Payment Card Industry (PCI)
PTS HSM Security Requirements

Technical FAQs for use with Version 4.0

December 2021

Table of Contents

HSM Device Evaluation: *Frequently Asked Questions*

These technical FAQs provide answers to questions regarding the application of PCI's (Payment Card Industry) physical and logical HSM device security requirements as addressed in the *PCI PTS Hardware Security Module Security Requirements* manual. 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 Questions

Q 1 Typical HSM deployments include those at data centers or other secure facilities such as payment card personalizers. Are there any stipulations or restrictions by PCI on either form factors or usage scenarios?

A *PCI shall approve devices that are intended for use as HSMs in secure facilities and which meet the PCI HSM security requirements. Implementation and deployment considerations are the responsibly of the individual payment brands.*

Q 2 June 2012: What part of the HSM lifecycle does the PCI HSM standard cover?

A *The PCI HSM standard covers the lifecycle of the HSM up to the point of its first delivery to the initial point of deployment facility. Subsequent stages of the HSM's lifecycle continue to be of interest to PCI and are controlled by other PCI standards*

Q 3 December 2013: If a user has taken delivery of an HSM for which the hardware has been approved for PCI HSM, and all of the PCI HSM requirements relating to manufacturing and to delivery to the point of initial deployment have been met, but the shipped firmware/software has not been approved for PCI HSM does the HSM become PCI HSM compliant when approved firmware/software is installed or the shipped firmware/software becomes approved at a later date?

Yes, subject to the condition that the chain of custody over the HSM following its receipt at the point of initial deployment has been controlled and is auditable, for example in accordance with the requirements of PCI PIN or PCI P2PE.

The software version identifiers for the approved and non-approved firmware/software versions must be distinct, with the identifier for the approved firmware/software appearing on the PCI HSM approval. The HSM is only compliant with PCI HSM during the period that it is running firmware/software has been approved for PCI HSM.

Q 4 December 2013: Is it permissible to install firmware/software which is not PCI HSM approved on an HSM which is fully PCI HSM compliant, and for the PCI HSM compliance

of the HSM to be restored at a later date by installing an approved version of firmware/software?

A *The PCI HSM compliance of the HSM ceases when the non-approved firmware/software is installed. The PCI HSM compliance of the HSM is restored if approved firmware/software is subsequently installed, subject to the condition that the chain of custody over the HSM following its receipt at the point of initial deployment has been controlled and is auditable, for example in accordance with the requirements of PCI PIN or PCI P2PE.*

The software version identifiers for the approved and non-approved firmware/software versions must be distinct, with the identifier for the approved firmware/software appearing on the PCI HSM approval. The HSM is only compliant with PCI HSM during the period that it is running firmware/software has been approved for PCI HSM.

Q 5 September 2015: Some attacks are technically simple in that they do not require an extensive identification, like sniffing a communication on standard interfaces like USB/Ethernet between devices. How is the attack value calculation to be performed then?

A *For technically simple attacks that do not require an extensive identification, like sniffing a communication on standard interfaces like USB/Ethernet between devices, all cost factors besides time and expertise should be disregarded. Also, attack time and expertise is to be considered only for the identification of the general device setup and the property to be attacked (e.g., the interface type).*

Q 6 September 2015: In occurrences where it is necessary to return a device to the device vendor for maintenance, are there any restrictions on what must happen to the secret keys in the device?

A *When a device is returned to the vendor for maintenance, mechanisms must be in place to automatically cause the erasure of all previously loaded acquirer secret keys upon servicing the device—e.g., loading a new public RSA key causes the erasure of all previously loaded secret keys.*

Q 7 September 2015: Can a device meet the PTS HSM requirements without having an active tamper response mechanism to zeroize secret and private keys during a penetration attack?

A *No. Regardless of which modules of the PTS HSM standard the device is designed to comply with, penetration of the device must cause the automatic and immediate erasure of any secret and private keys such that it becomes infeasible to recover the keying material. Secret or private cryptographic keys that are never used to encrypt or decrypt data, or are not used for authentication are excluded from this requirement, as such keys would never be keys involved in protecting customer PINs or customer card data.*

Q 8 October 2015: Are HSMs that provide for multiple ‘virtualized’ instances operating with different keysets within a single physical HSM permitted under the PCI HSM approval process?

A *PCI does not aim to mandate or prevent any specific implementations or instantiations of HSM devices, but requires that any device that is to be advertised as PCI HSM approved meets the requirements outlined in the current version of the PCI HSM DTRs. Multiple ‘virtualized’ instances of HSMs are permitted, but must be confirmed to sufficiently mitigate attacks that aim to leak cryptographic information between such instances through both direct memory access, bypassing of hypervisor controls, and side channels such as cache timing or processor utilization.*

Q 9 June 2016: Some HSMs exist as standalone cards/components which are meant to be installed into a larger chassis/compound enclosure. Are there any special requirements which must be met for HSMs with this form factor?

A *Yes. If an HSM is meant to be installed into a chassis/compound enclosure, a mechanism must be provided to validate the hardware and firmware version of the HSM. If this mechanism requires performing a procedure to retrieve this information (I.e., via a software library function call), the procedure must only be able to so via a direct connection to the HSM module. Alternatively, a digital signature process may be used whereby the identification information can be shown to chain back to a known vendor PKI signing key.*

Q 10 November (update) 2018: Several requirements stipulate that if the device is restricted to deployment in Controlled Environments as defined in ISO 13491, then specific restrictions apply in the attack techniques that can be used. If the restrictions preclude any viable attacks for a specific requirement, how must that be presented in the evaluation report?

A *The report must present attack scenarios as stipulated in the derived test requirements. These must be presented without the restrictions of the Controlled Environment with notation highlighting the steps that are not allowed per the controlled environment restrictions. The report would indicate the attack is feasible if the device is not deployed in a Controlled Environment or a more robust Secure Environment.*

The device will be noted under both ‘Additional Information’ and within the vendor security policy posted on the PCI website that the device is restricted to use within a Controlled or a Secure Environment as defined in ISO 13491, and that usage outside of a Controlled or a Secure Environment invalidates the approval. HSMs that are PCI Approved for Controlled or Secure Environments shall not be used in Uncontrolled or Minimally controlled Environments.

Q 11 November 2021: PTS vendors are required to make all source code pertinent to Security Requirements available to the test laboratories. Multiple test requirements require the test laboratories to review that code to facilitate validation to the applicable Security Requirements. Should those code segments (snippets) be included in the reports?

A *Yes, unless stated in the test requirement that the sample is not required, the segment or snippet is considered evidence of meeting the security requirement. Code samples serve as evidence in a manner similar to the inclusion of pictures of hardware components as evidence in meeting physical requirements.*

HSM Requirement A1

Q 1 September 2015: In the event of tamper, the device must become immediately inoperable and result in the automatic and immediate erasure of any secret information that may be stored in the device, such that it becomes infeasible to recover the secret information. Guidance notes provide that secret or private keys do not need to be zeroized if either or both of the following conditions exist:

- **If any of these keys are not zeroized, then other mechanisms must exist to disable the device, and these keys must be protected in accordance with Requirement A5.**
- **The keys are never used to encrypt or decrypt data, or are not used for authentication.**

Do any other conditions apply?

A *The keys (secret or private) are never used to encrypt or decrypt other keys. Keys that can be used to download other keys to make the device operable must either be zeroized or rendered inoperable for use in downloading new keys. E.g., both symmetric KEKs used for key loading using symmetric techniques and private keys associated with key loading using asymmetric techniques. The device must enforce that tampered devices require withdrawal from use for inspection, key reloading, and re-commissioning. It is not sufficient to rely upon procedural controls for this.*

Q 2 September 2015: A device uses a key that is randomly generated internally in the secure processor to protect other keys. This key is stored in the clear and protected within a register in the same secure processor. The secure processor resides within a secure area of the device. This key is used to encrypt other keys, which are stored encrypted outside the secure processor—e.g., in flash memory that also resides within the secure area of the device. Upon tamper, the device erases this internally generated key but leaves intact the other keys encrypted by this key, which can no longer be used because the device cannot decrypt them. Under A1, must the device also zeroize these encrypted keys upon tamper?

A *The device need not zeroize these encrypted keys provided that they are encrypted using appropriate algorithms and key sizes as defined in Requirement B11.*

HSM Requirement A4

Q 1 September 2015: What standards and methods are used for measuring "electro-magnetic emissions"?

A *Vendors should take into account that EM emissions can be a risk to PIN data, and should design to address this risk. There are many methods for shielding and minimizing EM emissions. The vendor must describe to the laboratory in writing how EM emissions are addressed by the device design. The laboratory will examine evidence provided by the vendor to determine if the evidence supports the vendor's assertion. Evidence can include the device itself, design documents, third-party test results and approvals. Testing will be performed as necessary.*

HSM Requirement B1

Q 1 Does the device need to have an electronic audit record for pre-operatonal self-tests?

A *Yes. The device must include an audit record showing the self-test execution and record the result.*

HSM Requirement B4

Q 1 September 2015: What parties may possess keys used for the cryptographic authentication of firmware updates?

A *The firmware is the responsibility of the device vendor, and as such the cryptographic keys that authenticate it within the device must be held solely by the vendor or their designated agent.*

Q 2 September 2015: Firmware updates must be cryptographically authenticated, and if the authentication fails, the update is rejected and deleted. Are there any circumstances where firmware can be updated without authentication?

A *Some chipsets are not designed for firmware updates, but only to support firmware replacement. The deletion of the existing firmware and cryptographic keys during the replacement does not allow for the authentication of the new firmware to occur.*

In such cases it is acceptable to update the firmware without authentication if the process requires that the device be returned to the vendor's facilities and results in the secure zeroization of all secret and private keys contained within the device.

Q 3 September 2015: If a device supports firmware updates, the device must cryptographically authenticate the firmware, and if the firmware is not confirmed, the firmware update must be rejected and deleted. Can a device completely load new firmware before checking its authenticity and overwrite its primary copy of existing authenticated code if it retains a secure backup copy of the existing authenticated code?

A *Yes, provided the following is true:*

- *The new code is cryptographically authenticated prior to execution.*
- *If the new code fails authentication, the backup copy of code is cryptographically authenticated, and if the backup copy is successfully authenticated, the device boots from the backup copy and the backup is then used to overwrite the new code that failed authentication.*
- *If both firmware versions fail authentication, the device fails in a secure manner.*

HSM Requirement B7

Q 1 September 2015: Is it acceptable to XOR key components during key loading to satisfy the authentication requirements of B7?

- *The XOR of key components alone is not enough to constitute authentication. Some type of authentication of the users that use the key loading function, or authentication of the key-loading command is required.*

Q 2 September 2015: For devices that require the use of authentication data to access sensitive functions, and the authentication data are static, can the authentication data be sent with the device?

A *The authentication data can be sent with the device only when the authentication data is in tamper-evident packaging, such as the use of PIN mailers. Otherwise separate communication channels must be used with pre-designated recipients.*

Q 3 September 2015: Plain-text secret or private keys and their components may be injected into a HSM using a key loader (which has to be some type of secure cryptographic device). Are there any restrictions on loading keys via this methodology?

A *Yes, the loading of plain-text secret or private keys and their components using a key-loader device is restricted to a controlled environment.*

Q 4 September 2015: Devices may have functions for zeroizing secret and private keys in the device. Are these functions considered sensitive services that require authentication?

A *Yes, the intentional zeroization of secret or private keys in a non-tamper event is the execution of functions that are not available during normal use. This requires authentication consistent with the implementations of other sensitive services, such as the use of PINs/passphrases. If implemented, the device must force the authentication values to be changed from default values upon configuration of the device. The authentication mechanism may optionally employ dual control techniques.*

HSM Requirement B11

Q 1 Are HSMs allowed to have keys that are not unique per device?

A *Yes, but only for load balancing and disaster recovery purposes.*

Q 2 September 2015: Is it acceptable for a device to have the ability to use Master Keys as both key-encryption keys for session key and as fixed keys—i.e., the Master Key could be used to encrypt PIN blocks and to decrypt session keys?

A *No. A key must be used for one purpose only as mandated in ANSI X9.24 and ISO 11568.*

Q 3 September 2015: Is it acceptable to use the same authentication technique for loading both cryptographic keys and firmware?

A *The technique may be the same, but the secrets used for authentication must be different. Example: If RSA signatures are used, the RSA private key used to sign cryptographic keys for loading must be different from the private key used to sign firmware.*

Q 4 September 2015: Is it acceptable to use TDES ECB mode encryption for session keys when using the Master Key/session key technique?

A *Yes. TDES ECB mode can be used to encrypt session keys.*

Q 5 September 2015: Is it acceptable to load double-length 128-bit TDES key components into a device in smaller bit-values (e.g., two 64-bit parts held by key custodian 1 and two 64-bit parts held by key custodian 2)?

A *Yes, provided the 128-bit cryptographic TDES keys (and key components) are generated and managed as full double-length 128 bit TDES keys during their entire life cycle in accordance with ANSI X9.24 and ISO 11568.*

For example, it would be acceptable to generate a full-length 128-bit TDES key component, but load it into the device as two 64-bit component halves.

It would not be acceptable to generate 64 bit keys or key components separately, and then concatenate them for use as a double length key after generation.

If key-check values are used to ensure key integrity, they must be calculated over the entire 128-bit key component or the resultant 128-bit key, but never on a portion of the key or key component. In addition, the resultant key inside the device must be recombined in accordance with PCI requirements and ANSI/ISO standards. Similarly for triple-length keys, the entire 192 bit key component or the resultant 192-bit key must be used to calculate the key-check values.

Q 6 September 2015: Under what conditions is it acceptable for a device to allow single component plain-text cryptographic keys to be loaded via a keypad?

A *None. A device must not accept entry of single component plain-text cryptographic keys via a keypad. Full-length key components and encrypted keys may be loaded via a keypad if the requirements for sensitive functions are met.*

Q 7 September 2015: TR-31 defines three keys. A key block protection key (KBPK), a key block encryption key (KBEK) and a key block MAC key (KBMK). The KBPK is used to calculate the KBEK and the KBMK. Can the KBPK be used for any other purpose?

A *No, in order to meet the requirement that a key is used only for a single purpose as defined in ANSI X9.24, the key block protection key is only used to calculate the KBEK and the KBMK, and is not used for any other purpose. Only the KBPK is used to generate the KBEK and the KBMK key; no other key is used for this purpose.*

Q 8 September 2015: The Guidance for DTR B11 states, "A device may include more than one compliant key-exchange and storage scheme. This does not imply that the device must enforce TR-31 or an equivalent scheme, but it must be capable of implementing such a scheme as a configuration option." If the use of TR-31 as the key-exchange mechanism is optional, must there be an explicit device configuration change to enable/disable TR-31 as the "active" key-exchange scheme?

A *Yes an explicit configuration change is required. The change is considered a sensitive service and must meet the requirements of B7, protection of sensitive services.*

Q 9 September 2015: Are there any restrictions on how the master key is loaded into the device?

A *The initial master key (MK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., a keypad, IC cards, key-loading device, etc. Subsequent loading of the master key may use asymmetric techniques, manual techniques, self-generation, etc. Keys are not allowed to be reloaded by any methodology in the event of a compromised device, which must be withdrawn from use.*

Q 10 May (update) 2018: Can secret keys or their components be used for other purposes such as passwords/authentication codes to enable the use of sensitive services?

A *No. The use of secret keys or their components for other purposes violates the requirement that keys be used for their sole intended purpose, e.g., key encipherment or PIN encipherment, etc.*

Q 11 September 2015: The PCI PIN Security Requirements stipulate that any cryptographic device used in connection with the acquisition of PIN data that is removed from service must have all keys stored within the device destroyed that have been used (or potentially could be) for any cryptographic purpose. If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys. Does this apply only to symmetric keys?

A *No, this applies to any secret or private key used by the device for PIN encipherment, firmware validation, display prompt control or the protection of any of those same keys during loading to the device or storage within the device, including private keys used in connection with remote key distribution using asymmetric techniques. This requirement applies to both vendor and acquirer-originated or controlled keys. This does not include public keys present or used by the device.*

The vendor must provide decommissioning instructions and associated mechanisms for rendering all such keys non-recoverable to an adversary that are verifiable by the evaluation laboratory. These techniques include, but are not limited to:

- *Specific menu commands to zeroize stored keys*
- *Inducement of a tamper event to zeroize those keys*

- *Encryption by a key of equal or greater strength that is itself zeroized, i.e., only cryptograms of the protected keys are recoverable.*

Q 12 September 2020: Devices must support the ANSI TR-31 key-derivation methodology for TDES keys, and for AES keys must support either the TR-31 methodology or the ISO 20038 methodology. In either case, equivalent methods can be used where subject to an independent expert review and said review is publicly available as described. What characteristics enforced in TR-31 and ISO 20038 must be considered in determining equivalence?

A *"Equivalency" must be demonstrated in the context of security proofs. The equivalent method must provably accomplish the functions of key integrity, restricting key usage, preventing key reuse, and the secrecy of keys. Specifically, an equivalent key block scheme must minimally offer the following properties:*

a) *It must prevent the loading of PIN, MAC, and/or Data keys - or any keys used to manage these within the key hierarchy - from being used for another purpose. IPEK, KEKs, and derivation keys must be uniquely identified where supported.*

b) *It must prevent the determination of key length for variable length keys.*

c) *It must ensure that the key can only be used for a specific algorithm (such as TDES or AES, but not both).*

d) *It must ensure a modified key or key block can be rejected prior to use, regardless of the utility of the key after modification. Modification includes changing any bits of the key, as well as the reordering or manipulation of individual single DES keys within a TDES key block.*

e) *Where different key block formats are supported, with some providing the above protections and some not, it must be humanly readable from the key block prior to loading/use which format is implemented. E.g., by looking at the commands sent to the device.*

f) *It must support all symmetric algorithms implemented by the device(s) that are to use the key blocks.*

g) *Where asymmetric algorithms are supported, the algorithm type, padding and signature formats must be identified in the key block.*

h) *It must use NIST approved modes of operation, with separate keys used for confidentially and authenticity. Any keys used must not be related in a reversible way.*

The equivalent block may optionally support other characteristics such as:

i. *A key version number that prevents the use of older or expired keys.*

ii. *Support for key 'direction' (uni-directional keys) so that a MAC key may be identified as 'verify only', or a data key as 'encrypt only'.*

iii. *Support for key purposes other than PIN, MAC, and Data.*

iv. *Support for both TDES and AES (where devices implementing the key blocks only support one of these algorithms – transitional only – new devices must support AES).*

v. *To implement confidentiality controls over any key metadata other than the key length.*

vi. *Support for asymmetric algorithms.*

Q 13 September 2020: HSMs are required to support key blocks using the ASC X9 TR-31 key-derivation methodology for TDES keys, and for AES keys must support either the TR-31

methodology and/or the ISO 20038 methodology. TR-31 and ISO 20038 are methods to package keys (the key blocks) for conveyance or storage, but they use symmetric mechanisms for that and for key conveyance require a symmetric key exchange key that is pre-shared for use as the key block protection key. Where a symmetric key is not previously established with a POI device for remote key distribution, and asymmetric methods will be used, is it required to support a key block methodology?

A *Yes. A method such as ASC X9 TR 34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport must be used. Under TR-34, similar to TR-31 and ISO 20038, the Key Block consists of three parts:*

- *The Key Block Header (KBH) which contains attribute information about the Key and the Key Block*
- *The confidential data that is being exchanged/stored*
- *The Key Block Binding Method*

However, TR-34 uses asymmetric methods for the Key Block Binding Method, instead of the symmetric methods used in TR-31 or ISO 20038 which require that a symmetric key was previously exchanged between the POI device and the KDH.

Q 14 December 2020: Devices must support the ANSI TR-31 key-derivation methodology for TDES keys, and for AES keys must support either the TR-31 methodology or the ISO 20038 methodology. In either case, equivalent methods can be used where subject to an independent expert review and said review is publicly available for peer review. What constitutes publicly available?

A *Publicly available" means posted in a forum or otherwise published such that it is available for peer review for the time frame for which the solution is relied upon.*

Any proprietary posting that would require peers to know in advance where to find it is not in the spirit of "publicly available"; however, if a notice is given in a cryptographic forum or publication that provides a link to the proprietary posting, that suffices.

HSM Requirement B13

Q 1 September 2015: Is it acceptable for a PIN-encryption key to be used as a key-encrypting key, or for a key-encrypting key to be used as a PIN-encrypting key?

A *No. A key must be used for one purpose only as mandated by ANSI X9.24 and ISO 11568-3.*

Q 2 September 2015: Can a device use a key-encrypting key to encrypt or decrypt key-tag information along with a key?

A *Yes, associated key-tag information such as the algorithm, key expiration, usage, or key MAC may be encrypted or decrypted along with the key using a key-encrypting key. The key and its tag are bound together using a chaining mode of encipherment as defined in IS0 10116.*

HSM Requirement B18

Q 1 September 2015: The operating system of the device must contain only necessary components and must be configured securely and run with least privilege. What is considered an "operating system" for PCI purposes?

A *In the scope of PCI PTS, any underlying software providing services for code running in the device is considered part of the operating system. Examples of such services include: system initialization and boot, hardware abstraction layers, memory management, multitasking, synchronization primitives, file systems, device drivers and networking stacks. Services that provide security or may impact security are, in addition, considered firmware.*
Operating systems may range from hardware abstraction layer libraries and embedded micro-kernels, to complex multi-user operating systems.

HSM Requirement B20

Q 1 February 2020: Can an HSM operating in PCI-mode support known weak cryptographic algorithms/key sizes not otherwise allowable when used for EMV card personalization?

Yes, when used for EMV card personalization an HSM when operating in PCI mode may support:

- *SHA-1*
- *RSA keys less than 2048*

This must result in a distinct firmware version and any other usage beyond card personalization invalidates the approval.

All other usage must meet the requirements for minimum key sizes and parameters for algorithm(s) that are stipulated in Appendix D of the PCI HSM Derived Test Requirements, the usage of SHA-2 or higher for a hashing algorithm and only recognized format-preserving Feistel-based Encryption Modes (FFX), if FPE is supported

HSM Requirement C1

Q 1 ISO 9564 and requirement C1 require that the HSM's security policy enforce the prohibition of the translation of PIN block formats from ISO format 0 to IS0 format 1. Are there any circumstances where it is permitted that HSMs allow the translation of PIN blocks from ISO format 0 to ISO format 1?

A *Yes, if a unique session key is used for every ISO format 1 PIN block, and the key uniqueness is guaranteed by the functionality of the HSM and is not reliant upon APIs exercised by the host application.*

Q 2 September (update) 2015: Are HSMs allowed to support non-ISO PIN block formats and non-ISO algorithms?

A *Yes; however, the HSM must provide functionality to enforce a policy that meets B15:*

In addition, the vendor must provide the rationale for the use of any other algorithms used.

Q 3 May (update) 2018: Is the device allowed to share PCI relevant keys and passwords/authentication codes between PCI approved mode of operation and non-PCI approved mode of operation?

A *No. The device must either enforce separation of all PCI relevant keys and passwords/authentication codes between the two modes or the device must zeroize all PCI relevant keys and passwords/authentication codes when switching between modes except as follows.*

If the device includes an internally generated hardware key, for example inside a secure microcontroller that can't be updated or output, it does not need to be zeroized and may be shared between the two modes if its only use is for internal storage protection.

Q 4 September 2015: Is there any impact on the device's approval if the laboratory evaluated security policy is changed by the vendor?

A *The content of the security policy is part of the evaluation of a device by the laboratory and is an integral input upon which the approval of a device is based. Deployers rely on the security policy in order to ensure that they do not breach the conditions of a device's approval. Any change to the security policy which impacts on the security requirements of the device must be evaluated in order for the device to remain approved. Additionally, any change to the functionality offered by the device impacting information required to be contained in the security policy must be reflected in an update to the listed security policy document.*

Depending on the nature of the changes, this may be reflected in updates (e.g., appendices) to an existing security policy, or as additional security policies posted to the website. In all cases, all approved product versions must be addressed in security policies posted to the PCI website.

Q 5 May 2018: The PCI PTS Lab Requirements prohibit a PTS lab from creating any vendor-documentation. Are there any scenarios where a PTS lab may assist a vendor in creating documentation?

A *In some cases, a PTS vendor may revise a Security Policy for grammar, formatting, or spelling edits for a device under evaluation. which requires grammar, formatting, or spelling edits. to be submitted to PCI to place on the portal. In this case, the PTS lab performing the evaluation This may be done to assist the vendor in by editing the Security Policy to creating a document sufficient to be submitted to PCI. In this case, the PTS lab will provide the following as part of the evaluation report submission:*

- A track-changed/redlined version of the edited Security Policy, showing the original text created by the vendor as well as the updated text
- *A clean copy of the edited Security Policy for posting.*

HSM Requirement L2

Q 1 September 2015: Many devices are designed so that third parties can create and load applications. Vendors often support this by providing third parties the tools needed to create and load applications. How can a vendor ensure that the application will not need to be controlled by the vendor?

A *If applications are not considered firmware, they do not need to be controlled by the vendor. The device design must prevent applications from impacting functions and features governed by the requirements. Examples of functions that must not be influenced by "non-firmware" applications include: key management (key selection, key authentication, key generation, key loading, etc.), self-tests, time between PIN block encryptions, access to sensitive services, limits on sensitive services, firmware update and authentication, tamper response, etc.*