Payment Card Industry (PCI)

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

Modular Security Requirements

Version 4.0

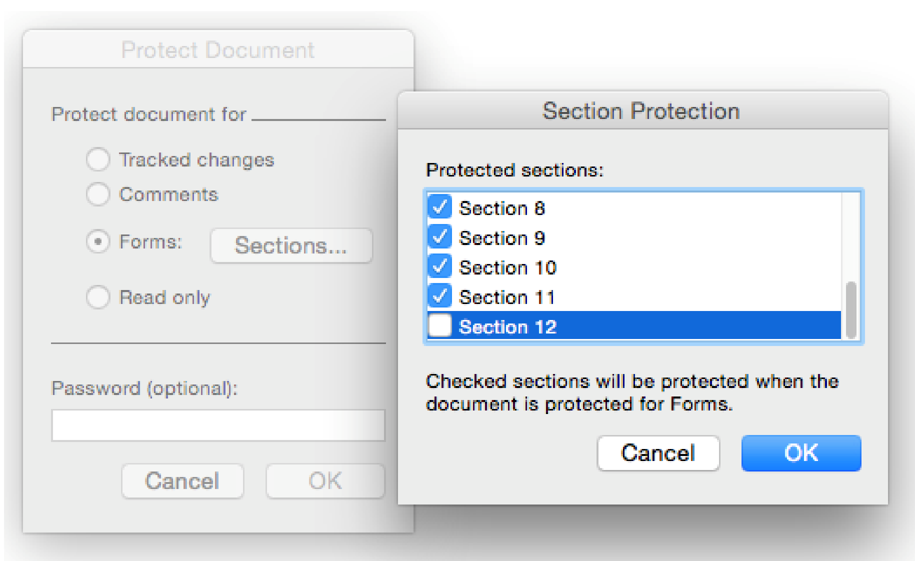
December 2021

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
February 2016	3.x	PCI	RFC version
June 2016	3.0	PCI	Requirements for key-loading devices and HSM remote administration platform requirements added. Device Management Information submitted by vendors is now validated. See *PCI PTS HSM - Summary of Requirements Changes from Version 2.0 to 3.0.*
December 2021	4.0	PCI	Added new module, "Cloud-based HSMs as a Service – Multi-tenant Usage Security Requirements."

Note to Assessors

When protecting this document for use as a form, leave Section 12 (final page of this document) unprotected to allow for insertion of a device-specification sheet. Under "Tools / Protect Document," select "Forms" then "Sections," and un-check Section 12 as illustrated below.



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
- Key generation
- Key injection

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:

- 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:

Cloud-based HSMs as a Service – Multi-tenant Usage Security Requirements

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.

Life Cycle

Life cycle 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*.

Related Publications

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

Publication Title	Reference
Retail Financial Services - Symmetric Key Management	ANSI X9.24
Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	ANSI X9.42
Key Establishment Using Integer Factorization Cryptography	ANSI X9.44
Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography	ANSI 9.63
Symmetric Key Cryptography for the Financial Services Industry—Wrapping of Keys and Associated Data	ANSI X9.102
Public Key Cryptography: The Elliptical Curve Digital Signature Algorithm (EDCSA)	ANSI X9.142
Retail Financial Services - Interoperable Secure Key Block Specification	ANSI X9.143
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ASC X9 TR 31
Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport	ASC X9 TR 34
FIPS PUB 140-2: Security Requirements for Cryptographic Modules	FIPS
FIPS PUB 140-3: Security Requirements for Cryptographic Modules	FIPS
FIPS PUB 186-5: Digital Signature Standard (DSS)	FIPS
Personal Identification Number (PIN) Management and Security	ISO 9564
Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher	ISO 9797-1
Financial Services—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
Financial Services—Secure Cryptographic Devices (Retail)	ISO 13491
Financial Services — Requirements for message authentication using symmetric techniques	ISO 16609
Information Technology – Security techniques – Encryption algorithms – Part 1: General	ISO/IEC 18033-1

Publication Title	Reference
Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers	ISO/IEC 18033-3
Information Technology – Security techniques – Encryption algorithms – Part 5: Identity Based Ciphers	ISO/IEC 18033-5
Guidelines on Triple DES Modes of Operation	ISO TR 19038
Banking and related financial services -- Key wrap using AES	ISO 20038
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	NIST SP 800-22
Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication	NIST SP 800-38B
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
Recommendation for Random Number Generation Using Deterministic Random Bit Generators	NIST SP 800-90A Revision 1
Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	NIST SP 800-131A Revision 2
Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters	NIST SP 800-186
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

December 2021

<table>
<tr><th colspan="26">HSM Identifier</th></tr>
<tr><td>Device Manufacturer:</td><td colspan="25"></td></tr>
<tr><td>Marketing Model Name/Number:</td><td colspan="25"></td></tr>
<tr><td rowspan="3">Hardware Version Number[A]:
Use of "x" represents a request for field to be a variable.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
<tr><td colspan="25">Additional versions:</td></tr>
<tr><td rowspan="3">Firmware Version Number[A]:
Use of "x" represents a request for field to be a variable.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
<tr><td colspan="25">Additional versions:</td></tr>
<tr><td>Firmware Version Number:</td><td colspan="25"></td></tr>
<tr><td>Application Version Number:
(if applicable)</td><td colspan="25"></td></tr>
<tr><td>Designed for deployment only in an environment meeting at least the security requirements of a controlled environment as defined in ISO 13491-2?</td><td colspan="25">Yes ☐
No ☐</td></tr>
</table>

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.

[A] See "Optional Use of Variables in the Identifier," following page.

Optional Use of Variables in the Device Identifier

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

Firmware Version Number – Request for Use of the Variable "x"

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

Evaluation Module 1: Core Requirements

A – Physical Security Requirements

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

Number	Description of Requirement	Yes	No	N/A
A1	The device 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 device, 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[B].	☐	☐	☐
A2	The security of the device is not compromised by altering environmental conditions or operational conditions (for example, subjecting the device to temperatures or operating voltages outside the stated operating ranges).	☐	☐	☐
A3	Sensitive functions or information are only used in the protected area(s) of the device. Sensitive information and functions dealing with sensitive information are protected from unauthorized modification or substitution, without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation [B].	☐	☐	☐
A4	Determination of any PCI-related secret or private cryptographic key resident in the device or used by the device, by penetration of the device requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for initial exploitation[B].	☐	☐	☐
A5	Emanations from the device (including power fluctuations and timing) cannot be feasibly used to recover PIN and/or account data or other PCI security-related cryptographic keys resident in the device.	☐	☐	☐

[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 device is operating as designed, the device runs self-tests (a) when pre-operational and at least once per day or (b) using continuous error checking, to check firmware (authenticity check), security mechanisms for signs of tampering, and whether the device is in a compromised state. When specific critical operations are performed, the device performs conditional tests. The techniques and actions of the device upon failure of a self-test are consistent with those defined in FIPS PUB 140-2/140-3.	☐	☐	☐
B2	The device'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 device outputting sensitive information.	☐	☐	☐
B3	The device must support firmware updates. The device must cryptographically authenticate the firmware, and if the authenticity is not confirmed, the firmware update is rejected and deleted. The update mechanism ensures security—i.e., integrity, mutual authentication, and protection against replay—by using an appropriate and declared security protocol when using a network connection.	☐	☐	☐
B3.1	If the device supports applications, the firmware must support the authentication of applications loaded into the device consistent with B3.	☐	☐	☐
B4	The device provides secure interfaces that are kept logically separate by distinguishing between data and control for inputs as well as between data and status for outputs.	☐	☐	☐
B5	The device must automatically clear or reinitialize its internal buffers that hold sensitive information once the information is no longer needed, including when: ▪ The transaction is completed, ▪ The device has timed out, or ▪ The device recovers from an error state.	☐	☐	☐
B6	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/authentication codes. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	☐	☐	☐

<table>
<tr><th>Number</th><th>Description of Requirement</th><th>Yes</th><th>No</th><th>N/A</th></tr>
<tr><td>B7</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>Clear-text keys</td><td>No</td><td>Yes</td><td>No</td></tr>
<tr><td>Clear-text key components</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td>Enciphered keys/components</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
</table></td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B8</td><td>If random numbers are generated by the device 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>B9</td><td>The device uses accepted cryptographic algorithms, modes, and key sizes.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B10</td><td>The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support key blocks as defined in DTR 77</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B11</td><td>The device ensures that if cryptographic keys within the secure device boundary are rendered invalid for any reason—e.g., tamper or long-term absence of applied power—the device will fail in a secure manner.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B12</td><td>The device 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, account-data encryption, data-encrypting key, or key-encrypting key contained in or protected by the device. The device 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>B13</td><td>There is no mechanism in the device 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 critical security parameters (CSPs) to components that could negatively impact security.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B14</td><td>If the device is designed to be used for PIN management, the device shall meet the PIN-management requirements of ISO 9564. The PIN-encryption technique implemented in the device is a technique included in ISO 9564.</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td>B15</td><td>The device includes cryptographic mechanisms to support secure logging of transactions, data, and events, to enable auditing.</td><td>☐</td><td>☐</td><td>☐</td></tr>
</table>

Number	Description of Requirement	Yes	No	N/A
B16	If the device 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 device supports virtualization such that it can act as multiple logically separate devices.	☐	☐	☐
B17	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.	☐	☐	☐
B18	The device has the ability to return its unique device ID.	☐	☐	☐
B19	Devices 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 device 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 device 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 device and indicate the services available for each role in a deterministic tabular format. The device is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the device are those allowed by the policy.	☐	☐	☐

Evaluation Module 2: Key-Loading Devices

D – Key-Loading Devices

Number	Description of Requirement	Yes	No	N/A
D1	If the device is capable of generating asymmetric key pairs and/or secret keys, the private or secret key or its precursors will not be visible in clear-text form at any time during the generation process.	☐	☐	☐
D2	If the device is capable of generating symmetric keys or asymmetric key pairs that are not used by the device, the key or key pair and all related secret and private seed elements are deleted immediately after the transfer process.	☐	☐	☐
D3	The device retains no information that could disclose any key that the device has already transferred into another cryptographic device.	☐	☐	☐
D4	If the device is composed of several components, it is not possible to move a secret or private key within the device from an asset domain of higher security to an asset domain providing lesser security.	☐	☐	☐
D5	Once the device has been loaded with cryptographic keys, there is no feasible way in which the functional capabilities of the device can be modified without causing the automatic and immediate erasure of the cryptographic keys stored within the device or causing the modification to be otherwise detected before the device is next used to load a key.	☐	☐	☐

Evaluation Module 3: Remote Administration

E – Logical Security

Number	Description of Requirement	Yes	No	N/A
E1	The device is designed in such a way that it cannot be put into operational service until the device initialization process has been completed. This will include all necessary keys and other relevant material needed to be loaded into it.	☐	☐	☐
E2	The following operator functions that may influence the security of a device are permitted only when the device is in a sensitive state—i.e., under dual or multiple control: ▪ Disabling or enabling of device functions ▪ Change of passwords/authentication codes or data that enable the device to enter the sensitive state. The secure operator interface is so designed that entry of more than one password/authentication code (or some equivalent mechanism for dual or multiple control) is required in order to enter this sensitive state and that it is highly unlikely that the device can inadvertently be left in the sensitive state.	☐	☐	☐

F – Devices with Message Authentication Functionality

Number	Description of Requirement	Yes	No	N/A
F1	If the message authentication device can be manually activated and can contain different MAC keys, the identity of the key used is displayed by the device. The device only outputs a confirmation or denial of a MAC provided for verification, never the clear-text-computed MAC.	☐	☐	☐
F2	The length of the MAC being generated or verified is in accordance with ISO 16609.	☐	☐	☐
F3	If the device uses two keys for MAC generation or verification, the technique utilized is in accordance with ISO 16609.	☐	☐	☐
F4	If the message authentication device is designed to use unidirectional MAC keys, a MAC key is only used for one type of MAC function—i.e., verify the MAC of received text or generate and output a MAC for a text being transmitted.	☐	☐	☐

G – Devices with Key-Generation Functionality

Number	Description of Requirement	Yes	No	N/A
G1	Unauthorized removal of the device from its operational location is deterred by one or more of the following mechanisms: ▪ The device includes mechanisms such that the removal of the device from its operational location will cause the automatic erasure of the cryptographic keys contained within the device; or ▪ Removal of the device would be of no benefit because its tamper-resistance or tamper-responsive characteristics ensure that the extraction of cryptographic keys or other secret data is not feasible.	☐	☐	☐
G2	The device will not output any clear-text key except under dual control. Such dual control is enforced by means such as the following: ▪ The device requires that at least two passwords/authentication codes be correctly entered within a period of no more than five minutes before the device will output a key. ▪ The device requires that at least two different, physical keys (marked "not to be commercially reproduced") be concurrently inserted in the unit before it will output a key.	☐	☐	☐
G3	The following operator functions (if available) require the use of sensitive states: ▪ Manual input of control data—e.g., key-verification code—to enable export, import or use of a key; and ▪ Permitting movement of the device without activating a key-erasure mechanism.	☐	☐	☐
G4	Any proprietary functions are either: ▪ Totally equivalent to a series of standard and approved functions; or ▪ Limited to use only keys that, by virtue of key separation, cannot be used with keys, or modified keys, of non-proprietary functions.	☐	☐	☐

H – Devices with Digital Signature Functionality

Number	Description of Requirement	Yes	No	N/A
H1	The private key is managed such that: ▪ The asymmetric private and public key pair is generated within the digital signature device; and ▪ The asymmetric private key is only exported outside the original digital signature device under dual control; and ▪ Mechanisms for the control of the use of the private key are provided.	☐	☐	☐
H2	For audit and control purposes, the binding between the public key and the identity of the owner of the private key is readily determined by: ▪ Use of public key certificates, where the public key certificate was obtained from an authorized certificate authority—e.g., the vendor's PKI; or ▪ Use of public key certificates and appropriate certificate management procedures; or ▪ Other equivalent mechanisms to irrefutably determine the identity of the owner of the corresponding private key.	☐	☐	☐

Evaluation Module 4: Cloud-based HSMs as a Service – Multi-tenant Usage and Remote Management Security Requirements

I – Cloud Physical Security Requirements

Number	Description of Requirement	Yes	No	N/A
I1	The HSM processing element must meet all PCI HSM physical and logical requirements, including protection of sensitive data to an attack potential of at least 35 per HSM processing element for identification and initial exploitation, with a minimum of 15 for initial exploitation[A].	☐	☐	☐
I2	HSM virtualization systems must be either: ▪ Installed and operated in an environment meeting at least the security requirements of a controlled environment, or ▪ Protect the stored and processed sensitive data to an attack potential of at least 26 per HSM virtualization system for identification and initial exploitation, with a minimum of 13 for initial exploitation[A].	☐	☐	☐
I3	HSM virtualization systems that provide for switching/routing of secure channels between the HSM Solution Consumer and one or more HSM processing elements, must manage the cryptographic keys and operations used for these functions within a tamper-responsive system (to attack potential of at least 26 per HSM virtualization system for identification and initial exploitation, with a minimum of 13 for initial exploitation[A].	☐	☐	☐
I4	Where the HSM processing element and HSM virtualization system are contained in the same physical execution environment, the HSM virtualization system must meet all HSM processing element security requirements.	☐	☐	☐
I5	The HSM processing element must ensure that clear-text secret and private keys are processed in execution paths and memory areas that are isolated from keys of any other HSM Solution Consumer and/or code that is not included in the scope of the HSM processing element evaluation.	☐	☐	☐

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

J – Cloud Logical Security Requirements

Number	Description of Requirement	Yes	No	N/A
J1	It must not be possible to import or export the keys of an HSM Solution Consumer from the HSM processing element without approval from the HSM Solution Consumer. The approval must be cryptographically authenticated.	☐	☐	☐
J2	Each HSM processing element must require the use of cryptographic methods for identification and authentication prior to the provisioning of secret keys, or establishment of any logical secure channel.	☐	☐	☐
J3	Operations performed with the cryptographic keys of an HSM Solution Consumer must require a cryptographically verifiable approval or request from the key owner.	☐	☐	☐
J4	Clear-text sensitive data, including PINs and secret/private cryptographic keys, must never be exposed outside of an HSM processing element. Clear-text cardholder data, including PAN data, must be managed within an HSM processing element or an environment compliant to PCI DSS.	☐	☐	☐
J5	All key-management operations involving the cryptographic key of HSM Solution Consumers, including validation of key wrapping, must be performed within the HSM processing element.	☐	☐	☐
J6	All HSM processing element storage areas, temporary or otherwise, must be cleared of sensitive data prior to allowing processing using a set of cryptographic keys belonging to another HSM Solution Consumer. This includes but is not limited to registers, cache, scratchpad memory, etc. Erasure must accommodate for any memory virtualization or wear-leveling implemented in the system.	☐	☐	☐
J7	Each HSM Solution must be able to provide a cryptographically verifiable, unique ID that includes unique identification of the hardware and firmware versions of each HSM processing element and HSM virtualization system used in that solution. Any and all updates to the firmware must be logged and include references to previous ID numbers if the firmware updates these.	☐	☐	☐
J8	Firmware updates for HSM processing elements must be signed using a dual-control process, using cryptographic keys maintained within a FIPS 140-2/3 level 3 or higher HSM or a PCI-approved HSM. The firmware update method must prevent installation of any version of firmware older than the currently installed version unless all cryptographic keys are erased from the HSM processing element.	☐	☐	☐

K – Cloud Provisioning / Management Security Requirements

Number	Description of Requirement	Yes	No	N/A
K1	Connections between the HSM virtualization system, HSM processing elements, as well as to any HSM Solution Consumers, must implement a secure channel. The HSM Solution must support independent secure channels for interfaces to HSM Solution Providers and HSM Solution Consumers, including independent secure channels for each unique HSM Solution Consumer.	☐	☐	☐
K2	Updates to the HSM Solution that may impact the configuration or operation of that solution must be approved by the HSM Solution Consumers prior to implementing the change. If the HSM Solution Consumer is able to update or configure the firmware and/or settings of the HSM Solution with which they interface, such configuration must be isolated from any other HSM Solution Consumers.	☐	☐	☐
K3	Changes to HSM configuration options that may affect the compliance of an HSM Solution Customer must be cryptographically authenticated. Changes made by one HSM Solution Consumer must not affect the compliance status of any other HSM Solution Consumer.	☐	☐	☐
K4	The HSM processing element must establish a unique provisioning key for each HSM Solution Consumer. Key establishment must implement a key-agreement process, such as Diffie-Hellman, which provides perfect forward secrecy.	☐	☐	☐
K5	HSM processing element tamper keys used to protect the keys of more than one HSM Solution Consumer must be unique per HSM processing element. This key must be generated within the HSM processing element using an approved random number generation process, and must not be exportable, or able to be disclosed, outside of the HSM by any means.	☐	☐	☐
K6	The HSM Solution must support the ability to disable or suspend access to cryptographic keys owned by an HSM Solution Consumer for any HSM processing element	☐	☐	☐
K7	It must be possible for an HSM Solution Consumer to maintain an external log of all HSM operations, indicating which HSM virtualization system(s) and HSM processing element(s) were involved in all operations performed.	☐	☐	☐
K8	Where it is possible that more than one HSM processing element may be operating on the cryptographic keys of the same HSM Solution Consumer at any one time, these HSM processing elements must be maintained in an environment meeting at least the security requirements of a controlled environment. ***Note:*** *This requirement is designed to reduce the risk of key compromise as the cryptographic keys of HSM Solution Consumers are spread across multiple HSM processing elements for the purpose of elastic processing.*	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
K9	There must be a publicly available security policy that outlines how the HSM Solution is implemented, what cryptographic services are provided, how the HSM Solution Consumer and components of the HSM Solution are authenticated, and how to securely disable or deprecate the storage of cryptographic keys of specific HSM Solution Consumers from any or all components of that solution.	☐	☐	☐
K10	The HSM Solution must implement a public vulnerability management and disclosure policy. This must provide: ▪ Methods for the secure disclosure to the impacted user organization of any vulnerabilities as they are found, ▪ Ranking and addressing vulnerabilities in a timely matter, and ▪ Methods for any HSM Solution Consumers of the HSM Solution to be informed of the vulnerabilities.	☐	☐	☐

Evaluation Module 5: Life Cycle Security Requirements

L – Device Security Requirements During Manufacturing

Note: *In the following requirements, the device under evaluation is referred to as the "device."*

The device manufacturer, subject to PCI payment brand site inspections, confirms the following. The PCI test laboratories will validate this information via documentation reviews and by means of evidence that procedures are properly implemented and used. Any variances to these requirements will be reported to PCI for review.

Number	Description of Requirement	Yes	No	N/A
L1	Change-control procedures are in place so that any intended change to the physical or functional capabilities of the device causes a re-certification of the device under the impacted security requirements of this document. Immediate re-certification is not required for changes that purely rectify errors and faults in software in order to make it function as intended and do not otherwise remove, modify, or add functionality.	☐	☐	☐
L2	The firmware and any changes thereafter have been inspected and reviewed using a documented and auditable process and verified by the vendor as being free from hidden and unauthorized or undocumented functions.	☐	☐	☐
L3	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.	☐	☐	☐
L4	The device is assembled in a manner that the hardware components used in the manufacturing process are those hardware components certified by the Section A Security Requirements evaluation, and that unauthorized substitutions have not been made.	☐	☐	☐
L5	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.	☐	☐	☐
L6	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, the device 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 and to prevent unauthorized modifications to the physical or functional characteristics of the device.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
L7	The device 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 device, unknown and unpredictable to any person, and installed in the device. 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. Authentication by secret information is mandatory in HSM v4.	☐	☐	☐
L8	Security measures are taken during the development and maintenance of device's 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 device's 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 device's security-related components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the device's security-related components.	☐	☐	☐
L9	Controls exist over the repair process and the subsequent inspection/testing process to ensure that the device has not been subject to unauthorized modification.	☐	☐	☐

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

Note: *In the following requirements, the device under evaluation is referred to as the “device.”*

The device manufacturer, subject to PCI payment brand site inspections, confirms the following. The PCI test laboratories will validate this information via documentation reviews and by means of evidence that procedures are properly implemented and used. Any variances to these requirements will be reported to PCI for review.

Note: *“Initial key loading” pertains to the loading of payment transaction keys used by the acquiring organization.*

Number	Description of Requirement	Yes	No	N/A
M1	The device should be protected from unauthorized modification with tamper-detection 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 device. Where this is not possible, the device 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 device 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 they are managing is compliant with this requirement.	☐	☐	☐
M2	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. In the absence of defined agreements stipulating otherwise, the device vendor remains responsible.	☐	☐	☐

M3	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 cannot feasibly be determined by unauthorized personnel.
		☐	☐	☐

M4	The device’s development-security documentation must provide means to the facility of initial deployment to assure the authenticity of the TOE’s security-relevant components.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
M5	If the manufacturer is in charge of initial key loading, the manufacturer must verify the authenticity of the device's security-related components.	☐	☐	☐
M6	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 device's security-related components.	☐	☐	☐
M7	Each device shall have a unique visible identifier affixed to it—i.e., model name and hardware version—and shall be retrievable by a query using secure, cryptographically protected methods.	☐	☐	☐
M8	The vendor must maintain a manual that provides instructions for the operational management of the device. This includes instructions for recording the entire lifecycle of the device's security-related components and the manner in which those components are integrated into a single device—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.

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

Compliance Declaration Statement – Form B

Compliance Declaration	
Device 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 device is: ☐ In full compliance with the standards set forth above in this document ☐ Not in full compliance with the standards set forth above in this document 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

Device Manufacturer:	
Model Name and Number:	

Instructions

For any statement, A1-A7, B1-B19, 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

Appendix A: Requirements Applicability Matrix

Inside evaluation modules, requirements applicability depends upon the functionalities a device under test provides. Four functionalities have been identified, as shown below.

Functionality	Description
HSM	This is functionality that must be met by all HSM approval classes as delineated in Appendix B—i.e., Hardware Security Module, Key-Loading Device, Remote Administration Platform and Multi-tenant HSM.
Key-Loading Devices	This is functionality that must be met by devices that perform key injection of either clear-text or enciphered keys or their components. The devices may perform other services such as key generation.
Remote Administration	This is for platforms that are used for remote administration of HSMs. Such administration may include device configuration and key-loading services.
Multi-tenant HSM	This is functionality that must be met by HSMs intended for multi-tenant usage—i.e., concurrent multi-organizational usage.
Remote-managed HSM	This is functionality that must be met by HSMs that will be remotely managed and are dedicated for usage by a specific organization.

Appendix B: Applicability of Requirements

Having identified functionalities, a device under evaluation needs to meet or exceed requirements formed by the union of all requirements applicable to each of the functionalities. Please refer to Appendix A: Requirements Applicability Matrix.

For compound devices, it is possible that these requirements are met or exceeded by the relevant module(s) if the corresponding requirements are fully covered; however, it remains up to the testing house's judgment to evaluate on a case-by-case basis whether supplementary testing is required.

To determine which requirements apply to a device, the following steps must take place:

1. Identify which of the functionalities the device supports.
2. For each of the supported functionalities, report any marking "X" corresponding to the listed requirement. "X" stands for "applicable," in which case the requirement must be considered for evaluation. In all cases, if a security requirement is impacted, the device must be assessed against it.

Requirement	HSM	Key Loading	Remote Admin	Multi-tenant HSM	Remote-Man. HSM	Conditions
	Hardware Security Module					
	Core Physical Security Requirements					
A1	X	X		X	X	
A2	X	X		X	X	
A3	X	X	X	X	X	
A4	X	X		X	X	
A5	X	X		X	X	
	Core Logical Security Requirements					
B1	X	X	X	X	X	
B2	X	X		X	X	
B3	X	X		X	X	
B3.1	X	X		X	X	
B4	X	X		X	X	
B5	X	X		X	X	
B6	X	X	X	X	X	
B7	X	X		X	X	
B8	X	X	X	X	X	
B9	X	X	X	X	X	

Requirement	HSM	Key Loading	Remote Admin	Multi-tenant HSM	Remote-Man. HSM	Conditions
	Core Logical Security Requirements (continued)					
B10	X	X	X	X	X	
B11	X	X	X	X	X	
B12	X	X		X	X	
B13	X			X	X	
B14	X			X	X	
B15	X	X		X	X	
B16	X	X		X	X	
B17	X	X		X	X	
B18	X	X		X	X	
B19	X			X	X	
	Policy and Procedures Requirements					
C1	X	X	X	X	X	
	Key-Loading Devices					
D1		X	X			
D2		X	X			
D3		X	X			
D4		X	X			
D5		X	X			
	Remote Administration Platform					
	Logical Security					
E1			X			
E2			X			
	Devices With Message Authentication Functionality					
F1			X			
F2			X			
F3			X			
F4			X			

Requirement	HSM	Key Loading	Remote Admin	Multi-tenant HSM	Remote-Man. HSM	Conditions
	Devices With Key-Generation Functionality					
G1			X			
G2		X	X			
G3		X	X			
G4			X			
	Devices With Digital Signature Functionality					
H1			X			
H2			X			
	Cloud-based HSMs as a Service – Multi-tenant Usage Security					
	Cloud Physical Security					
I1				X		
I2				X		
I3				X		
I4				X		
I5				X		
	Cloud Logical Security					
J1				X	X	
J2				X	X	
J3				X	X	
J4				X	X	
J5				X	X	
J6				X		
J7				X	X	
J8				X	X	
	Cloud Provisioning/Management Security					
K1				X	X	1st statement Multi-tenant only
K2				X		
K3				X		

Requirement	HSM	Key Loading	Remote Admin	Multi-tenant HSM	Remote-Man. HSM	Conditions
	Cloud Provisioning/Management Security (continued)					
K4				X		
K5				X		
K6				X		
K7				X		
K8				X		
K9				X	X	
K10				X	X	
	Life Cycle					
	During Manufacturing					
L1	X	X	X	X	X	
L2	X	X	X	X	X	
L3	X	X	X	X	X	
L4	X	X	X	X	X	
L5	X	X	X	X	X	
L6	X	X	X	X	X	
L7	X	X	X	X	X	
L8	X	X	X	X	X	
L9	X	X	X	X	X	
	Between Manufacturer and Point of Initial Deployment					
M1	X	X	X	X	X	
M2	X	X	X	X	X	
M3	X	X	X	X	X	
M4	X	X	X	X	X	
M5	X	X	X	X	X	
M6	X	X	X	X	X	
M7	X	X	X	X	X	
M8	X	X	X	X	X	

Glossary

Term	Definition
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity.
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(s)	Any code or script that is not firmware and can be loaded onto the device.
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.
Atomic	A single command that has a defined set of input criteria/values and a defined set of output responses. No intermediate responses, states, or indications of operation are returned until the defined output is provided. For example, chaining together a set of common and related commands (MAC verify, verify PIN, check CVV, check cryptogram, etc.) to minimize traffic on the HSM link.
Audit Trail	A chronological record of system activities that 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.
Authentication	The process for establishing unambiguously the identity of an entity, process, organization, or person.
Authentication Code	See *Password*.
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. A value used to identify a key without revealing any bits of the actual key itself. Check values are computed by encrypting an all-zero block using the key or component as the encryption key, using the leftmost n-bits of the result; where n is at most 24 bits (6 hexadecimal digits/3 bytes). This method may be used for TDEA. TDEA may optionally use, and AES shall use a technique where the KCV is calculated by MACing an all-zero block using the CMAC algorithm as specified in ISO 9797-1 (see also NIST SP 800-38B). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MACed using the TDEA block cipher, while a 128-bit AES key or component will be MACed using the AES-128 block cipher.
Ciphertext	An encrypted message.
Clear text	The intelligible form of an encrypted text or of its elements—e.g., components.
Clear-text Key	An unencrypted cryptographic key, used in its current form.
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 clear-text 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/authentication codes—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.

Term	Definition
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of clear-text data into ciphertext data, ▪ The transformation of ciphertext data into clear-text 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.
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.
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 clear text (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 TRSMs—e.g., terminals.
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*.
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.
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.

Term	Definition
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 Loading	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.
Elliptic-curve cryptography (ECC)	ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
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 clear text into ciphertext.
Encrypted Key (Ciphertext Key)	A cryptographic key that has been encrypted with a key-encrypting key, a PIN, or a password/authentication code in order to disguise the value of the underlying clear-text key.
Encryption	See *Encrypt*.
Entropy	The uncertainty of a random variable.

Term	Definition
Environmental Failure Protection (EFP)	Use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions outside of the module's normal operating range.
EPROM	Erasable programmable read-only memory.
Error-detection Code (EDC)	Value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data
Error State	A state when the cryptographic module has encountered an error condition (e.g., failed a self-test). There may be one or more error conditions that result in a single module error state. Error states may include: "Hard" errors that indicate an equipment malfunction and 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 requiring maintenance, service, or repair of the cryptographic module.
Evaluation Laboratory	Independent entity that performs a security evaluation of the device 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 device that provides security protections needed to comply with these device security requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under these device security requirements.
Hardware (Host) Security Module (HSM)	See *Secure Cryptographic Device*.

Term	Definition
Hash	A (mathematical) function, which is a non-secret algorithm that takes any arbitrary-length message as input and produces a fixed-length hash result. Approved hash functions satisfy the following properties: ▪ One-Way. It is computationally infeasible to find any input that maps to any pre-specified output. ▪ 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.
HSM Processing Element	Physical system that performs operations using user cryptographic keys (working keys) of an HSM Solution Consumer.
HSM Solution	The sum of the HSM processing element and HSM virtualization system, which is exposed to the HSM Solution Consumer as the "Cloud HSM" to which they interface.
HSM Solution Consumer	Individual or system authorized to interface with and use an HSM Solution. An HSM Solution Consumer may perform multiple roles such as administration and operations but not those involving the set-up and maintenance of the underlying HSM Solution.
HSM Solution Provider	The entity that sets up and maintains an HSM Solution exposed to one or more HSM Solution Consumers.
HSM Virtualization System	System that authenticates the HSM Solution Consumer, provides virtualization of functions and HSM API commands, and assigns one or more HSM processing elements to perform tasks as required. An HSM processing element and HSM Virtualization System may be a single physical element or implemented in virtualized/cloud environment elements.
Initialization Vector (IV)	A binary vector used as the input to initialize the algorithm (a stream or block cipher) for the encryption of a clear-text block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
Initial Key Loading	Pertains to the loading of payment transaction keys used by the acquiring organization.
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.

Term	Definition
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.
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.

Term	Definition
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 Loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.
Key-Loading Device	An SCD that may be used for securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. Key-transfer and loading functions include the following: ▪ Export of a key from one secure cryptographic device (SCD) to another SCD in clear-text, component, or enciphered form; ▪ Export of a key component from an SCD into a tamper-evident package—e.g., blind mailer; ▪ Import of key components into an SCD from a tamper-evident package; ▪ Temporary storage of the key in clear-text, component, or enciphered form within an SCD during transfer.
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 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
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 clear-text 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.

Term	Definition
Least Privilege	In information security, computer science, and other fields, the principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.
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 clear-text 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).
Multi-tenant HSM	These are HSMs intended for multi-tenant usage—i.e., concurrent multi-organizational usage. These would be typically implemented in connection with an HSM as a service provider
Non-invasive Attack	Attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module.
Non-Reversible Transformation	See *Irreversible Transformation.*
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.

Term	Definition
Physical Execution Environment	The (sub)components and register transfer level (RTL) systems on which the software is executed. Two processing cores on a single die that share cache memory and other subsystems would be considered to be within the same physical execution environment. Separate silicon dies or physical processors would be an example of separate physical execution environments.
Physical Protection	The safeguarding of a secure cryptographic device or of cryptographic keys or other critical security parameters using physical means.
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.
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.
Pre-operational Self-test	Test performed by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and transitions to the operational state.
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.*
Public Security Parameters (PSPs)	Security-related public information whose modification can compromise the security of a cryptographic module. For example, public cryptographic keys, public key certificates, self-signed certificates, trust anchors, one-time passwords associated with a counter and internally held date and time. **Note:** A PSP is considered protected if it cannot be modified or if its modification can be determined by the module.
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.
Remote Administration Platform (RAP)	Platforms that are used for remote administration of HSMs. Such administration may include device configuration and cryptographic key-loading services.
Remote-managed HSM	These are HSMs that are designed to support remote management—e.g., non-console—for device configuration and cryptographic key loading. These HSMs differ from Multi-tenant HSMs in that they are designed for usage dedicated to a specific organization. They may exist as HSMs owned and operated by a specific organization or HSMs provided by a third party as part of an HSM as a service implementation.
Removable Cover	A part of a cryptographic module's enclosure that permits physical access to the contents of the module.
RNG	Random number generator.

Term	Definition
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.
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 clear-text 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 clear-text 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 Security Parameters (SSPs)	Critical security parameters (CSP) and public security parameters (PSP).
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.

Term	Definition
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.
Simple Power Analysis (SPA)	Direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions) in relation to the electrical power consumption of a cryptographic module for the purpose of extracting information correlated to a cryptographic operation.
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 information (e.g., key components) that individually convey no knowledge of the resultant combined information (e.g., a 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.
Strong	Not easily defeated; having strength or power greater than average or expected; able to withstand attack; solidly built.
Strong Cryptography	Cryptography using algorithms and key sizes as defined in Appendix D of the PCI HSM DTR document.
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.

Term	Definition
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.
Unique Accountability	Actions are attributable to a specific person or role.
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.
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