Payment Card Industry (PCI)
PTS HSM Security Requirements

Technical FAQs for use with Version 1.0

March 2011

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.*

HSM Requirement A6

Q 2 **ISO 9564 and requirement A6 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 3 **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 4 **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.*

HSM Requirement B3

Q 5 **Are HSMs allowed to have keys that are not unique per device?**

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

HSM Requirement B14

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.*