Payment Card Industry (PCI)

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

Security Requirements

Version 2.0

May 2012

Document Changes

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

Table of Contents

About This Document

Purpose

HSMs (Hardware Security Modules) play a critical role in helping to ensure the confidentiality and/or data integrity of financial transactions. Therefore, to help engender trust in the legitimacy of the financial transactions being supported, it is imperative that HSMs are appropriately secure during their entire lifecycle. This includes manufacturing, shipment, use, and decommissioning. The purpose of this document is to provide guidance and direction for appropriately designing HSMs to meet the security needs of the financial payments industry, and for protecting those HSMs up to the point of initial deployment. Other security requirements apply at the point of deployment for the management of HSMs involved with financial payments industry.

This document provides vendors with a list of all the security requirements against which their products will be evaluated in order to obtain Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) device approval.

HSMs may support a variety of payment-processing and cardholder-authentication applications and processes. The processes relevant to the full set of requirements outlined in this document are:

- PIN processing
- 3-D Secure
- Card verification
- Card production and personalization
- EFTPOS
- ATM interchange
- Cash-card reloading
- Data integrity
- Chip-card transaction processing

There are many other applications and processes that may utilize general-purpose HSMs, and which may necessitate the adoption of all or a subset of the requirements listed in this document. However this document does not aim to develop a standard for general-purpose HSMs for use outside of applications such as those listed above that are in support of a variety of payment-processing and cardholder-authentication applications and processes for the financial payments industry.

Scope of the Document

This document is part of the evaluation-support set that laboratories require from vendors (details of which can be found in the *PCI PTS Device Testing and Approval Guide*), and the set may include:

- A companion *PCI PTS Vendor Questionnaire* (where technical details of the device are provided)
- Product samples
- Technical support documentation

Upon successful compliance testing by the laboratory and approval by the PCI SSC, the PCI PTS HSM device will be listed on the PCI SSC website. Commercial information to be included in the Council's approval must be provided by the vendor to the test laboratory using the forms in the "Required Device Information" section of this document.

Main Differences from Previous Version

This document has been enhanced to include:

- The updating of attack methodologies that can be considered to reflect a more comprehensive approach;
- The updating of algorithms and key sizes to be consistent with those stipulated in *PTS POI Security Requirements v3;*
- The inclusion of criteria to support remote key-loading techniques using public-key methods to require compliance with PCI-defined criteria for key sizes and mutual authentication between host and device.

Furthermore, this document introduces a two-tier approval structure for HSMs. These tiers differentiate only in the “Physical Derived Test Requirements” section as delineated in the *PCI PTS HSM Derived Test Requirements*. HSMs may be approved as designed for use in controlled environments as defined in ISO 13491-2: *Banking — Secure cryptographic devices (retail)* **or** approved for use in any operational environment.

Foreword

The requirements set forth in this document are the minimum acceptable criteria for the Payment Card Industry (PCI). The PCI has defined these requirements using a risk-reduction methodology that identifies the associated benefit when measured against acceptable costs to design and manufacture HSM devices. Thus, the requirements are not intended to eliminate the possibility of fraud, but to reduce its likelihood and limit its consequences.

HSMs are typically housed in a secure environment and managed with additional procedural controls external to the device.

These HSM security requirements were derived from existing ISO, ANSI, and NIST standards; and accepted/known good practice recognized by the financial payments industry.

Evaluation Domains

Device characteristics are those attributes of the device that define its physical and its logical (functional) characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device, for example, the penetration of the device to determine its key(s) or to plant a sensitive data-disclosing “bug” within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a clear-text PIN-encryption key.

The evaluation of physical security characteristics is very much a value judgment. Virtually any physical barrier can be defeated with sufficient time and effort. Therefore, many of the requirements have minimum attack-calculation values for the identification and initial exploitation of the device based upon factors such as attack time, expertise and equipment required. Given the evolution of attack techniques and technology, the PCI payment brands will periodically review these attack calculations for appropriateness.

Device Management

Device management considers how the device is produced, controlled, transported, stored, and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

This document is concerned with the device management for HSM devices only up to receipt at the point of deployment. Subsequent to receipt of the device at the point of deployment, the responsibility for the device falls to the acquiring financial institution and its agents (e.g., merchants and processors), and is covered by the operating rules of the participating PCI Payment Brands and other security requirements, such as the *PCI PIN Security Requirements*.

FIPS 140-2 Requirements

Some requirements in this manual are derived from requirements in Federal Information Processing Standard 140-2 (FIPS 140-2). These requirements are identified in this document with an asterisk (*) in the number column.

Because many FIPS 140-2 evaluations only cover a subsection of the HSM and with a number of possible security levels, existing evaluation evidence for an HSM certified against FIPS 140-2 will be assessed as follows.

The evaluator 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.

Related Publications

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

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 (PTS) Point of Interaction (POI) 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.*

Required Device Information

May 2012

HSM Identifier	
HSM Manufacturer:	
Marketing Model Name/Number:	
Hardware Version Number[A]:	_ _
Use of "**x**" represents a request for field to be a Variable	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Firmware Version Number:	
Application Version Number: (if applicable)	
Designed for deployment only in controlled environments as defined in ISO 13491-2?	**Yes** ☐ **No** ☐

At the end of this form under "Device Specification Sheet," attach documentation highlighting device characteristics, including photos. These photos are to include both external and internal pictures of the device. The internal pictures are to be sufficient to show the various components of the device.

Optional Use of Variables in the HSM Identifier

[A]Hardware Version Number – Request for Use of the Variable "x"

Note: *The firmware version number may also be subject to the use of variables in a manner consistent with hardware version numbers. See the* PCI PTS Device Testing and Approval Program Guide *for more information.*

Variable "x" Position	Description of Variable "x" in the Selected Position

A – Physical Security Requirements

All HSMs must meet the following **physical** security requirements.

Number	Description of Requirement	Yes	No	N/A
A1*	The HSM uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the HSM, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device. There is no demonstrable way to disable or defeat the mechanisms and access internal areas containing sensitive information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation[A].	☐	☐	☐
A2	Failure of a single security mechanism does not compromise HSM security. Protection against a threat is based on a combination of at least two independent security mechanisms. If the HSM relies upon visible tamper evidence for protection, the HSM has characteristics such that penetration of the device results in visible tamper evidence that has a high probability of being detected.	☐	☐	☐
A3	If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this area to access sensitive data. Immediate access to sensitive data, such as PIN or cryptographic data, is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of sensitive data.	☐	☐	☐
A4	The security of the HSM is not compromised by altering environmental conditions or operational conditions (for example, subjecting the HSM to temperatures or operating voltages outside the stated operating ranges).	☐	☐	☐
A5	Sensitive functions or information are only used in the protected area(s) of the HSM. Sensitive information and functions dealing with sensitive information are protected from modification or substitution, without requiring an attack potential of at least 26 per HSM for identification and initial exploitation, with a minimum of 13 for initial exploitation[A].	☐	☐	☐

* Derived from *Federal Information Processing Standard* 140-2 (FIPS 140-2)

[A] As defined in Appendix A of the *PCI HSM DTRs*

Number	Description of Requirement	Yes	No	N/A
A6	There is no feasible way to determine any sensitive information by monitoring electro-magnetic emissions, power consumption, or any other internal or external characteristic without an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation[B].	☐	☐	☐
A7	Determination of any PCI-related cryptographic key resident in the device or used by the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation[B].	☐	☐	☐

[B] As defined in Appendix A of the *PCI HSM DTRs*

B – Logical Security Requirements

All HSMs must meet the following **logical** requirements.

Number	Description of Requirement	Yes	No	N/A
B1*	To ensure that the HSM is operating as designed, the device runs self-tests when powered up and at least once per day to check firmware (authenticity check), security mechanisms for signs of tampering, and whether the HSM is in a compromised state. When specific critical operations are performed, the HSM performs conditional tests. The techniques and actions of the HSM upon failure of a self-test are consistent with those defined in FIPS PUB 140-2.	☐	☐	☐
B2	The HSM's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the HSM outputting clear-text PINs or other sensitive information.	☐	☐	☐
B3	The firmware, and any changes thereafter, has been inspected and reviewed using a documented process that can be audited and is certified as being free from hidden and unauthorized or undocumented functions.	☐	☐	☐
B4	If the HSM implements firmware updates, the device cryptographically authenticates the firmware integrity, and if the authenticity is not confirmed, the firmware update is rejected and deleted.	☐	☐	☐
B5*	The HSM provides secure interfaces that are kept logically separate by distinguishing between data and control for inputs and also between data and status for outputs.	☐	☐	☐
B6	The HSM must automatically clear or reinitialize its internal buffers that hold sensitive information prior to reuse of the buffer, including when: • The transaction is completed, • The HSM has timed out, or • The HSM recovers from an error state.	☐	☐	☐
B7*	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	☐	☐	☐

* Derived from *Federal Information Processing Standard* 140-2 (FIPS 140-2)

<table>
<tr><th>Number</th><th>Description of Requirement</th><th>Yes</th><th>No</th><th>N/A</th></tr>
<tr><td>B8*</td><td>Private and secret key entry is performed using accepted techniques according to the table below.
<table>
<tr><th rowspan="2">Key Form</th><th colspan="3">Technique</th></tr>
<tr><th>Manual</th><th>Direct</th><th>Network</th></tr>
<tr><td>Plaintext keys</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Plaintext key components</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td>Enciphered keys</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
</table></td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B9*</td><td>If the device generates random numbers in connection with security over sensitive data, the random number generator has been assessed to ensure that it is generating sufficiently unpredictable numbers.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B10*</td><td>The HSM uses accepted cryptographic algorithms, modes, and key sizes.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B11</td><td>The key-management techniques implemented in the HSM conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support ANSI TR-31 key-derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B12</td><td>The HSM ensures that if cryptographic keys within the secure HSM boundary are rendered invalid for any reason (e.g., tamper or long-term absence of applied power), the HSM will fail in a secure manner.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B13*</td><td>The HSM ensures that each cryptographic key is only used for a single cryptographic function. It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in or protected by the HSM. The HSM does not permit any of the key-usage information to be changed in any way that allows the key to be used in ways that were not possible before the change.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B14</td><td>There is no mechanism in the HSM that would allow the outputting of private or secret clear-text keys, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security. All cryptographic functions implemented shall not output clear-text CSPs to components that could negatively impact security.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B15</td><td>If the HSM is designed to be used for PIN management, the HSM shall meet the PIN-management requirements of ISO 9564. The PIN-encryption technique implemented in the HSM is a technique included in ISO 9564.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B16</td><td>The HSM includes cryptographic mechanisms to support secure logging of transactions, data, and events to enable auditing.</td><td>☐</td><td>☐</td><td>☐</td></tr>
</table>

* Derived from *Federal Information Processing Standard* 140-2 (FIPS 140-2)

Number	Description of Requirement	Yes	No	N/A
B17	If the HSM supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS/firmware of the device, including, but not limited to, modifying data objects belonging to another application or the OS/firmware. Similarly, enforcement of separation must be provided if the HSM supports virtualization such that it can act as multiple logically separate HSMs.	☐	☐	☐
B18	The operating system/firmware of the device must contain only the software (components and services) necessary for the intended operation. The operating system/firmware must be configured securely and run with least privilege.	☐	☐	☐
B19	The HSM has the ability to return its unique device ID.	☐	☐	☐
B20	HSMs that are designed to include both a PCI mode and a non-PCI mode must not share secret or private keys between the two modes, must provide indication as to when the HSM is in PCI mode and not in PCI mode, and must require dual authentication when switching between the two modes.	☐	☐	☐

C – Policy and Procedures

Number	Description of Requirement	Yes	No	N/A
C1	A user-available security policy from the vendor addresses the proper use of the HSM in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the HSM and indicate the services available for each role in a deterministic tabular format. The HSM is capable of performing only its designed functions, i.e., there is no hidden functionality. The only approved functions performed by the HSM are those allowed by the policy.	☐	☐	☐

D – Device Security Requirements During Manufacturing

The HSM manufacturer, subject to Association site inspections, confirms the following. The PCI test laboratories do not currently validate this information; however, the vendor is still required to complete these forms and the information will be reported to PCI for review and, if necessary, corrective action.

Number	Description of Requirement	Yes	No	N/A
D1	Change-control procedures are in place so that any intended change to the physical or functional capabilities of the HSM causes a re-certification of the device under the Physical Security Requirements or the Logical Security Requirements of this document. Immediate re-certification is not required for changes which purely rectify errors and faults in software in order to make it function as intended and do not otherwise remove, modify, or add functionality.	☐	☐	☐
D2	The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing lifecycle, e.g., using dual control or standardized cryptographic authentication procedures.	☐	☐	☐
D3	The HSM is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Physical Security Requirements evaluation, and that unauthorized substitutions have not been made.	☐	☐	☐
D4	Production software (e.g., firmware) that is loaded to devices at the time of manufacture is transported, stored, and used under the principle of dual control, preventing unauthorized modifications and/or substitutions.	☐	☐	☐
D5	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the HSM and any of its components are stored in a protected, access-controlled area or sealed within tamper-evident packaging to prevent undetected unauthorized access to the device or its components.	☐	☐	☐
D6	If the HSM will be authenticated at the facility of initial deployment by means of secret information placed in the device during manufacturing, this secret information is unique to each HSM, unknown and unpredictable to any person, and installed in the HSM. Secret information is installed under dual control to ensure that it is not disclosed during installation, or the device may use an authenticated public-key method.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
D7	Security measures are taken during the development and maintenance of HSM security related components. The manufacturer must maintain development-security documentation describing all the physical, procedural, personnel, and other security measures that are necessary to protect the integrity of the design and implementation of the HSM security-related components in their development environment. The development-security documentation shall provide evidence that these security measures are followed during the development and maintenance of the HSM security-related components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the HSM security-related components.	☐	☐	☐
D8	Controls exist over the repair process and the inspection/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.	☐	☐	☐

E – Device Security Requirements Between Manufacturer and Point of Initial Deployment

The HSM manufacturer, subject to association site inspections, confirms the following. The PCI test laboratories do not currently validate this information; however, the vendor is still required to complete these forms, and the information will be reported to PCI for review and, if necessary, corrective action.

Number	Description of Requirement	Yes	No	N/A
E1	The HSM should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the HSM. Where this is not possible, the HSM is shipped from the manufacturer's facility to the facility of initial deployment and stored en route under auditable controls that can account for the location of every HSM at every point in time. Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage that they are managing is compliant with this requirement.	☐	☐	☐
E2	Procedures are in place to transfer accountability for the device from the manufacturer to the facility of initial deployment. Where the device is shipped via intermediaries such as resellers, accountability will be with the intermediary from the time at which they receive the device until the time it is received by the next intermediary or the point of initial deployment.	☐	☐	☐
E3	While in transit from the manufacturer's facility to the facility of initial deployment, the device is: ⊡ Shipped and stored in tamper-evident packaging; and/or ⊡ Shipped and stored containing a secret that: • Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and • Can be verified by the initial-key-loading facility, but that cannot feasibly be determined by unauthorized personnel.	☐	☐	☐
E4	The device's development-security documentation must provide means to the facility of initial deployment to assure the authenticity of the TOE security-relevant components.	☐	☐	☐
E5	If the manufacturer is in charge of initial-key loading, the manufacturer must verify the authenticity of the HSM security-related components.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
E6	If the manufacturer is not in charge of initial-key loading, the manufacturer must provide the means to the facility of initial deployment to assure the verification of the authenticity of the HSM security-related components.	☐	☐	☐
E7	Each device shall have a unique visible identifier affixed to it or should be identifiable using secure, cryptographically-protected methods.	☐	☐	☐
E8	The vendor must maintain a manual that provides instructions for the operational management of the HSM. This includes instructions for recording the entire life cycle of the HSM security-related components and of the manner in which those components are integrated into a single HSM, e.g.: • Data on production and personalization • Physical/chronological whereabouts • Repair and maintenance • Removal from operation • Loss or theft	☐	☐	☐

Compliance Declaration – General Information – Form A

This form and the requested information are to be completed and returned along with the completed information in the applicable Evaluation Module forms.

HSM Manufacturer Information			
HSM Manufacturer:			
Address 1:			
Address 2:			
City:		**State/Prov:**	
Country:		**Mail Code:**	
Primary Contact:			
Position/Title:			
Telephone No:		**Fax:**	
E-mail Address:			

Compliance Declaration Statement – Form B

Compliance Declaration	
HSM Manufacturer:	
Model Name and Number:	
I, *(Name)*	
☐ Am an officer of the above company, authorized to verify compliance of the referenced equipment. ☐ Am an officer of the designated laboratory, authorized by the manufacturer to verify compliance of the referenced equipment.	
I hereby attest that the above-referenced model of HSM is: ☐ In full compliance with the standards set forth above in the Manufacturer Self-Assessment Form. ☐ Not in full compliance with the standards set forth above in the Manufacturer Self-Assessment Form as indicated in the attached Exception Form (*Form C*).	

Signature ✳	*Date* ✳
Printed Name ✳	*Title* ✳

At the end of this form under "Device Specification Sheet," attach a sheet highlighting device characteristics, including photos. These photos are to include both external and internal pictures of the device. The internal pictures are to be sufficient to show the various components of the device.

Compliance Declaration Exception – Form C

HSM Manufacturer:	
Model Name and Number:	

Instructions

For any statement, A1-A7, B1-B20, C1, D1-8 or E1-E8, for which the answer was a "NO" or an "N/A," explain why the answer was not "YES."

Statement Number	Explanation

Glossary

Term	Definition
Access Controls	Controls to ensure that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity.
Active Erasure	Mechanism that intentionally clears data from storage through a means other than simply removing power (e.g. zeroization, inverting power).
Advanced Encryption Algorithm (AES)	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
ANSI (ANS)	American National Standards Institute. A U.S. standards accreditation organization.
Application Programming Interface (API)	A source code interface that a computer system or program library provides to support requests for services to be made of it by a computer program.
Asymmetric Cryptographic Algorithm	See *Public Key Cryptography.*
Asymmetric Key Pair	A public key and related private key created by and used with a public-key cryptosystem.
Audit Journal	A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results.
Audit Trail	See *Audit Journal.*
Authentication	The process for establishing unambiguously the identity of an entity, process, organization, or person.
Authorization	The right granted to a user to access an object, resource or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource or function.
Availability	Ensuring that legitimate users are not unduly denied access to information and resources.
Base (Master) Derivation Key (BDK)	See *Derivation Key.*

Term	Definition
Check Value	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible. Check values shall not allow the determination of the secret key.
Ciphertext	An encrypted message.
Clear-text	See *Plaintext.*
Compromise	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
Computationally Infeasible	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it with the current or predicted power of computers.
Conditional Test	A test performed by a cryptographic module when the conditions specified for the test occur.
Confidentiality	Ensuring that information is not disclosed or revealed to unauthorized persons, entities, or processes.
Critical Functions	Those functions that, upon failure, could lead to the disclosure of CSPs. Examples of critical functions include but are not limited to random number generation, cryptographic algorithm operations, and cryptographic bypass.
Critical Security Parameters (CSP)	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and personal identification numbers (PINs)) whose disclosure or modification can compromise the security of a cryptographic module.
Cryptographic Boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware and software components of a cryptographic module.
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines: - The transformation of plaintext data into ciphertext data, - The transformation of ciphertext data into plaintext data, - A digital signature computed from data, - The verification of a digital signature computed from data, - An authentication code computed from data, or - An exchange agreement of a shared secret.

Term	Definition
Cryptographic Key Component (Key Component)	One of at least two parameters having the characteristics (for example, format, randomness) of a cryptographic key that is combined with one or more like parameters, for example, by means of modulo-2 addition, to form a cryptographic key. Throughout this document, key component may be used interchangeably with secret share or key fragment.
Cryptoperiod	Time during which a key can be used for signature verification or decryption; it should extend well beyond the lifetime of a key (where the lifetime is the time during which a key can be used to generate a signature and/or perform encryption).
Cryptosystem	A system used for the encryption and decryption of data.
Data Encryption Algorithm (DEA)	A published encryption algorithm used to protect critical information by enciphering data based upon a variable secret key. The Data Encryption Algorithm is defined in ***ANSI X3.92:*** *Data Encryption Algorithm* for encryption and decrypting data.
Decipher	See *Decrypt.*
Decrypt	A process of transforming ciphertext (unreadable) into plaintext (readable).
Decryption	See *Decrypt.*
Derivation Key	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the Derived Unique Key Per Transaction key management method. Derivation keys are normally used in a transaction-receiving (e.g., acquirer) TRSM in a one-to-many relationship to derive or decrypt the Transaction (the derived keys) Keys used by a large number of originating (e.g., terminals) TRSMs.
DES	Data Encryption Standard (see *Data Encryption Algorithm*). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm.
Device	See *Secure Cryptographic Device.*
Dictionary Attack	Attack in which an adversary builds a dictionary of plaintext and corresponding ciphertext. When a match can be made between intercepted ciphertext and dictionary-stored ciphertext, the corresponding plaintext is immediately available from the dictionary.
Differential Power Analysis (DPA)	An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.
Digital Signature	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.

Term	Definition
Double-Length Key	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDES cryptographic algorithm.
DTP	Detailed Test Procedure
DTR	Derived Test Requirement
Dual Control	A process of using two or more separate entities (usually persons), operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key-generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see *Split Knowledge.*
DUKPT	Derived Unique Key Per Transaction: a key-management method that uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction originating TRSM. The unique transaction keys are derived from a base-derivation key using only non-secret data transmitted as part of each transaction.
ECB	Electronic codebook
EEPROM	Electronically erasable programmable read-only memory
EFP	Environmental failure protection
EFTPOS	Electronic funds transfer at point of sale
Electromagnetic Emanations (EME)	An intelligence-bearing signal, which, if intercepted and analyzed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment.
Electronic Code Book (ECB) Operation	A mode of encryption using a symmetric encryption algorithm, such as DEA, in which each block of data is enciphered or deciphered without using an initial chaining vector or previously (encrypted) data blocks.
Electronic Key Entry	The entry of cryptographic keys into a security cryptographic device in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.
Encipher	See *Encrypt.*
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data, i.e., the process of transforming plaintext into ciphertext.
Encrypted Key (Ciphertext Key)	A cryptographic key that has been encrypted with a key-encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.
Encryption	See *Encrypt.*
Entropy	The uncertainty of a random variable.
EPROM	Erasable programmable read-only memory.

Term	Definition
Error State	A state wherein the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service, or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.
Evaluation Laboratory	Independent entity that performs a security evaluation of the HSM against the PCI Security Requirements.
Exclusive-OR	Binary addition with no carry, also known as modulo 2 addition, symbolized as "XOR" and defined as: 0 + 0 = 0 0 + 1 = 1 1 + 0 = 1 1 + 1 = 0
FIPS	Federal Information Processing Standard.
Firmware	Any code within the HSM that provides security protections needed to comply with these HSM security requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under these HSM security requirements.
Hardware (Host) Security Module (HSM)	See *Secure Cryptographic Device.*
Hash	A (mathematical) function, which is a non-secret algorithm, which takes any arbitrary length message as input and produces a fixed length hash result. Approved hash functions satisfy the following properties: 1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output. 2) Collision Resistant. It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output. It may be used to reduce a potentially long message into a "hash value" or "message digest" which is sufficiently compact to be input into a digital signature algorithm. A "good" hash is such that the results of applying the function to a (large) set of values in a given domain will be evenly (and randomly) distributed over a smaller range.
Hexadecimal Character	A single character in the range 0-9, A-F (upper case), representing a four-bit string

Term	Definition
Initialization Vector (IV)	A binary vector used as the input to initialize the algorithm (a stream or block cipher) for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals.
IPsec	Internet Protocol security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
Irreversible Transformation	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.
ISO	International Organization for Standardization. An international standards setting organization composed of representatives from various national standards.
Joint Interpretation Library (JIL)	A set of documents agreed upon by the British, Dutch, French and German Common Criteria Certification Bodies to provide a common interpretation of Common Criteria for composite evaluations, attack paths, attack quotations, and methodology.
KEK	See *Key-Encrypting Key.*
Key	See *Cryptographic Key.*
Key (Secret) Share	One of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that less than a quorum does not provide any information about the key.
Key Agreement	A key establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
Key Archive	Process by which a key no longer in operational use at any location is stored.
Key Backup	Storage of a protected copy of a key during its operational use.
Key Bundle	The three cryptographic keys (K1, K2, K3) used with a TDEA mode.
Key Component	See *Cryptographic Key Component.*
Key Deletion	Process by which an unwanted key, and information from which the key may be reconstructed, is destroyed at its operational storage/use location.

Term	Definition
Key Destruction	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location. Information may still exist at the location from which the key may be feasibly reconstructed.
Key-distribution host (KDH)	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to the EPP or PED and the financial-processing platform communicating with those EPPs/PEDs. A KDH may be an application that operates on the same platform that is used for PIN translation and financial-transaction processing. The KDH may be used in conjunction with other processing activities. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys.
Key-Encrypting (Encipherment Or Exchange) Key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys. Also known as a key-encryption or key-exchange key.
Key Establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key Fragment	See *Cryptographic Key Component.*
Key Generation	Creation of a new key for subsequent use.
Key Instance	The occurrence of a key in one of its permissible forms, that is, plaintext key, key components and enciphered key.
Key Loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.
Key Pair	Two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is known only to the appropriate entities.
Key Replacement	Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.
Key Storage	Holding of the key in one of the permissible forms.
Key Termination	Occurs when a key is no longer required for any purpose and all copies of the key and information required to regenerate or reconstruct the key have been deleted from all locations where they ever existed.
Key Transport	A key establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
Key Usage	Employment of a key for the cryptographic purpose for which it was intended

Term	Definition
Key Variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Key-Loading Device	A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
Keying Material	The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships.
Legitimate Use	Ensuring that resources are used only by authorized persons in authorized ways.
Manual Key Distribution	The distribution of cryptographic keys, often in a plaintext form requiring physical protection, but using a non-electronic means, such as a bonded courier.
Manual Key Entry	The entry of cryptographic keys into a secure cryptographic device, using devices such as buttons, thumb wheels, or a keyboard.
Master Derivation Key (MDK)	See *Derivation Key.*
Master Key	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a Master Key. May also be known as Master File Key or Local Master Key, depending on the vendor's nomenclature.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data (example: a Hash-Based Message Authentication Code).
Non-Reversible Transformation	See *Irreversible Transformation.*
Opaque	Impenetrable by light (i.e., light within the visible spectrum of wavelength range of 400nm to 750nm); neither transparent nor translucent within the visible spectrum.
Operator	An individual accessing a cryptographic module or a process (subject) operating on behalf of the individual, regardless of the assumed role.
Passive Erasure	Mechanism that clears data from storage through removal of power.
Password	A string of characters used to authenticate an identity or to verify access authorization.
Personal Identification Number (PIN)	A numeric personal identification code that authenticates a cardholder in an authorization request that originates at a terminal with authorization only or data capture only capability. A PIN consists only of decimal digits.
Physical Protection	The safeguarding of a secure cryptographic device or of cryptographic keys or other critical security parameters using physical means.

Term	Definition
Physically Secure Environment	An environment that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or a room built with continuous access control, physical security protection, and monitoring.
PIN	See *Personal Identification Number.*
PIN-Encipherment Key (PEK)	A PEK is a cryptographic key that is used for the encryption or decryption of PINs.
PIN Entry Device (PED)	A device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor and storage for PIN processing sufficiently secure for the key management scheme used, and firmware. A PED has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell.
Plaintext	The intelligible form of an encrypted text or of its elements.
Plaintext Key	An unencrypted cryptographic key, which is used in its current form.
Private Key	A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.
PRNG	Pseudo-random number generator.
PROM	Programmable read-only memory.
Pseudo-Random	A process that is statistically random, and essentially unpredictable, although generated by an algorithmic process.
Public Key	A cryptographic key, used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Term	Definition
Public Key (Asymmetric) Cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques, such as RSA, there are four elementary transformations: sign and verify for signature systems, and encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exists asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and where used the four elementary transformations and the corresponding keys should be kept separate. See *Asymmetric Cryptographic Algorithm.*
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware based 'noise' mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
Removable Cover	A part of a cryptographic module's enclosure that permits physical access to the contents of the module.
RNG	Random number generator.
ROM	Read-only memory.
RSA Public Key Cryptography	Public key cryptosystem that can be used for both encryption and authentication.
Salt	A random string that is concatenated with other data prior to being operated on by a one-way function. A salt should have a minimum length of 64-bits.
Secret Key	A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. A secret key (symmetrical) cryptographic algorithm uses a single secret key for both encryption and decryption. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.
Secret Key (Symmetric) Cryptographic Algorithm	A cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Term	Definition
Secret Share	See *Key Share.*
Secure Cryptographic Device	A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes or both, including cryptographic algorithms.
Secure Cryptoprocessor	A secure cryptoprocessor is a dedicated computer on a chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures that give it a degree of tamper resistance.
Secure Key Loader	A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
Security Policy	A description of how the specific module meets these security requirements, including the rules derived from this standard and additional rules imposed by the vendor.
Sensitive (Secret) Data (Information)	Data that must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs, and secret and private cryptographic keys, and includes design characteristics, status information, and so forth.
Sensitive Functions	Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs and passwords.
Sensitive Services	Sensitive services provide access to the underlying sensitive functions.
Session Key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g., an encryption key and a MAC key.
SHA-1	Secure Hash Algorithm. SHA-1 produces a 160-bit message digest.
SHA-2	A set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512). SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.
Shared Secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key-derivation function to derive session keys.
Single-Length Key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
SK	Session key.
Split Knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
SSL	Secure Sockets Layer.
Status Information	Information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.

Term	Definition
Strong	Not easily defeated; having strength or power greater than average or expected; able to withstand attack; solidly built.
Symmetric (Secret) Key	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
Tamper Detection	The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.
Tamper-Evident	A characteristic that provides evidence that an attack has been attempted.
Tamper-Resistant	A characteristic that provides passive physical protection against an attack.
Tamper-Responsive	A characteristic that provides an active response to the detection of an attack.
Tampering	The penetration or modification of an internal operation and/or insertion of active or passive tapping mechanisms to determine or record secret data or to alter the operation of the device.
TDEA	See Triple Data Encryption Algorithm.
TDES	See Triple Data Encryption Standard.
TECB	TDEA electronic codebook.
TLS	Transport Layer Security.
TOE	Target of evaluation.
Triple Data Encryption Algorithm (TDEA)	The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.
Triple Data Encryption Standard (TDES)	See *Triple Data Encryption Algorithm.*
Triple-Length Key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.
Unprotected Memory	Components, devices, and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a secure cryptographic device.
User	Individual or (system) process authorized to access an information system or that makes use of the trust model to obtain the public key of another user. An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.
UserID	A string of characters that uniquely identifies a user to the system.
Variant of a Key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key. For example exclusive-OR'ing a non-secret constant with the original key.
Verification	The process of associating and/or checking a unique characteristic.

Term	Definition
Working Key	A key used to cryptographically process the transaction. A Working Key is sometimes referred to as a data key, communications key, session key, or transaction key.
XOR	See *Exclusive-OR.*
Zeroization (zeroize)	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.
Zeroized	The state after zeroization has occurred.

Device Specification Sheet

As instructed under “Required Device Information” and “Compliance Declaration Statement – Form B,” use this section to attach a device-specification sheet that provides:

1. A description of device characteristics
2. External photos
3. Internal photos, sufficient to show the various components of the device