Payment Card Industry (PCI)

PIN Transaction Security (PTS) Hardware Security Module (HSM)

Evaluation Vendor Questionnaire

Version 2.0

May 2012

Document Changes

Date	Version	Author	Description
April 2009	1.0	PCI	New Release
October 2011	1.1	PCI	Modifications for consistency with PCI POI requirements
February 2012	2.x	PCI	RFC version - Modifications for consistency with PCI POI requirements.
May 2012	2.0	PCI	Public release

Table of Contents

Related Publications

The following ANSI, ISO, FIPS, NIST, and PCI standards are applicable and related to the information in this manual.

Data Encryption Algorithm	ANSI X3.92
Banking—Retail Financial Services Symmetric Key Management	ANSI X9.24
Key Establishment Using Integer Factorization Cryptography	ANSI X9.44
Public Key Cryptography for the Financial Services ECDSA	ANSI X9.62
Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography	ANSI 9.63
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ANSI TR-31
FIPS PUB 140-2: Security Requirements for Cryptographic Modules	FIPS
Personal Identification Number (PIN) Management and Security	ISO 9564
Banking—Key Management (Retail)	ISO 11568
Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques	ISO 11770-2
Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)	ISO 11770-3
Banking—Secure Cryptographic Devices (Retail)	ISO 13491
Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers	ISO/IEC 18033-3
Guidelines on Triple DES Modes of Operation	ISO TR19038
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	NIST SP 800-22
Recommendations for Key Management – Part 1:General	NIST SP 800-57
Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	NIST SP 800-67
Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements	PCI SSC
Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements	PCI SSC
Payment Card Industry (PCI) PIN Security Requirements	PCI SSC

Note: *These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.*

Questionnaire Instructions

1. Complete the information below for the HSM being evaluated.

2. Identify all sections of the questionnaire corresponding to those questions in the form of the *PCI Hardware Security Module (HSM) Security Requirements* manual (“HSM Security Requirements”) for which you answered “**YES**.”

3. Complete each item in those identified sections.

4. Provide sufficient detail to thoroughly describe the HSM attribute or function.

5. Refer to and provide additional documentation as necessary.

6. Vendor must provide detail in the comments section for all “N/A” answers

   Example: Question A1.1 in the form of the *PCI Hardware Security Module Security Requirements* manual was answered with a “**YES**.” Therefore, all items (1 through 5) in Section A1.1 of this questionnaire must be answered.

HSM Identifier	
HSM Manufacturer:	
Marketing Model Name/Number:	
Hardware Version Number:	
Firmware Version Number:	
Application Version Number: (if applicable)	

Questionnaire completed by:

Signature ↑	*Date ↑*
Printed Name ↑	*Title ↑*

A – Core Physical Security Characteristics

Section A1

If the answer to A1 in the *PCI HSM Security Requirements* was “YES,” describe:

1	All mechanisms protecting against tampering.
2	The tamper action(s) that trigger(s) the mechanisms.
3	The response of the HSM to tamper detection. (This should include a written description of how the tamper mechanisms work and how erasure of secret information and/or inoperability is accomplished.)
4	The type of erasure (active or passive).
5	The details of what is erased upon tamper detection and the locations (e.g., RSA firmware authentication key is erased from the cryptographic processor flash) and the mechanisms used to erase the data.
6	Any reference documentation (e.g., security architecture, schematics, block diagrams) that describes the tamper detection circuitry or erasure process.
7	What areas of the HSM contain sensitive components and/or information?
8	Why the tamper mechanisms of the HSM prevent access to areas containing sensitive components and information without requiring a minimum attack potential of 20.

A1, continued

9	Whether sensitive information may exist when a human operator is present. Yes □ No □ In what area(s) may it exist? Provide the documentation that describes the inspection process that must be performed.

Comments:

Section A2

If the answer to A2 in the *PCI HSM Security Requirements* was "YES," describe:

1	The combinations of tamper detection and/or tamper evidence.
2	How the security mechanisms work.
3	How the security mechanisms are independent.
4	Why the security mechanisms do not rely upon insecure services and characteristics.
5	The characteristics designed to offer tamper resistance.
6	Who is intended to inspect the device for tamper evidence?

Comments:

Section A3

If the answer to A3 in the *PCI HSM Security Requirements* was "YES," describe:

1	Whether the device permits access to internal areas for maintenance or service. Yes □ No □
2	The internal areas that can be accessed and the components located in those areas.
3	The location of all physical access ports.
4	The mechanisms protecting those physical access ports.
3	How access to sensitive data such as PIN or cryptographic data is prevented by the design of the internal areas if the answer to 1 above is **"YES."**
4	The mechanism that causes immediate erasure of sensitive data if the answer to 1 above is **"YES."**
5	How is the mechanism triggered?
6	What sensitive data is erased?
7	The erasure method.
8	If passive erasure is used, how it occurs rapidly enough to prevent an attacker from opening the device and stopping erasure before it is effective.

Comments:

Section A4

If the answer to A4 in the *PCI HSM Security Requirements* was "YES," describe:

1	The operational and environmental conditions for which the HSM was designed.
2	Why the security of the HSM is not compromised by operational and environmental conditions.
3	The tests performed to ensure the security on the changing operational and environmental conditions. (Provide test reports.)
4	Why the measures are sufficient and effective.
5	The design of the environmental failure protection (EFP) response mechanisms.
6	The conditions that cause the EFP to trigger.
7	The response of these mechanisms when triggered.

Comments:

Section A5

If the answer to A5 in the *PCI HSM Security Requirements* was “YES,” describe:

1	All of the HSM’s public keys.
2	What sensitive information and functions exist?
3	Where sensitive functions are executed and where sensitive information is used.
4	How sensitive information and functions dealing with sensitive information are protected from modification.
5	Provide the rationale for why the measures are sufficient and effective and would require a per-HSM attack potential of at least 25 to defeat.
6	How public keys used for functions that impact security-related functions are protected from modification and substitution.
7	The authorized methods for modifying and replacing public keys.

Comments:

Section A6

If the answer to A6 in the *PCI HSM Security Requirements* was "YES," describe:

1	The design of all mechanisms intended to resist tamper.
2	The HSM's protection against monitoring electromagnetic emissions.
3	Any electromagnetic emission testing that has been performed. Provide data for tests performed .
4	The HSM protections against monitoring power consumption. Provide data for tests performed .
5	Any other internal or external characteristics considered. If applicable, provide data for tests performed.
6	The rationale for why the HSM implementation is such that the determination of sensitive information by monitoring sound, electro-magnetic emissions, or power consumption requires an attack potential of at least 25.

Comments:

Section A7

If the answer to A7 in the *PCI HSM Security Requirements* was “YES,” describe:

1	The device components that store or use cryptographic keys related to the operations under the scope of the device requirements.
2	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components’ design.
3	Whether the device includes any tamper-detection and response mechanisms in these components. Yes □ No □
	If so, provide responses to Section A1.1.
4	Whether the device includes any tamper-resistance mechanisms in these components. Yes □ No □
	If so, provide responses to Section A1.1.
5	The rationale for why the device implementation is such that the cost of determining any PCI HSM-related cryptographic key resident in the device—either by penetration of the device or by monitoring emanations from the device (including power fluctuations)—exceeds an attack potential of at least 35, with a minimum of 15 for exploitation.

Comments:

B – Core Logical Security Characteristics

Section B1

If the answer to B1 in the *PCI HSM Security Requirements* was "YES," describe:

1	In detail, each self-test performed by the HSM on power-up and periodically during operation. Which of the techniques are consistent with FIPS PUB 140-2?
2	How the periodic self-tests are induced.
3	How frequently the periodic self-tests are executed.
4	The conditional tests performed by the HSM. Which of the techniques are consistent with FIPS PUB 140-2?
5	How the conditional self-tests are induced.
6	The status provided by the HSM when power-up, periodic, and conditional self-tests execute successfully.
7	The actions of the HSM on a failure of each self-test
8	The algorithms used to perform the power-on firmware authenticity and integrity test. If the HSM supports firmware load, describe the firmware-load test, including the algorithms used.

Comments:

Section B2

If the answer to B2 in the *PCI HSM Security Requirements* was "YES," describe:

1	Which commands are accepted by the HSM?
2	How the commands are linked to the device modes.
3	What type of parameter and data checking is performed?
4	Why the functionality is not influenced by logical anomalies.
5	Any tests that have been performed to ensure the functionality is not influenced by logical anomalies. Provide a rationale why the test coverage is sufficient**.**
6	How sensitive information or PINs are prevented from being outputted in clear-text.

Comments:

Section B3

If the answer to B3 in the *PCI HSM Security Requirements* was “YES,” describe:

1 The documented firmware review process and frequency.

2 The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.

Comments:

Section B4

If the answer to B4 in the *PCI HSM Security Requirements* was "YES," describe:

1	What cryptographic algorithms and keys are used for firmware authentication?
2	What is the device's response if firmware to be updated cannot be authenticated?

Comments:

Section B5

If the answer to B5 in the *PCI HSM Security Requirements* was "YES," describe:

1	How the HSM's data input, data output, control input, and status output interfaces are kept logically separate.
2	All data that is passed in and out of each logical interface.
3	The HSM's response to erroneous commands.
4	The HSM's response to erroneous data.

Comments:

Section B6

If the answer to B6 in the *PCI HSM Security Requirements* was "YES," describe:

1	The data that is automatically cleared from the HSM's internal buffers when a transaction is completed.
2	The location of all buffers that are cleared.
3	The process used to clear the buffers.
4	The time-out period for the HSM.
5	The action taken by the HSM upon time-out.

Comments:

Section B7

If the answer to B7 in the *PCI HSM Security Requirements* was "YES," describe:

1	All of the administration services provided by the HSM (or make reference to a document that contains this information).
2	Which services require the assistance of two separately authenticated operators or a single authenticated operator.
3	The sensitive functions provided by the HSM.
4	How the HSM controls the access and use of sensitive functions.
5	The authentication method used to access sensitive services.
6	Whether an external device is used to authenticate to the HSM to access sensitive services and its protections**.** Yes □ No □
7	How the authentication data used to access sensitive services in the HSM reader is protected, as it is input/output via the interface.
8	Which of the following is true for the data referred to in 7 above: □ Data inputs cannot be discerned from any displayed characters. □ Data inputs cannot be discerned by monitoring audible or electro-magnetic emissions. □ Sensitive data is cleared from internal buffers upon exiting a secure mode.
9	The interface used to authenticate to access sensitive services.
10	The rationale for the value chosen for the limit on the number of function calls (services). Also, describe how the limit minimizes the risks from unauthorized use of sensitive functions.
11	The rationale for the chosen time limit. Also, describe how the time limit minimizes the risks from unauthorized use of sensitive functions.

B7, continued

12	Whether, when the limits are exceeded, the HSM requires the operators to re-authenticate. Yes □ No □	
13	The measures that ensure that entering or existing sensitive services do not reveal or otherwise affect sensitive information**.**	
14	The management of any data used for authentication. *Examples of authentication data are passwords, cryptographic keys, and hardware tokens*. Include:	
15	▪ The number of devices that share the same keys or passwords.	
	▪ Cryptographic algorithms used for authentication, if applicable.	
	▪ Data size (key or password length).	
	▪ How authentication data is distributed to legitimate users.	
	▪ How authentication data can be updated.	
16	For each of the implemented authentication techniques, provide a calculation for the associated probability that a random attempt will succeed.	
17	For each of the implemented authentication techniques, provide a calculation for the associated probability that for multiple attempts within a one-minute period, a random attempt will succeed.	
18	The HSM's response to false authentication data.	
19	The authorized methods for accessing and manipulating CSPs.	

Comments:

Section B8

If the answer to B8 in the *PCI HSM Security Requirements* was "YES," describe:

1	All CSP components that are entered or output using split-knowledge/dual-control procedures. Indicate how many components each CSP is split into and how many components are required to reconstruct the original CSP.
2	If knowledge of *n* components is required to reconstruct the CSP, the rationale stating how the knowledge of any *n*-1 components contains no other information about the original CSP other than the length.
3	The implemented CSP component-entry/output techniques (manual, direct, device).
4	How the CSP components are entered into the HSM without traveling through any enclosing or intervening systems.
5	Whether the HSM supports split knowledge/dual control CSP component-entry/output procedures via a network connection.
6	All keys that are entered or output in enciphered form and the algorithm used to encipher each key.
7	All keys that are entered or output in plain-text form.
8	The implemented plain-text key-entry/output techniques and how the keys are directly entered into the HSM without traveling through any intervening systems.
9	Whether the HSM supports the manual or network techniques for plain-text key entry/output procedures.
10	What mechanisms are in place to record audit information.

B8, continued

11	Each combination of key-exchange technique and key-storage mechanism supported by the HSM (e.g., ANSI TR-31).
12	If applicable, the secure device or interface used for the loading of clear-text cryptographic data.

Comments:

Section B9

If the answer to B9 in the *PCI HSM Security Requirements* was "YES," describe:

1	The design of each of the implemented RNG(s) and/or PRNG(s).
2	Any standards the RNG(s) and/or PRNG(s) have been designed to comply with.
3	For each type of CSP generated by the HSM, indicate the RNG and/or PRNG used.
4	How cryptographic key components and other CSPs are generated using a random or pseudo-random process, such that it is not possible to predict any secret value or determine that certain values are more probable than others from the total set of all the possible values.
5	The tests performed to demonstrate that the numbers produced are sufficiently unpredictable.
6	How the random number generator is used to protect or produce sensitive data.

Comments:

Section B10

If the answer to B10 in the *PCI HSM Security Requirements* was "YES," describe:

1	All algorithms implemented within the HSM, their associated key sizes, and the modes used (e.g., TDES CBC, RSA PKCS #1 v2.1).
2	How each algorithm is used**.**
3	All security protocols (e.g., SSL, TLS, IPsec, etc.) supported by the HSM.
4	The combination of algorithms (e.g., cipher suites) supported for each protocol.
5	All prior algorithm certifications and/or test results. (Please provide certificates, letters of approval, or test reports.)
6	Any relevant documentation, such as security-evaluation reports, schematics, data sheets, vendor test procedures and test reports about the encryption algorithm, padding mechanism, and mode of operation being used.
7a	The credentials of the expert reviewer that assessed the security of the mode of operation used by the encryption algorithm (if a non-standardized mode of operation is in use).
7b	How the expert reviewer is independent to the vendor**.**

Comments:

Section B11

If the answer to B11 in the *PCI HSM Security Requirements* was “YES,” describe:

1	The fixed key, master key/session key, or unique key per transaction (UKPT) PIN-protection technique.	
2	Whether each key is used for only one cryptographic purpose. Yes □ No □ How is this enforced?	
3	How keys are protected during key storage against unauthorized disclosure and substitution.	
4	How key separation is ensured during key storage.	
5	All cryptographic algorithms implemented by the HSM.	
6	For all cryptographic keys that reside within an operational HSM, indicate the following:	
	▪ Name	
	▪ Key size	
	▪ Associated cryptographic algorithm	
	▪ The data that may be encrypted under the key	
	▪ The number of instances or registers for that key type	
	▪ How the key is identified by the HSM so that it is used only as intended	
7	Whether the HSM has the ability to erase cryptographic keys. Yes □ No □	
8	What keys may be erased?	
9	What process is used for erasure?	

B11, continued

10	Under what circumstances are keys erased? Describe for all device states (power-on, power-off, sleep mode).
11	What other data may be erased? Under what circumstances?
12	How all keys present or otherwise used in the device are loaded, including who the key is generated by (e.g., acquirer or manufacturer) generates and whether the keys are loaded encrypted or as plain-text or as encrypted or plain-text components/secret shares.

B11, continued

13	Whether there is a key-distribution technique present that uses an asymmetric algorithm with a public key for the exchange of symmetric secret keys, address each of the following points.	
	▪ Whether a random/pseudo-random key-generation process is used such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others.	Yes □ No □
	Whether the random source is tested in a suitable manner before key generation.	Yes □ No □
	▪ How the authenticity of public keys is ensured.	
	▪ Whether there is a certificate hierarchy.	Yes □ No □
	How certificates (signed public keys of the key-exchange partners) are generated; i.e., who signs?	
	▪ Whether there is mutual device authentication.	Yes □ No □
	If certificates are used, how are they tested and accepted or rejected?	
	▪ Whether there is a secure formatting and padding of the message used which contains the symmetric secret key.	Yes □ No □
	▪ Whether the correctness of the message structure is tested by the receiver.	Yes □ No □
	▪ Which effective key length(s) is/are utilized for all the cryptographic algorithm(s) in question?	
	If RSA is used, is the key length at least 2048 bit with SHA-2 or greater?	Yes □ No □
14	Whether single component keys can be loaded and the algorithm used to encrypt them during key entry.	
15	All storage and usage locations for each key ever present in or used by the device.	
16	Each combination of key-exchange technique and key-storage mechanism supported by the HSM (e.g., ANSI TR-31).	

Comments:

Section B12

If the answer to B12 in the *PCI HSM Security Requirements* was “YES,” describe:

1	The HSM’s behavior when cryptographic keys are lost.
2	How the HSM fails in a secure manner when the cryptographic keys are rendered invalid.
3	Any status provided by the HSM when cryptographic keys rendered invalid.
4	How the device determines that a key has been rendered invalid.

Comments:

Section B13

If the answer to B13 in the *PCI HSM Security Requirements* was "YES," describe:

1	How the HSM ensures that cryptographic keys are only used for a single cryptographic function.
2	How the HSM ensures that cryptographic keys are only used for an intended purpose, and indicate which of the following methods are supported: □ Physical segregation □ Storing keys enciphered under a KEK dedicated to encipherment of a specific type of key □ Modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage, e.g., key tags.
3	For every key used for PIN encryption, indicate what type of data can be encrypted or decrypted.
4	How encrypted PIN data is distinguished from all other data encrypted or plain-text.
5	All key-encrypting keys.
6	What data can be encrypted using key-encrypting keys.
7	How this data is distinguished from all other data.
8	How encrypted keys are distinguished from all other data.

Comments:

Section B14

If the answer to B14 in the *PCI HSM Security Requirements* was "YES," describe:

1	Whether there is a mechanism that will allow the output of plain-text secret or private cryptographic keys or plain-text PIN. Yes □ No □ If yes, describe the mechanism.
2	How is the outputting of plain-text keys and plain-text PINs prevented?
3	In what locations within the HSM may cryptographic keys exist in plain-text?
4	Under what circumstances a plain-text key may be transferred from each of the above locations to another location within the HSM.

Comments:

Section B15

If the answer to B15 in the *PCI HSM Security Requirements* was "YES," describe:

1	The PIN-block formats supported by the HSM.
2	The method used by the HSM to ensure that journaled transaction messages do not contain a plain-text PIN.
3	All key-encryption keys and associated algorithms.

Comments:

Section B16

If the answer to B16 in the *PCI HSM Security Requirements* was "YES," describe:

1	The HSM's logging mechanism, and list the data and events logged.
2	How the log data is protected from unauthorized modification, substitution, and deletion.
3	The method used to provide a time stamp for audit events.
4	The dual-control mechanism for deletion if logs are stored internally.

Comments:

Section B17

If the answer to B17 in the *PCI PTS POI Security Requirements* was “YES,” describe:

1	Whether the device support multiple applications. Yes □ No □
	If yes, provide a list of these applications, and identify those with security impact.
	If yes, how is the separation between applications with security impact from those without security impacts enforced?
2	For each security relevant application, list by groups the data objects and their location.
3	Which mechanism prevents applications from accessing data objects not belonging to them.
4	If the HSM allows customers or integrators to install additional applications, how the HSM’s design prevents the embedded application from:
	▪ Having access to the top-level master keys which protect the working keys- i.e., it cannot extract or modify the top-level master key.
	▪ Having access to operator or security officer functions, and so cannot change security configurations or change privileges.
	▪ Introducing new primitive cryptographic functions (although it can use these to implement new composite functionality).
	How the embedded application is separated from the approved HSM functionality by an internal security boundary that prevents embedded applications from obtained any elevated privilege or access to any data belonging to other embedded or host side.

B17, continued

Comments:

Section B18

If the answer to B18 in the *PCI PTS POI Security Requirements* was “YES,” describe:

1	The method of ensuring that the operating system contains only the components and the services necessary for the intended operation.
2	The procedures used for maintenance and updates of the operating system.
3	The rationale for why the method used to enforce least privilege is effective.
4	The rationale for why all the components and services in the configuration list are necessary.

Comments:

Section B19

If the answer to B19 in the *PCI HSM Security Requirements* was "YES," describe:

1	The format of the HSM's unique device ID.
2	How the unique device ID can be obtained from the HSM.
3	How the unique device ID is assigned.
4	Whether it is possible to change the HSM's unique device ID. Yes □ No □ If yes, provide a description.
5	How exactly is the HSM uniquely identified using cryptographic methods?
6	What acceptable algorithms are used for uniquely identifying the HSM through cryptographic means?

Comments:

Section B20

If the answer to B20 in the *PCI HSM Security Requirements* was "YES," describe:

1	Describe the differences between PCI and non-PCI mode, including (but not limited to) services/functions available, algorithms, PIN translations, and PIN/key input or output:
2	Describe the process/commands for switching between PCI and non-PCI mode.
	If remote (over a network such as Ethernet or WiFi), what authentication and replay prevention mechanisms are used?
	If direct (e.g., through serial or keypad on the device), what authentication mechanism is used?
3	How does the device prevent keys from being shared between PCI and non-PCI mode (zeroization or isolation)?
4	How does the device indicate that it is in PCI or non-PCI mode?

Comments:

C – Policy and Procedures

Section C1

If the answer to C1 in the *PCI HSM Security Requirements* was "YES," describe:

1	Whether the security policy is available to potential customers. Yes □ No □
2	How changes to the security policy document are controlled.
3	The roles supported by the HSM.
	The services available for each role.
4	How the HSM is configured to comply with the security policy.
5	Whether the HSM supports PIN translation. Yes □ No □
	If so, what formats does it support and what translations to/from does it support?

Comments:

Device Diagrams (Optional)

If you wish to include diagrams or other illustrations in support of the relevant device's functionality, please insert them here.