Payment Card Industry (PCI)
PTS HSM Security Requirements

Technical FAQs for use with Version 3.0

November 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 **October 2011: Some requirements are derived from requirements in Federal Information Processing Standard 140-2 (FIPS 140-2). These requirements are identified with an asterisk (*) in the security requirements number column. How much reliance may an evaluator place upon work performed under FIPS 140-2?**

A *Evaluations performed under the FIPS 140-2 program that resulted in a FIPS 140-2 certification may be considered in a PCI HSM evaluation. In order to do so, the PCI evaluating laboratory must have access to the prior evaluation report(s) under the FIPS 140-2 program. The evaluator then will establish:*

- *The HSM components that were evaluated;*
- *The security level of the evaluation;*
- *That the existing FIPS certification covers the full HSM functionality for all the related requirements.*

In all cases, regardless of any prior work, the evaluating lab is responsible for performing the degree of work necessary to ensure the compliance of the device under evaluation to the requirements.

Q 3 **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 4 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 5 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 6 September 2015: When is an "N/A" response to a requirement acceptable?

A *An "N/A" response is acceptable in two cases: First, if compliance is achieved by meeting another requirement option, if one exists. Second, if the characteristics governed by the requirement are absent in the device. The evaluation laboratory will verify that all responses are appropriate.*

Q 7 May (update) 2018: What is the definition of "Secret Information?"

A *"Secret information" is any cryptographic keys or passwords/authentication codes that the device relies on to maintain security characteristics governed by PCI requirements.*

Q 8 September 2015: Some components of a device may include cryptographic keys that cannot be erased. Are there any instances when this would be acceptable? See Requirements A1 and A5.

A *Cryptographic keys that are never used to encrypt or decrypt data; or are not used for authentication, do not need to be considered secret data, and therefore do not need to be erased.*

Q 9 September 2015: What is a "Delta"

Revisions to approved devices are termed "deltas." Delta reviews involve the laboratory assessing the changes based on the current major version (e.g., 1.x, 2.x, etc.) of the requirements that were used for the approval of the device. Examples of deltas include:

- *Revisions to existing firmware or hardware on existing approved devices to add or modify functionality*
- *Maintenance fixes on devices that have expired and are no longer approved for new deployments*
- *The porting of a new set of firmware to an existing approved device.*

Q 10 September 2015: Does the device have to show the version numbers of the hardware, firmware and Application?

A *The device must show the version numbers of hardware and firmware like they have been approved and they are shown in the list of approved devices. The hardware number must be shown on a label attached to the device. The firmware and application version numbers, and optionally the hardware version number, must be shown on a display or otherwise made available upon request.*

Q 11 September 2015: Is it acceptable to make changes to an approved device's hardware or firmware and keep the existing version #s?

A *No. Any hardware changes to an approved device that has been deployed must result in a new hardware version #. Any firmware changes to an approved device must result in a new firmware version. 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 use of variable characters shall be validated by the test laboratory so as to not impact security. The use of variable characters is appropriate to delineate differences such as country usage code, customer code, communication interface, device color, etc.*

Q 12 September 2015: When submitting hardware and/or firmware changes on existing approved devices, must a vendor submit the device to the same lab as the one that did the initial evaluation?

A *Vendors may select a different lab then the lab that was used to perform the initial evaluation. However, the subsequent lab is free to determine the level of reliance they wish to place upon the prior lab's work, which may result in additional work than would otherwise be necessary. For Version 2 or higher reports, the delta lab or the final form factor lab shall have access to the prior lab's report(s), including any delta reports subsequent to the original evaluation. If those reports are not available, the delta lab or final form factor lab shall decline the engagement or else must complete a full evaluation of the device.*

Q 13 September 2015: Are PC-based instruments like protocol sniffers, USB attached oscilloscope adapters and graphical multimeters, etc. considered standard or specialized equipment.

A *PC-based instrument like those mentioned above shall be considered standard equipment, especially if they do not require dedicated hardware or adapters.*

Q 14 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 15 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 16 September 2015: Security requirements are normally available for a four-year period from date of publication for new evaluations of products. Products are approved until six years after the retirement/expiration of the version of security requirements against which they were approved. This results in approvals that are a minimum of six years and a maximum of ten years, depending on the timeframe in which the approval occurs in relation to the life cycle of the applicable security requirements. Modifications for approved devices, termed "deltas," can occur at any time during the product's approval.

Can products for which the approval has expired undergo deltas?

A *Yes. Vendors may need to make maintenance fixes to devices that the vendor has already sold, but must still provide support for. In addition, vendors may wish to port updated versions of firmware that were approved against newer security requirements to products for which the approval has expired. This may occur because customers of a vendor wish to standardize their deployment against a given version of firmware and/or to add functionality to that device.*

Q 17 September 2015: Technical FAQs are updated on a regular basis, and add clarifications for the application of defined security requirements. Are new FAQs applicable to devices that are currently in evaluation? Furthermore, must FAQs that were not in existence at the time of the original evaluation be considered in subsequent delta evaluations?

A *Yes. Technical FAQs not only add clarifications to requirements in order to provide a consistent and level playing field in the applications of those requirements, but may also address new security threats that have arisen. As such, technical FAQs are generally effective immediately upon publication.*

The intent is not to cause a device in evaluation to fail if otherwise it would not unless known exploitations exist. Unless such an exploitation exists, a product currently in evaluation will generally not be subject to new FAQs issued during the product's evaluation. This does not exempt a product from the applicability of the FAQ if the product must be reworked and resubmitted at a later date because of other issues that cause it to fail the evaluation.)

Devices undergoing delta evaluations must take into account the current FAQs of the associated major version of security requirements only for the security requirement(s) that are impacted by the delta change. For example, if a change impacts compliance with requirements B1 and B4, only the current FAQs associated with B1 and B4 must be taken into account as part of the delta.

Furthermore, it is not sufficient for the lab to determine that the change does not lessen the security of the device. Due to the evolution of threats and attack techniques from the time of the original evaluation (which may have occurred many years earlier) the lab must determine that the device still meets the relevant security requirements impacted by the change, given the changes in attack vectors. This is because whether deltas are done to enhance or fix functionality or for other purposes, the end result is to extend the life of the device in the marketplace.

In all cases, the evaluation laboratory must advise PCI SSC of the circumstances, and PCI SSC will make the final decision based upon the circumstances. Additionally, for both new and delta evaluations, the laboratory will also state in their submission the version of the security requirements used in the evaluations, as well as the publication date of the technical FAQs used.

Q 18 September 2015: The program manual stipulates that "Vendors or other third parties licensing approved products from other vendors to market or distribute under their own names are not required to pay a new evaluation fee if the only change is to the name plate. If firmware and/or hardware changes are made that require a PCI-recognized test laboratory to evaluate the changes for potential security impact, then the licensee shall be required to pay the new evaluation fee. In all cases the licensed device will receive a new approval number and the licensee vendor or third party shall be billed the annual listing fee for each such approval."

What are additional considerations for a third party to license an approved product from a vendor, whereby the third party wants to distribute it as their own product?

A *There are several additional considerations:*

1. *The licensee vendor cannot directly make the request. The licensor vendor must make the request on their behalf.*
2. *All such requests must be received by PCI SSC as a delta letter from one of the PCI SSC PTS recognized laboratories. If the only change is to the nameplate of the product, there is not any new evaluation fee, but as noted above, there will be an annual listing fee.*
3. *There is not any requirement for the licensee's version of the product to reference or list the original vendor.*
4. *Products may be licensed from another vendor even if the version of the security requirements against which the original product was approved is retired from use for new evaluations, as long as the approval has not expired.*
5. *As noted, licensed products requiring physical and/or logical changes will incur a new evaluation fee. However, as long as the original vendor continues the manufacture of the device on behalf of the licensee vendor, the licensed product can be evaluated against the security requirement's version against which the original product was evaluated and approved, even though those requirements may be expired for new approvals.*
6. *If the licensee vendor wishes to directly manufacture the licensed product, or have a third party other than the original vendor manufacture the licensed product on their behalf, the product must be reassessed as a new evaluation against the current version of security requirements—unless the licensor vendor can demonstrate that it retains both the intellectual property and engineering control. This is due to the potential for changes in plastics, etc. that may impact the security of the device.*

Vendors seeking multiple separate approval listings for their own products are subject to the same conditions for items 2, 3, 4 and 5 as applicable.

Q 19 September 2015: For attack potential calculations, information is classified as Public, Restricted or Sensitive. What are examples of each?

A *Information is considered Public if it can be easily obtained from the Internet or is provided without any control mechanisms. Examples include open protocol specifications and electronic component datasheets. Information with automated access controls mechanisms (such as online account subscription) without human intervention classifies as Public. Restricted information is distributed upon request and is subject to human-based control mechanisms. Examples of Restricted information are mechanical drawings for OEM device integration, external command API specifications, partial Gerber files, and secure processor datasheets available under NDA. Sensitive information is not intended to be distributed to external entities and is obtained by means such as "social engineering" theft or coercion. Typical examples are device schematics and firmware source code.*

Q 20 September 2015: For attack-potential calculations, if the same equipment used for the identification phase can be reused for exploitation, the equipment cannot be accounted for twice, but instead must be divided by two and spread equally over the two phases. Does a similar rational apply where parts are reused?

A *No. While equipment readily lends itself to reuse for each exploitation, parts are typically a one-time use for each exploitation. Each exploitation should have the same attack potential value. Accounting for parts that are reused in the initial exploitation only in the Identification phase, or even splitting between the Identification and Exploitation phases, will result in the initial exploitation having a lower attack-potential value than the actual subsequent exploitations. Therefore, parts used during the Identification phase that can be used in the initial exploitation must be counted fully in the Exploitation phase to equalize the attack-potential value across all exploitations. If it is not readily reusable (the part once used in installation becomes unusable for exploitation because, for example, it is glued with epoxy and difficult to remove), it can be accounted for twice—once in the Identification phase and again in the Exploitation phase.*

Q 21 September 2015: Hashing algorithms are an integral part of digital signatures. Digital signatures are frequently used in connection with meeting a number of security requirements, including those related to firmware updates, display prompt control, and remote key distribution. With the release of PCI PTS HSM v2, SHA-1 was explicitly prohibited for use, and only SHA-2 was allowed. Does this prohibition apply only to the signatures of the data that is being updated and to only the device's specific individual certificates, or to all certificates used by the device?

A *Hashing algorithms must possess two properties in order to be considered secure. First, they must be one way such that it is easy to compute the hash value, but given the hash value, it is infeasible to reproduce the original unhashed value. Second, they must be collision-free, i.e., it is not possible to find two different messages (sets of data) that hash to the same hash value.*
In recent years, successful attacks have been developed against two popular hashing algorithms. First MD-5 and then SHA-1 attacks have been successfully developed to make these algorithms non-collision-free. These attacks allow for the spoofing of authentication and the ability to produce counterfeit credentials.

Except as noted below, the use of SHA-1 is prohibited for all digital signatures used on the device that are used in connection with meeting PCI security requirements. This includes certificates used by the device that are non-device-specific that are part of a vendor PKI, up to and including a vendor root certificate.

The only exception to this is that the initial code on ROM that initiates upon the device start may authenticate itself using SHA-1, but all subsequent code must be authenticated using SHA-2.

Q 22 September 2015: Vendors may provide application toolkits for third parties to develop applications that cannot impact any of the functionality needed to comply with PCI requirements. Can a vendor provide a toolkit that allows third parties to implement applications that supplant the cryptographic processing of PCI Payment Brand PIN or Card data that is provided for in the approved vendor firmware?

A *No, the addition of applications that replace or disable the PCI evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to PTS HSM Security Requirements and listed as such in the approval listings. Specifically, those applications must be validated to ensure that:*

- *It cannot adversely affect the security features of the product that are relevant to the PCI HSM approval.*
- *It cannot modify any of the cryptographic functionality of the HSM or introduce new primitive cryptographic functionality. However, new composite functionality that builds on existing primitives is permitted.*
- *The application is strongly authenticated to the HSM secure controller by digital signature.*
- *The application can only work on the keys it alone manages and cannot affect or see any other keys.*

A mechanism must exist to display the application version upon request.

The vendor must provide clear security guidance for the development and implementation of the aforementioned additional applications. This guidance at a minimum must define procedural controls to ensure that the applications are properly reviewed, tested and authorized.

Applications, in this context, are functional entities that execute within the secure boundary of the HSM and may or may not provide services external to the HSM. Applications are typically processes or tasks that execute under the control of an Operating System (OS) or software executive routine.

Q 23 September 2015: In the approval listing, the vendor must provide via the evaluation lab pictures detailing all security relevant components of the approved device. These pictures are then placed on the PCI website as part of the approval listing. Are there any other stipulations?

A *Yes, at least one of the pictures must fulfill the requirement that the hardware version number must be shown on a label attached to the device. Note that for devices with multiple approved hardware versions, only one such illustration is necessary to facilitate purchasers of these devices recognizing how to determine the approved version(s).*

Q 24 September 2015: What are the algorithms and associated minimum key lengths that are acceptable for use with the default operation of any open protocol used in a HSM?

A *The minimum requirements for cryptographic algorithms used to provide security to any confidential data, including data transmitted using open protocols, is specified in DTR B11. Only TDES, RSA, ECC, DSA, and AES are acceptable for encryption or signing operations. SHA256 or above may also be used for hashing purposes.*

Q 25 September 2015: Vendors are allowed to use a combination of fixed and variable alphanumeric characters in device hardware and firmware version identifiers, provided that variable characters are not used for any physical or logical device characteristics that impact security. Can variables be used as part of the model name?

A *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 in both the evaluation report and for display on the approval listing.*

Q 26 September 2015: SHA-1 is prohibited for use in conjunction with digital signatures. Is SHA-1 prohibited for other usages?

A *SHA-2 or higher is recommended for other usages, but SHA-1 may be used in conjunction with the generation of HMAC values and surrogate PANs (with salt), for deriving keys using key derivation functions (i.e., KDFs) and random number generation. Where applicable, appropriate key length minimums as delineated in the Derived Test Requirements are also required.*

Q 27 September 2015: When assessing a device for a delta review, is it the number of changes or the number of types of changes that determine whether a delta is acceptable. For example, a vendor makes a change to the tamper grids and signal routing on six PCBs within a device. According to the delta scoping guidance in the program manual, the inclusion of four or more hardware change types as categorized in the program guide in a single delta submission for a previously approved PTS device may effectively represent a new device and should be subject to its own full assessment against the latest version of the current PTS Standard. Does such a change as described count as six changes or as a single change since they are all of the same change 'type' according to the guidance?

A *The delta scoping guide states that it is the number of types of identified changes. For the example above, that would constitute one change and not six. This meets the criteria for a delta.*

Q 28 September 2015: If a device is submitted that has internal hardware changes sufficient to require a new evaluation, but does not have any external changes, can the device still be submitted as a delta?

A *No. Even though the external appearance is identical, the degree of changes made internally requires that the device receive a full evaluation against a current requirements version available for use in new evaluations and if the evaluation is successful, it will result in a new approval number. Furthermore, while the new device will have a different hardware version then the existing device, and if the firmware is modified, a different firmware version, it is also required to have a new model name/number. This is to prevent confusion in the market, especially if issues arise subsequent to deployment impacting only one of the approvals, but not the other(s).*

Q 29 September 2015: If an existing approved device undergoes a hardware change that does not impact any of the internal components but impacts the appearance of the device, i.e., the only change is to the exterior of the device, can that change be treated as a delta?

A *Yes, such changes in casing plastics that result in a change in the device's look and feel is a permitted hardware type change under the delta guidance provided the amended device remains consistent to the device's original form factor. The change must result in a new hardware version number and a change in the model identifier.*

Q 30 September 2015: Can an approved product change the entire operating system and the change is treated as a delta e.g., from a proprietary system to a Linux based system?

A *In general, any change in firmware is permitted as a delta. However, completely changing the OS must be treated as a new evaluation. The change must also result in a new firmware version number and a change in the model identifier.*

Q 31 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 32 September 2015: Vendors are allowed to make revisions to approved devices, provided the changes are evaluated by an approved lab. What limits are placed on the number and type of changes that are allowed?

A *The large number of possible changes and their impacts cannot be determined in advance. Changes will be assessed on a case-by-case basis. Vendors should contact one of the recognized laboratories for guidance. Laboratories will consult with PCI on an as needed basis to determine if a change is too great to be addressed under the delta process. The laboratories will determine whether the change impacts security. In all cases, changes that impact security require an assessment that must be presented in the delta report. At a minimum, for a given change type, all requirements identified in the Delta Evaluations – Scoping Guidance of the PCI PIN Transaction Security Device Testing and Approval Program Guide must be assessed for security impact. A rationale must be presented in the delta report for each change that is determined to not have a security impact.*

Q 33 September 2015: If the firmware is composed of independent blocks (e.g. bootloader, main firmware, kernel), how should the firmware version number be managed?

A *The displayed firmware version number must represent all firmware in the device.*

- *If firmware blocks have independent version numbers then the version number display should include the version number of each firmware block.*
- *If a single version number is used, then a documented process must be used to ensure the single version number is updated whenever changes are made to any of the firmware blocks in the device.*

Q 34 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 35 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 36 September 2016: The program manual states that hardware and firmware version number identifiers may consist of a combination of fixed and variable alphanumeric characters, whereby a lowercase "x" is used by PCI to designate all variable fields. The "x" represents fields that the vendor can change at any time to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device color, etc. What are examples of options that cannot be addressed by use of a variable field, but must be addressed by a fixed character?

A *Options that cannot be a variable character include those that directly pertain to meeting security requirements. Examples include remote administration, KLD, privacy shield, FIPS mode or PCI mode support. If wildcards are used, the specific configurations validated by the PTS Recognized Lab must be explicitly noted on the approval.*

In addition, all wildcard options, both security and non-security relevant, must be clearly defined and documented as to the options available and their function in both the evaluation report and in the security policy.

Q 37 February 2017: Vendors may make devices that are only intended to be sold and/or manufactured by other vendors. Can devices such as these be evaluated and listed, even though the original vendor may never directly sell these devices?

A *Yes, these devices can be evaluated and listed as long as the following criteria is met:*

The device must be fully capable of performing its intended functionality for the approval class it is evaluated against and can be sold as is as a fully functional product. This does not preclude the device requiring additional software such as payment applications, but the firmware of the device must meet all applicable requirements.

The device must have its own evaluation and product listing

Each of the 2nd vendors that use the device design and/or manufacture the device must have their own full evaluation (NOT A DELTA) and separate listing.

Devices that require additional hardware and/or firmware to operate (such as individual components) would not be allowed to be assessed. Those components must be integrated into a device design that meets the required PTS (HSM or POI) requirements.

Q 38 **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 39 **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 40 **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 41 **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 A5

Q 1 September 2015: Does "The keys resident in the device, *if determined*..." mean plain-text keys or does it include encrypted keys as well.

A *The requirement is referring to plain-text keys.*

HSM Requirement B1

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

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

Q 2 September 2015: What is required to meet B1?

A The device must perform an internal self-test automatically at least once every day, in addition to at power-up. Firmware integrity tests may use techniques such as SHA-2 or equivalent. Authenticity testing must use cryptographic methods (MACs, digital signature or encryption). The hash must either be cryptographically protected using a key (e.g., HMAC-SHA-2) or physically protected equivalent to a secret key. LRC, CRC and other non-cryptographic methods and weak cryptographic methods (e.g., SHA-1, MD5) are not allowed as the primary mechanisms for either authentication or integrity checking.

Q 3 September 2015: Is it acceptable to perform a self-test after several minutes of inactivity rather than once every 24 hours?

A *Yes, as long as it is 24 hours or less. Note that the power-up self-tests are still required.*

Q 4 **September 2015: B1 requires that firmware integrity and authenticity be tested every 24 hours. Some firmware, such as a boot block, is rarely executed. For such firmware, is it acceptable to perform an integrity and authenticity check prior to execution, rather than every 24 hours?**

A *Yes, it is acceptable to test such firmware immediately prior to each execution rather than once every 24 hours. However, note that all firmware must additionally be checked as part of the self-test performed at startup.*

HSM Requirement B2

Q 1 **September 2015: The device's functionality must not be influenced by logical anomalies. This includes assessment of the device's interfaces and associated communication methods. What type of evidentiary matter should a vendor provide a lab to support this assessment?**

A *The vendor shall provide evidentiary matter providing details on internal testing including, but not limited to, the following:*

- *Source code reviews targeting specific relevant security–critical functionalities*
- *Vulnerability analysis; that includes gathering and considering evidence necessary to perform practical testing*
- *Penetration testing to validate the robustness of the device to protect against feasible attacks by addressing known attack methods. For example (but not restricted to) fuzzing; using appropriate tools and techniques*
- *Audits of relevant existing test evidence, which may be utilized where appropriate, by giving justifications for validity of evidence and test methodologies overall.*

The laboratory shall determine the veracity of the material provided to determine the degree of reliance that may be placed upon the evidence, and where necessary, the laboratory shall extend the testing

HSM Requirement B3

Q 1 **September 2015: What is considered "firmware"? (OS, EPROM code, DLL's, parameter files, applications, kernel code)?**

A *Firmware is considered to be any code within the device that provides security protections needed to comply with PCI HSM requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI HSM requirements.*

Q 2 **September 2015: What methods are acceptable to "certify" firmware?**

A *"Certify firmware" refers to self-certification. This requirement, in essence, requires the vendor to have implemented and to use internal quality control and change control systems. With these systems in place, the vendor is in control of the code and can attest to the fact that the code is free of hidden or unauthorized functions by answering yes to B3.*

Q 3 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.*

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: What PIN block formats are allowed?**

A *ISO 9564–1 PIN block formats 0, 1, 3 or 4 are acceptable for online transactions.*

Q 4 **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 5 **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 6 **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 7 **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 8 September 2015: ISO 11568-2 *Symmetric ciphers, their key management and life cycle* and ANSI X9.24-1 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques stipulate that a key-encipherment key shall be at least of equal or greater strength than the key that it is protecting. What keys does this apply to in a device?

A *This applies to any key-encipherment keys used for the protection of secret or private keys stored in the device or for keys used to encrypt any secret or private keys for loading or transport to the device. For purpose of this requirement, the following algorithms and keys sizes by row are considered equivalent.*

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	168	2048	224	2048/224

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. DSA for digital signatures, and Diffie-Hellman and MQV key agreement key sizes refer to the size of the modulus (p) and the minimum size of a large subgroup (q).

AES keys, of 128 bits or larger are considered stronger than any of the aforementioned.

This does not apply to keys that are used for authentication purposes, such as keys used to validate firmware. The sizes of those keys must at minimum be as stipulated in B4. DES keys with an effective length of 112 bits may also be used, as long as they are not used to protect stronger keys, such as those stated above.

Q 9 September 2015: Version 2 stipulates that the device must provide support for TR-31 or an equivalent methodology for maintaining the TDES key bundle. Under what circumstances does this apply?

A *If the device supports the exchange of TDEA keys between itself and another device (e.g., a remote host) encrypted under a shared symmetric key, the device must provide support for TR-31 or an equivalent methodology for this key conveyance. This does not imply that the device must support TR-31 or an equivalent methodology between the device and an external ICC reader, but it optionally may do so. The device may also optionally support TR-31 or an equivalent methodology for the storage of keys encrypted under a symmetric key. 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 10 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 11 September 2015: A device may support key-check values to validate the successful entry of symmetric key components and/or keys. Are there any restrictions on the use of key-check values?

A *Yes. Any returned values shall not exceed six hexadecimal characters and should be at least four hexadecimal characters in length.*

Q 12 September 2015: Requirement B11 stipulates that the device must support TR-31 or equivalent. Key blocks that support padding include a key length that allows the key to be distinguished from the pad characters. In TR-31, the key-length information and padding are encrypted along with the key itself by the KEK (termed the key block encryption key). Does this violate the requirement that a cryptographic key be only used for one purpose, e.g., key encipherment?

A *No. For all TDEA modes of operation, the three cryptographic keys (K1, K2, K3) define a TDEA key bundle. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle cannot be unbundled for any purpose—i.e., must never be used separately for any other purpose. A key used to encrypt the key bundle may include in the encrypted portion of the key bundle the key-length information and padding as necessary to protect the integrity of the key bundle.*

Q 13 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 14 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 15 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 16 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 17 September 2020: PIN Security Requirement 18-3 requires the implementation of key blocks. Interoperable methods include those defined in ASC X9 TR-31 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 for peer review:*

- *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) and*
- *Has ten or more years of experience in the relevant subject and*
- *Subscribes to an ethical code of conduct and would be subject to an ethics compliance process if warranted and.*
  - *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.

Q 18 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 19 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 20 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 B15

Q 1 May 2019: ISO 9564-1 stipulates various criteria for translations between PIN block formats. The HSM Derived Test Requirements illustrates in TB15.3 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. Do any other restrictions apply?

A *Yes. The following restrictions on translations between PIN block formats must be enforced regardless of the key management methodology used:*

- *Only ISO formats 0, 3 and 4 shall be supported in calculating values used for PIN verification that are derived from the PIN and PAN, e.g. PIN offsets and PIN verification values (PVV).*
- *For ISO formats 0 and 3, when calculating values derived from the PIN and PAN, if the portion of the account number enciphered in the input encrypted PIN block does not agree with the input PAN, the calculated value shall not be returned except in the following case: where the introduction of a new PAN is required to support account number changes for card issuance, support for change of PAN during calculation of the derived value shall be provided only while the host security modules are in a sensitive state and under dual control.*
- *For ISO format 4, when calculating values (such as PVVs or offsets) derived from the PIN and PAN, if PAN 1 used for the derivation of the calculated value does not agree with PAN 2 used in the plain text PAN field, the calculated value shall not be returned except in the following case: where the introduction of a new PAN is required to support account number changes for card issuance, support for change of PAN during calculation of the derived value shall be provided only while the host security modules are in a sensitive state and under dual control*
- *No integrity checks shall be performed on the PIN digits themselves. If integrity checks are performed on the deciphered PIN field, then they shall only be performed on the first byte of that field (control field and PIN length field) and the fill digits.*

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 the following:*

"The tester shall examine the security policy and other relevant documentation submitted by the vendor to verify that the security policy can be implemented to support the following configuration and that implementation is easily identifiable in reviewing system settings.

- *ISO formats 0, 1, 2, 3 and 4 cannot be translated into any non-ISO format.*
- *Format 2 PIN blocks shall be constrained to offline PIN verification and PIN change operations in ICC environments only.*
- *Translation of PIN block formats that include the PAN, to PIN block formats that do not include the PAN, shall not be supported. In particular, ISO PIN-block formats 0, 3, and 4 are not translated into any PIN-block formats other than 0, 3, or 4*
- *PIN-block translations from ISO format 0, 3, or 4 to any of ISO format 0, 3, or 4 do not support a change in PAN. This translation restriction is not applicable to surrogate PANs used in tokenization implementations.*
- *If ISO format 1 is translated to ISO format 0, 3, or 4, it is not translated back to ISO format 1.*

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.*