 September 2021: For POI devices, a key-encipherment key (KEK), frequently called a Terminal Master Key (TMK) is loaded physically (from a KLD or in components or shares) or using asymmetric techniques. This key is subsequently used to encrypt PIN encryption keys (PEKs) for distribution. If the initially loaded PEK is not changed, is that fixed key?

A *No. Changing the PEK on a regular basis is considered a best practice, but not changing it does not constitute fixed key when a terminal master key (TMK) is available to use for replacement.*

PIN Security Requirement 3

Q 1 **October 2022: ISO 9564 stipulates restrictions on translations between PIN block formats, that are applicable when the HSM does not enforce unique-key-per-transaction encryption for the resulting PIN block. For example, translations from PIN block formats 0, 3 or 4 to PIN block format 1 is not allowed unless that stipulation is met. How must this unique-key-per-transaction encryption be enforced by the HSM?**

A *The HSM must enforce the UKPT exception by integrating the UKPT derivation of the PIN encryption key used in the PIN block translation with the translation operation. This may be done as a function call available in the standard HSM firmware or via a custom function. Alternatively, the HSM only supports UKPT as the default state.*

It is not acceptable to require a series of separate function calls from an external application to make this translation.

PIN Security Requirement 6

Q 1 **May 2019: Printers used for printing key components must not be used for other purposes and must not be networked—i.e., locally connected in a system that is dedicated to the printing of key components and is not connected to any other system. Are there any circumstances where the printing system can have connectivity for the conveyance of encrypted keys to another system related to PIN processing?**

A *Yes, if the printing system is protected by a firewall(s) from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to:*

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

Q 2 September 2022: When can a manual (handwritten) capture of generated key components be performed outside of a secure room?

A *It may be acceptable to generate and manually write down key shares/components outside of a secure room for the purpose of establishing shared keys with other organizations, when there exists no other compatible way of communication—e.g., smart cards—under the following conditions (see requirement 13-2 for loading of clear-text keying material):*

- *Only approved Secure Cryptographic Devices (SCDs) are used—i.e., key shares/components are displayed on the integrated display of a PCI or FIPS approved SCD (e.g., an HSM or KLD). Key shares must never appear in memory outside the tamper-protected boundaries of an SCD or a Hardware Management Device (HMD).*
- *The process is performed in a controlled or higher environment as defined in ISO 13491-2.*
- *The principles of dual control and split knowledge must be followed.*
- *CCTV cameras must be positioned so they do not monitor any clear-text keying materials, combination locks, PIN pads, or keyboards used to enter passwords/authentication codes or other authentication credentials; otherwise, custodians must position their bodies to obscure monitoring (per 6-3.8).*

All other requirements concerning key generation (for example, requirement 6-1) apply.

Q 3 June 2023: Per requirement 13, PC-based key-loading software platforms that allow clear-text secret and/or private keys and/or their components to exist in memory outside the secure boundary of an SCD are no longer allowed. Does this also apply to specifically tasked PCs used for key generation during key loading to meet requirement 6-2?

A *Single-purpose computers with an installed SCD where clear keying material is injected directly from a secure port on the key-generating SCD to the target SCD (e.g., a POI device) can continue to be used. Effective 1 January 2023 the use of PCs where any cleartext keying material passes through the memory of the PC is no longer allowed.*

Note the SCD used must have a random number generator that has been approved consistent with requirement 5.

PIN Security Requirement 10

Q 1 **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 2 **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 3 **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.*

Q 4 **November 2020: When an initial symmetric key is loaded as a KBPK, for the purposes of these requirements is this considered an acquirer key in a manner similar to a TMK?**

A *Yes*

Q 5 October 2023: RSA keys with a modulus of 2048 bits can be used for the conveyance of 128-bit AES keys. This is an exception to the requirement that any keys used in key conveyance must be of equal or greater strength then the key conveyed. Are there any other exceptions?

A *No. This exception is only permitted in scenarios where asymmetric remote-key distribution is being used to convey an AES-128 key to a POI or HSM. In all other cases both the key used for wrapping and the key used for signing must be of equal or greater strength then the key conveyed.*

Please note, the referenced exception is a recognition of limitations that exist in current cryptographic technologies. It should be expected that this exception will be sunset at some future point after the publication of appropriate industry standards.

PIN Security Requirement 12

Q 1 December (update) 2022: Does the loading of clear-text private and secret key components/shares into HSMs require the use of secure cryptographic devices (SCDs) to protect those components/shares?

A *Yes. Effective 1 January 2024 it is required for any HSM used in production, even if located in a Secure Room meeting at least the requirements of 6-3, that the loading of cleartext private and secret key components/shares must use an SCD via one of the following methods:*

1. *An SCD such as a PCI approved KLD,*
2. *A PCI approved remote administration solution, or*
3. *Entering keying material through integrated keypads designed for secure entry that may exist on some HSM models*

Loading of cleartext private and secret key components/shares may also involve the use of Hardware Management Devices (HMDs) in conjunction with methods 2) and 3) where applicable.

Q 2 May 2024: What additional requirements exist for the remote loading of cryptographic keys into a HSM using a remote (non-console) connection?

A *Secret and private cryptographic keys and key components must be transported in a way that secures their confidentiality and integrity. All cryptographic keys, including public keys, must be secured for authenticity.*

Remote (non-console) loading of cryptographic keys using public key techniques must not rely on the use of unauthenticated public keys, or keys established during key agreement processes which do not ensure the authenticity of the keys established. Secure channels are required for remote connections but cannot be relied upon as the mechanism to provide confidentiality or authenticity controls.

PIN Security Requirement 13

Q 1 **January (update) 2020: 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.*

Q 2 **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.*

Q 3 **August 2019: New deployments of FIPS 140-2 HSMs that have migrated to the NIST Cryptographic Module Validation Program Historical List are not allowed for new deployments—i.e., additional HSMs and not replacements of existing HSMs with like for like—after December 2019. Does this apply to other Secure Cryptographic Devices (SCDs) such as Key Loading Devices (KLDs) that are dependent upon FIPS certification to qualify as an SCD?**

A *Yes, it does apply to other SCDs used to meet PIN Security Requirements.*

Q 4 **July (update) 2022: Does the remote administration of HSMs require the use of an SCD for the management of keying material and sensitive configuration settings?**

A *Any remote administration solution used for non-console access to HSMs must either:*

- *Use an SCD that is listed as a PCI HSM Remote Administration Platform (RAP) approval class or*
- *Is designated as a valid mechanism—i.e., function provided—on the Approved PTS Devices website in conjunction with the specific HSM approval(s) for which they are intended to be used. Note that mechanisms not validated to the RAP approval class require the use of a separate hardware-based appliance approved under the PCI PTS requirements as a Key Loading Device for the loading of any clear-text keying material.*

Q 5 **September 2022: Is it required to use a secure room that complies with requirement 32-9 to load keys into HSMs?**

A *No. Requirement 32-9 applies to the loading of keys to POI devices at a centralized location prior to deployment. This location is referred to as a key injection facility (KIF). A KIF may be operated by a third party or directly by the processor organization.*

The loading of clear-text key components and/or key shares outside of a KIF is addressed in requirement 13-2. Examples include HSMs and deployed POI devices where a secure cryptographic device, such as a PCI approved KLD is used. It may also involve the use of Hardware Management Devices (HMDs) or entering keying material through integrated keypads designed for secure entry that exist on PIN entry devices or that may exist on some HSM models.

PIN Security Requirement 14

Q 1 **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 clear-text 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 17

Q 2 **November 2020: Requirement 17 states that where two organizations or logically separate systems share a key to encrypt PINs (including key-encipherment keys used to encrypt PIN-encryption keys) communicated between them, that key must be unique to those two organizations or logically separate systems. Does this require that each communication link between the same two organizations or logically separate systems must implement a unique key?**

A *No. Multiple communication links between the same two organizations or logically separate systems are permitted to use the same keys for the same data types.*

PIN Security Requirement 18

Q 1 **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 2 **November 2015: Is the implementation of ANSI X9.143 the only method for meeting the requirement that encrypted symmetric keys must be managed in structures called key blocks?**

A *No. ANSI X9.143 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 3 **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.*

Q 4 **June (update) 2021: Organizations must implement key blocks for external connections to Associations and Networks by 1 January 2023. If a service provider cannot implement key blocks for all connections to other organizations because one or more of the external organizations do not support key blocks, what are the service provider's options for meeting the requirement?**

A *The service provider must implement key blocks for all external organizations that support key blocks by the deadline. The assessor must validate the service provider is capable of implementing key blocks for the other organization(s) who do not yet support key blocks when those organizations become capable.*

Furthermore, the assessor must note in the PSR report the organizations for which it has implemented key blocks and those organizations for which the service provider has not with the reason stated—e.g., the other organization does not support key blocks.

Q 5 **November 2020: Requirement 18 states that key blocks must be implemented for internal connections and key storage within Service Provider Environments. Does this apply to key conveyance between secure cryptographic devices within an organization?**

A *Yes. It applies to all key conveyance between systems within an organization, including keys stored on databases or in a device's unprotected memory.*

Q 6 **April 2021: Key blocks for the transport and storage of symmetric keys—i.e., AES and TDES keys—are required to be implemented in accordance with a three phased approach. Allowed formats for these key blocks are defined by the standards bodies, ANSI and ISO. In addition, proprietary—i.e., non-ANSI or ISO recognized—methods have been allowed if "equivalent." In September 2020, specific criteria that proprietary methods must meet in order to be verified as equivalent was published in the PCI PTS HSM Security Requirements Technical FAQs and in the PCI PTS POI Security Requirements Technical FAQs.**

PTS vendors or other third parties providing proprietary methods have until 1 January 2023 to meet these criteria. How does that impact assessments of Service Providers who have implemented these proprietary methods that have not yet achieved validation?

A *Until January 2023, Service Providers, where applicable, can continue to operate using existing proprietary methods that have not yet been validated under the defined process. Any newly developed proprietary methods must undergo the defined process prior to any implementations.*

Q 7 **October 2023: Does 18-3 apply anytime the key conveyance is organization to organization? For example, sending a BDK from a processor to a KIF or vice versa?**

A *Yes, the distribution of keys in key blocks organization-to-organization that aren't associations or networks (e.g., between a processor and their 3rd Party KIF Service Providers) is included in the Phase 3 sunrise.*

Q 8 **October 2023: Do the Key Block mandates apply to solutions that make use of M/S key solutions when electronically conveying Session key updates that are encrypted under each terminal's M/S KEK(s)?**

A *Yes, as part of the Phase 3 sunrise, the delivery of both Master Keys and Session keys must be delivered to POIs in Key Blocks.*

Q 9 October (update) 2022: PIN Security Requirement 18-3 requires the implementation of key blocks. Interoperable methods include those defined in ANSI X9.143 and ISO 20038. The requirement also allows for any equivalent method whereby the equivalent method includes the cryptographic binding of the key-usage information to the key value using accepted methods. How are equivalent methods determined?

A *Equivalent methods must be subject to an independent expert review and said review is publicly available:*

- *The review by the independent expert must include proof that in the equivalent method the encrypted key and its attributes in the Key Block have integrity protection such that it is computationally infeasible for the key to be used if the key or its attributes have been modified. Modification includes, but is not limited to:*
  - *Changing or replacing any bit(s) in the attributes or encrypted key*
  - *Interchanging any bits of the protected Key Block with bits from another part of the block*
- *The independent expert must be qualified via a combination of education, training, and experience in cryptology to provide objective technical evaluations that are independent of any ties to vendors and special interests. Independent expert is further defined below.*
- *The PTS laboratory will validate that any device vendors implementing this methodology have done so following all guidelines of said evaluation and peer review, including any recommendations for associated key management.*

An Independent Expert possesses the following qualifications:

- *Holds one or more professional credentials applicable to the field—e.g., doctoral-level qualifications in a relevant discipline or government certification in cryptography by an authoritative body (e.g., NSA, CES, or GCHQ);*
- *Has ten or more years of experience in the relevant subject;*
- *Subscribes to an ethical code of conduct and would be subject to an ethics compliance process if warranted;*
- *Has published at least two articles in peer-reviewed publications on the relevant subject or is recognized by his/her peers in the field—e.g., awarded the Fellow or Distinguished Fellow or similar professional recognition by an appropriate body, e.g., ACM, BCS, IEEE, IET, IACR.*

Independence requires that the entity is not subject to control, restriction, modification, or limitation from a given outside source. Specifically, independence requires that a person, firm or corporation who holds itself out for employment as a cryptologist or similar expert to more than one client company is not a regular employee of that company, does not work exclusively for one company and where paid, is paid in each case assigned for time consumed and expenses incurred.

Note: *Multiple individuals who collectively possess the necessary expertise who meet the independence criteria can be used. When using a group approach, each individual must have at least 10 years of experience in the relevant subject and must subscribe to an ethical code of conduct.*

Q 10 June 2023: Do Key Blocks apply to all PIN security-relevant symmetric keys?

A *Yes, key blocks must be used for all PIN security-relevant symmetric keys that are exchanged or stored – for example, Zone Master Keys (ZMKs), Key-Encipherment Keys (KEKs), Base Derivation Keys (BDKs), Terminal Master Keys (TMKs), and PIN-Encryption Keys (PEKs). This key block requirement applies whether the subject symmetric key is conveyed using asymmetric or symmetric techniques.*

Q 11 October (update) 2024: What key block methods are compliant?

A *For storage and distribution of symmetric keys using symmetric techniques the following are compliant:*

- *Where the key and sensitive attributes field are encrypted with AES, the methods in ISO 20038 or ANSI X9.143 or mechanism 2 of ISO/IEC 19772.*
- *Where the key and sensitive attributes field are encrypted with TDES, the methods in ANSI X9.143 or the TDKW method from ANSI X9.102.*

For storage and distribution of symmetric keys using asymmetric techniques the following are compliant:

- *ASC X9 TR-34.*
- *RSA OAEP encryption of, at least, the symmetric key with RSA signature over the encrypted key and attributes specified below to permit the KRD to authenticate the KDH.*
- *ECDH to allow derivation of a shared secret key followed by symmetric encryption of, at least, the symmetric key with ECDSA signature over the encrypted key and attributes specified below.*

Other symmetric or asymmetric methods not listed above can meet the intent of this requirement if they have been validated as equivalent based on criteria defined in PCI HSM and POI Technical FAQs and as listed in the "Additional Information" associated with the PCI approval listing for that device. Regardless, all methods must at a minimum include:

- *One or more attributes as set by the intended purpose definition that define the operations for which the key can be used.*
- *One or more attributes that define the cryptographic algorithm and mode of use for which the key can be used.*
- *One or more attributes that define whether the protected key may be transferred outside the cryptographic domain in which the key is found i.e., exportability. +*
- *Authentication over the encrypted key and attributes (i.e., MAC, digital signature, or authenticated encryption).*

Additionally, as the industry continues to migrate the POI and HSM infrastructure, key length obfuscation padding to the maximum length for the algorithm, 192 bits for TDEA and 256 bits for AES will be required for new deployments once appropriate future updates to the PCI Security Requirements for POI and HSM devices are published and take effect.

Q 12 September 2023: Can RSA OAEP Padding methods used to encrypt a key be considered as an acceptable method of achieving the Key Block requirements of 18-3?

A *No. Simple RSA OAEP encryption does not cryptographically bind the keys usage to the encrypted key material. Per 18-3, the key usage must be cryptographically bound to the key using accepted methods, such that it must be infeasible for the key to be used if the usage attributes have been altered. Acceptable methods include, but are not limited to:*

- *A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the Key Block, which includes the key itself - e.g., ANSI X9.143*
- *A digital signature computed over that same data - e.g., ASC X9 TR 34*
- *An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.*

Q 13 September 2023: Can TLS be enough to protect and bind the key usage to the encrypted key to meet the requirements of 18-3?

A *No. To support "defense in depth" it is encouraged to use TLS when delivering subject keys that are wrapped in key blocks. However, TLS alone does not cryptographically bind a key's usage to the encrypted key and thus cannot be used as a substitute for a key block. Additionally, TLS typically does not protect data flowing all the way into an SCD (e.g., HSMs or POI devices) that will use the subject key.*

Q 14 October (update) 2024: Regarding the implementation dates, does that mean all previously established keys have to be changed, or that only from that point onwards newly exchanged keys must use Key Blocks?

A *No, all previously established keys can still be used. Key Block Exchange Keys (e.g., an X9.143 Key-Block Protection Keys - (KBPKs), TR34 Asymmetric Key Wrapping Key, etc.) must be established for all connections sending keys after the implementation date.*

In the case of symmetric Key Encipherment Keys (KEK) currently used for delivering keys in cryptograms, there is no expectation for the existing KEK to be reissued as KBPKs. An existing KEK can be converted to a KBPK if your HSM or POI vendor has a method to accomplish this, or you have the components or shares to recreate it as a KBPK.

Q 15 October 2024: When using RSA OAEP for the distribution of symmetric keys using asymmetric techniques, does the KDH use the RSA public key from the KRD to directly encrypt the transactions keys, such as an IPEK or TMK?

A *No. As is specified by TR-34, the KRD's public key shall be used to encipher an ephemeral symmetric wrapping key which is used to encipher the transaction key. TR-34 includes the transaction key data, the transaction key usage details, and the signing identity into the encrypted data portion, and then signs the entire encrypted structure with a KDH signing key to ensure authentication of all the data between the KDH and KRD. Implementations that do not meet TR-34 must use an ephemeral symmetric wrapping key and as per FAQ #11 of requirement 18 are required to sign the encrypted transaction key along with key usage attributes with an RSA signing key from the KDH.*

Q 16 October 2024: Phase 3 requiring the implementation of key blocks takes effect January 2025 for all merchant hosts, point-of-sale (POS) devices and ATMs. Does this impact deployments of POI (POS and ATM) devices that existed before that date?

A *No. Existing deployments of POI devices are not required to convert to the use of key blocks but may optionally do so. New deployments must implement key blocks. For example:*

1) Where Master/Session key management is implemented via local key injection, key block protection keys must be established within the device to support the regular update of session keys post-deployment using X9.143.

2) Asymmetric methods (e.g., TR-34) may be used for the remote establishment of initial keys.

PIN Security Requirement 20

Q 1 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 2 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 1 **January (update) 2020: 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 stored in its own TEA 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 1 **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 2 **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 26

Q 1 **September 2022: Requirement 26 stipulates that logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. When these materials are returned to secure storage, does that require logging?**

A *Yes. The purpose of the logging is to track both when materials are removed from secure storage, and when they are returned.*

PIN Security Requirement 29

Q 1 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 2 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 3 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.*

Q 4 January (update) 2020: Requirement 31 states that SCDs removed from service temporarily for repair, must render all keying material irrecoverable. Are there any exceptions to this?

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 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.*

Q 5 November 2020: Are SCDs used for code signing required to be PCI approved devices?

A *No. Vendor documentation may be used to validate that devices used for code signing meet the criteria for an SCD. However, the devices must be managed meeting physical security controls specified in requirements 14 and 29.*

PIN Security Requirement 32

Q 1 November 2022: What additional considerations are there for remote (non-console) administration of HSMs?

A *Remote administration of HSMs requires the following:*

- *Non-console HSM access for the purposes of management and configuration must require the use of multifactor authentication.*
- *Non-console HSM access for the purposes of management and configuration must be performed using a secure channel—e.g., TLS connection. This bullet is a best practice until 1 April 2025, after which it will be required and must be fully considered during a PCI PIN assessment.*
- *Clear-text key components and/or key shares input to or output from the HSM must be secured through dual control and split knowledge.*
- *Non-console access which may be used for the loading of clear-text private and secret key components or key shares must originate from secure cryptographic devices that are validated and approved against one of the following:*
  - *PCI PTS HSM or*
  - *FIPS 140-2 or FIPS 140-3 level 3 or higher.*
- *Non-console access used for the loading of clear-text private and secret key components or key shares must use a key-encryption key that is specific for the purposes of key transport. Use of encryption provided by a secure channel is not sufficient to meet this requirement.*

Normative Annex A – Symmetric Key Distribution Using Asymmetric Techniques

Q 1 **January (update) 2020: 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—e.g., in a key-injection facility that meets the requirements in Annex B—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, Annex A does not apply. The secure environment and operational controls are depended upon for the integrity and security of the process. 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 2 **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.

Q 3 **November 2020: The introduction to Annex A states that ANSI TR-34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport represents a methodology complaint to Annex A. Under TR-34, both the Key Distribution Host (KDH) and the Key Receiving Device (KRD) have a common relationship with a Certificate Authority. In this context, what does common relationship mean?**

A *Common relationship means the KDH and KRD are part of the same PK—i.e., the KDH and KRD are under the same Root CA.*

Q 4 **November 2020: Do non-TR-34 remote key distribution implementations require that they be implemented as part of the same PKI?**

A *Yes*

Normative Annex A-1 – Remote Key Distribution Using Asymmetric Techniques Operations

PIN Security Requirement 15

Q 1 **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 2 **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).*

Q 3 **May 2019: Requirement 18-5 in Annex A states: Key Distribution Hosts (KDHs) shall only communicate with POIs for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking. Does this requirement preclude a terminal management system (TMS) from existing on the same platform as a KDH?**

A *KDH is a functionality, and it is not intended to infer a dedicated physical platform. A TMS functionality may exist on the same physical platform as a KDH provided the TMS does not enable a successful attack vector on the KDH. Therefore, the security of the environment containing the KDH and TMS must be maintained at the level required to secure the KDH.*

Normative Annex A-2 – Certification and Registration Authority Operations

PIN Security Requirement 28

Q 1 **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 e-mail constitute a comparable procedure?**

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

PIN Security Requirement 32

Q 1 **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 2 January (update) 2020: What are the minimum criteria for construct of Certification Authority room walls for offline—e.g., root—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 3 January (update) 2020: If a caged environment is used to meet requirement 32 for an online 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 1 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 2 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 3 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.*

Q 4 December 2024: Keys loaded to POI devices for the protection of cardholder data must meet the minimum key sizes defined in Normative Annex C. If an acquirer processor or merchant (Acquiring Entity) requires its independent KIF service provider to inject the POI devices of the processor or merchant with weaker keys than prescribed, is the KIF non-compliant to the PIN Security Requirements?

A *No, provided the KIF demonstrates the ability to the assessor for the injection of appropriately strong keys per Annex C. If weak keys are being injected at the explicit request of an Acquiring Entity, the liability for those keys is on the Acquirer. The KIF must maintain documentation regarding this request by the Acquirer. Furthermore, the assessor must note in the PIN ROC any Entity for which the KIF service provider has injected cryptographic keys that are not of appropriate strength.*

PIN Security Requirement 1

Q 1 **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 2 **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 12

Q 1 **November 2020: Does the use of TLS to convey keys in a KIF from a key loading device to a POI device constitute encrypted key loading?**

A *If the origin and termination points of the TLS connection are within the secure boundaries of the source and target devices—i.e., the KLD and the POI devices—then it constitutes encrypted key loading. If any private or secret keying material is in the clear outside of the secure boundaries of the source and target devices, then it does NOT constitute encrypted key loading.*

PIN Security Requirement 13

Q 1 **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 1 **October (update) 2024: 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 (asymmetric private and symmetric keys that are stored outside of the tamper protected boundary of an SCD: i) stored at a transaction host, ii) at a KIF; or iii) in the non-secure memory of a POI device.*

Additionally, key blocks must be used when encrypted keys (asymmetric private and symmetric keys) are transported over a network connection outside of a Controlled Environment as defined in ISO 13491.

Q 2 **October 2024: POI devices may be remotely loaded. This includes, but is not limited to where they are:**

- **Already deployed**
- **Located at a warehouse or other facility awaiting deployment**
- **Located with the same facility as the key loading device, but are remote from the key loading device itself, and must be loaded over a network connection.**

What circumstances would require the use of key blocks when loading the keys?

A *Whenever the keying material travels outside of a Controlled Environment per ISO 13491-2, or a Secure Environment as defined in requirement 32-9 (for example using a VPN), the keying material must be protected in a key block using either symmetric or asymmetric methodologies.*

If the keying material stays within a Controlled or Secure Environment, then the keying material can be encrypted without the use of key blocks.

PIN Security Requirement 29

Q 1 **January (update) 2020: The introductory text to Requirement 29 in Annex B states that secure room 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 room 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 room would be the secure room used for key injection.*

Test procedures include performing a physical inspection of the storage room 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 1 **November (update) 2020: Only encrypted key loading is allowed for POI v5 or higher devices after 2023 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.*
- *Terminal Master Keys (TMKs) and initial DUKPT keys.*

Q 2 **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 32-9 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 3 **January (update) 2020: Requirement 32 stipulates that a secure 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 room 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 room 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 or wire mesh is used to enclose the top of the room—then physical barriers must be to prevent observation of clear-text components or password entry from outside the secure room.*

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 32-9 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 allow only authorized access to the facility. Facility access is managed appropriately and the KIF environment:

- *Restricts Access*
- *Restricts Observation*
- *Facilitates the effective use of motion activated CCTV systems*
- *Prevents the passing or capture of restricted materials through openings.*

Q 4 January (update) 2020: 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 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.*
- *The injection system should be far enough away from the fencing to prevent an attacker from attaching a tapping device through the fence.*

Q 5 November (update) 2020: Requirement 32-9 only prohibits clear-text key injection for POI v5 and higher devices. Is that meant to continue to permit clear-text key injection for POI v4 and earlier devices, even after the stated effective dates?

A *Yes. The injection of clear-text keys into POI v4 and earlier devices will continue to be acceptable past the January 2024 date for entities engaged in key injection on behalf of others and the January 2026 date for entities engaged in key injection of devices for which they are the processor until such time that any such device has been mandated by a payment brand to be removed from service.*

Q 6 December 2023: How does the sunrise for encrypted key loading for POI v5 and higher devices impact the deployment of software updates to my existing estate.

A *Minor updates and patches that are not compliant with the encrypted key loading sunrise may continue to be deployed after 1 Jan 2024.*

Major software updates deployed to existing estates must include injection methods that are compliant with the encrypted key loading statements in 32-9.

Q 7 **December 2023: Effective 1 January 2024, the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of POI v5 and higher devices. Subsequent to that date, only encrypted key injection shall be allowed for POI v5 and higher devices. If a KIF service provider has customers with devices that do not have software supporting encrypted key loading what are the KIF service provider's options for meeting the requirement?**

A *After the effective date, it is only permissible to use non-encrypting methods with POI v5 and higher devices for existing deployments used by pre-existing merchants/legal entities that have not yet made the requisite updates to their software to support encrypted key loading.*

The requirements of 32-9 are met if a service provider demonstrates a capability for encrypted key loading for POI v5 and higher devices when onboarding new merchants/legal entities, or when pre-existing merchants/legal entities make use of major software updates.

Furthermore, the assessor must note in the PIN ROC the PIN acquiring service providers and the associated software solution(s) for which the KIF service provider has implemented encrypted key loading and those organizations and solutions for which the KIF service provider has not.

Q 8 **December 2023: Effective 1 January 2024, the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of POI v5 and higher devices. What constitutes a new deployment? Are repairs or like-for-like replacements of previously deployed devices exempt? What about expansions to existing estates?**

A *Repair, replacement with like-for-like POI devices, and expansion of existing deployments with non-compliant solutions may continue. Existing deployments' do not include or allow for the use of plaintext key loading for terminals which are to be used by new merchants or legal entities.*

Q 9 **May 2024: Encrypted key loading is required for the injection of keys into POI v5 and higher devices. Does this preclude the conveyance of clear keys or their components over a cable directly connected from an SCD to a POI device?**

A *Yes, for secret and private keys the keying material must be encrypted from the SCD used for key loading to the target device, i.e., the POI. This applies except where delineated in other PIN Security Requirements Technical FAQs for Requirement 32.*

Q 10 **May 2024: Does the conveyance of clear text private or secret keying material, either over a physical cable or using wireless methods, from a keyboard to a KLD meet the requirement for encrypted key loading for POI v5 and higher devices?**

A *No, the use of a non-SCD keyboard for entry of clear text keying material is not allowed. Additionally, the key material must be encrypted when being transmitted from the SCD keyboard to the KLD regardless of how the devices are connected.*

Q 11 October 2024: What are the minimum physical security requirements for a KIF or production line or repair center that performs key injection functions that do not make use of clear text components?

A *A KIF/Factory/Repair Center performing unauthenticated encrypted key injection on production lines and not injecting cleartext key components satisfies this objective by providing at least a Controlled Environment as defined in ISO 13491-2 for the injection operations. A Secure Environment, as defined in requirement 32-9 is only required when injecting cleartext key values or cleartext key components. Note that a Controlled Environment still requires physical input/output control (door and access control) along with several other requirements (refer to ISO 13491-2) but does not require dual occupancy.*

POI's may also be injected using authenticated key blocks in Uncontrolled Environments (ISO 13491-2), if the systems generating the key blocks are operated in at least a Controlled Environment.