Payment Card Industry (PCI)
PTS HSM Security Requirements

Technical FAQs for use with Version 2.0

December 2013

Table of Contents

HSM Device Evaluation: *Frequently Asked Questions* 3

General Questions 3
HSM Requirement B1 4
HSM Requirement B11 4
HSM Requirement C1 4

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?

A *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 certificate. 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 certificate. The HSM is only compliant with PCI HSM during the period that it is running firmware/software has been approved for PCI HSM.

HSM Requirement B1

Q 6 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.*

HSM Requirement B11

Q 7 Are HSMs allowed to have keys that are not unique per device?

A *Yes, but only for load balancing purposes.*

HSM Requirement C1

Q 8 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 9 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, and 3 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 and 3 shall not be translated into ISO PIN block format 1."*

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

Q 10 Is the device allowed to share PCI relevant keys and passwords 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 between the two modes or the device must zeroize all PCI relevant keys and passwords 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.