Payment Card Industry (PCI)

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

Modular Evaluation Vendor Questionnaire

Version 3.0

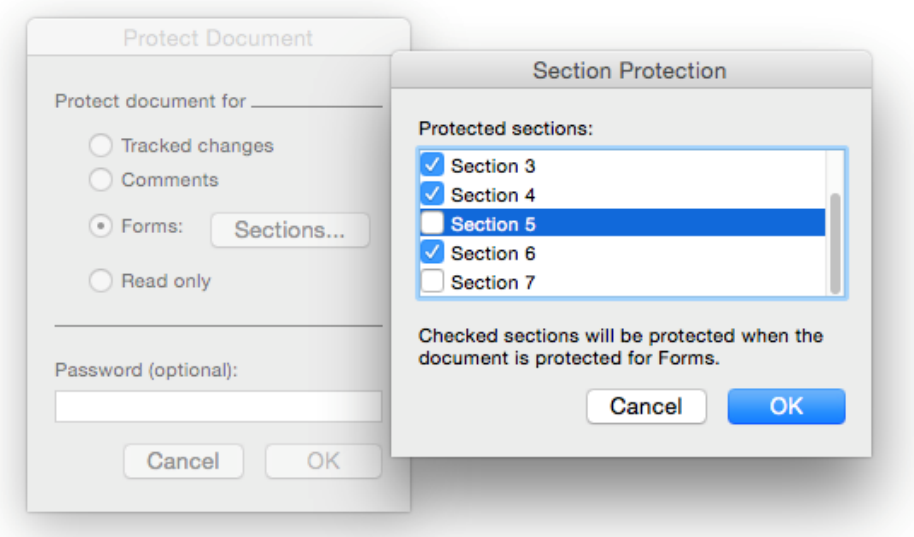
June 2016

Document Changes

Date	Version	Author	Description
April 2009	1.0	PCI	New Release
October 2011	1.1	PCI	Modifications for consistency with PCI POI requirements
February 2012	2.x	PCI	RFC version - Modifications for consistency with PCI POI requirements.
May 2012	2.0	PCI	Public release
February 2016	3.x	PCI	RFC version
June 2016	3.0	PCI	Addition of approval classes for key-loading devices and HSM remote administration platforms. Added device management. Additions to reflect major updates to DTRs. See *PCI PTS HSM - Summary of Requirements Changes from Version 2.0 to 3.0.*

Note to Assessors

When protecting this document for use as a form, leave Sections 5 and 7 (Annex B and "Device Diagrams") unprotected to allow for insertion of appropriate diagrams and reports. Under "Tools / Protect Document," select "Forms" then "Sections," and un-check Sections 5 and 7 as illustrated below.



Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Table of Contents

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Related Publications

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

Publication Title	Reference
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*
Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher	*ISO 9797-1*
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*
Financial services — Requirements for message authentication using symmetric techniques	*ISO 16609*
Information Technology – Security techniques – Encryption algorithms – Part 1: General	*ISO/IEC 18033-1*
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 TR19038*
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*

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Publication Title	Reference
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 1*
Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements	*PCI SSC*
Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements	*PCI SSC*
Payment Card Industry (PCI) PIN Security Requirements	*PCI SSC*

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

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Questionnaire Instructions

1. Complete the information below for the device being evaluated.
2. Identify all sections of the questionnaire corresponding to those questions in the form of the *PCI Hardware Security Module (HSM) Modular Security Requirements* ("HSM Modular Security Requirements") for which you answered "**YES**."
3. Complete each item in those identified sections.
4. Provide sufficient detail to thoroughly describe the device attribute or function.
5. Refer to and provide additional documentation as necessary.
6. Vendor must provide detail in the comments section for all "N/A" answers

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

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

Questionnaire completed by:

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

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Evaluation Module 1: Core Requirements

A – Physical Security Characteristics

Section A1

#	If the answer to A1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All mechanisms protecting against tampering.
2	The tamper action(s) that trigger(s) the mechanisms.
3	The response of the device to tamper detection. (This should include a written description of how the tamper mechanisms work and how erasure of secret information and/or inoperability is accomplished.)
4	The type of erasure (active or passive).
5	The details of what is erased upon tamper detection and the locations (e.g., RSA firmware authentication key is erased from the cryptographic processor flash) and the mechanisms used to erase the data.
6	Any reference documentation (e.g., security architecture, schematics, block diagrams) that describes the tamper-detection circuitry or erasure process.
7	The areas of the device that contain sensitive components and/or information.
8	In addition to tamper detection, other protection methods that exist to prevent access to sensitive information, or bug insertion.
9	The mechanisms protecting against physical penetration of the device.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to A1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
10	The secrets that are erased upon tampering and the mechanisms used to accomplish this.
11	How any secret information that is not erased is protected.
12	How the device is constructed, by attaching in Annex B at the end of the Questionnaire an exploded diagram of the device showing how all sub-components are assembled and connected internally.
13	Any volume-encapsulation methods used by the device that are designed to make penetration or reverse engineering difficult.
14	Any methods such as soldering, elastomeric strips or adhesives, plastic/metal walls, or others, that are used as part of the security features of the device.
15	How the security processor drives tamper-detection features.
16	Via attachment of a schematic diagram in Annex B at the end of the Questionnaire, the connections to all tamper-detection features, including switches and tamper grids of all device tamper circuits.
17	How passive components, connectors, or other items that carry tamper signals are protected against access.
18	How the device is protected from: ▪ Each side of the device ▪ The back of the device ▪ The front of the device
19	Why the device implementation is such it is not feasible to penetrate and alter the device to disclose sensitive information or to insert a sensitive-information-disclosing bug without requiring an attack potential of at least 26, with a minimum of 13 for exploitation.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to A1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
20	Whether sensitive information may exist when a human operator is present. Yes ☐ No ☐ In what area(s) may it exist? Provide the documentation that describes the inspection process that must be performed—for example, by including this information in Annex B at the end of the Questionnaire.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section A2

#	If the answer to A2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The operational and environmental conditions for which the device was designed.
2	Why the security of the device is not compromised by operational and environmental conditions.
3	The tests performed to ensure the security on the changing operational and environmental conditions. (Provide test reports.)
4	Why the measures are sufficient and effective.
5	The design of the environmental failure protection (EFP) response mechanisms.
6	The conditions that cause the EFP to trigger.
7	The response of these mechanisms when triggered.
8	Any glitch detection or prevention features used.
9	The tests performed to ensure the security on the changing of operational and environmental conditions. Provide test reports—for example, by including this information in Annex B at the end of the Questionnaire.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section A3

#	If the answer to A3 in the *PCI HSM Modular Security Requirements* was "YES," describe:	
1	All of the device's public keys.	
2	The sensitive information and functions that exist.	
3	Where sensitive functions are executed and where sensitive information is used. Include both long term and temporary storage locations, and any external memory used.	
4	How sensitive information and functions dealing with sensitive information are protected from unauthorized modification.	
5	Why the measures are sufficient and effective such that it is not feasible to modify sensitive information or functions dealing with sensitive information without requiring a per-device attack potential of at least 26 to defeat, with a minimum of 13 for exploitation.	
6	How public keys used for functions that impact security-related functions are protected from modification and substitution.	
7	The authorized methods for modifying and replacing public keys.	
8	How secret and private keys used for functions that impact security-related functions are protected from modification or substitution or disclosure.	
9	Whether signatures are used as a protection method. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ The algorithms and key lengths used for the signatures.	
	▪ Any padding schemes used for the signatures, and how this prevents padding oracle attacks.	
	▪ How modification of the sensitive information is prevented after signature validation.	

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to A3 in the *PCI HSM Modular Security Requirements* was "YES," describe:	
10	Whether physical protections are used as a protection method (for example, when plaintext information exists in external memory. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ Whether the physical protections cover all memory traces, vias, passive elements, or other areas of access.	
	▪ How the memory packages are protected, including access to BGA balls and traces on internal chip carriers of packages.	
11	Whether encryption is used as a protection method. Yes ☐ No ☐ If **"YES,"** describe:	
	▪ The algorithms and key lengths used.	
	▪ What modes of operation are used for the encryption.	
	▪ How encrypted values copied using physical access from one memory location to another are ensured to decrypt to values that do not reveal information about the original values and cannot be used to modify memory contents in a controlled manner.	
	▪ How the method of encryption prevents the exposure of sensitive information through building of a "dictionary" (i.e., look-up table) of possible encrypted values by writing know plaintext values via logical access and reading out ciphertext values via physical access.	
	▪ If a key stream mode of encryption is used (e.g., OFB), how the encryption of different data with the same key is prevented.	

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to A3 in the *PCI HSM Modular Security Requirements* was "YES," describe:	
12	For each integrated circuit element that may be programmed or configured in some way:	
	▪ The different ways in which the element may be programmed or configured.	
	▪ Any in-circuit testing or debugging features provided by these elements.	
	▪ The methods implemented to disable the programming/testing features.	
13	Whether applications and/or firmware are executed on the same processor that stores or operates on plaintext passwords, PINs, or public keys. Yes ☐ No ☐ If **"YES,"** describe:	
	What mechanisms are implemented to prevent these applications from modifying this information.	

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section A4

#	If the answer to A4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The design of all mechanisms intended to resist tamper.
2	The device's protection against monitoring electromagnetic emissions.
3	Any electro-magnetic emissions testing that has been performed. Provide data and results for the tests performed—for example, by placing this information in Annex B at the end of the Questionnaire.
4	The device protections against monitoring power consumption. Provide data and results for the tests performed—for example, by placing this information in Annex B at the end of the Questionnaire.
5	Any other internal or external characteristics considered. If applicable, provide data and results for the tests performed—for example, by placing this information in Annex B at the end of the Questionnaire.
6	The rationale for why the device implementation is such that the determination of sensitive information by monitoring sound, electro-magnetic emissions, or power consumption requires an attack potential of at least of at least 26, with a minimum of 13 for exploitation.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section A5

#	If the answer to A5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The device components that store or use cryptographic keys related to the operations under the scope of the device requirements.
2	The different cryptographic operations implemented with the device, whether they are implemented in software and/or hardware, and what side-channel analysis protections are implemented for each.
3	The protections the cryptographic processing elements implement to protect against attacks to force cryptographic errors, such as glitch attacks, and to protect against chip-level attacks to extract the cryptographic keys.
4	The tamper-evident characteristics—such as special coatings, seals, dye-releasing mechanisms, etc.—that are incorporated into the device components' design.
5	Whether the device includes any tamper-detection and response mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section A1.
6	Whether the device includes any tamper-resistance mechanisms in these components. Yes ☐ No ☐
	If so, provide responses to Section A1.
7	Why the device implementation is such that it is not feasible to determine any PCI device's security-related cryptographic key resident in the device—either by penetration of the device or by monitoring emanations from the device (including power fluctuations)—without requiring an attack cost potential of at least 35, with a minimum of 15 for exploitation.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to A5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
8	Why the programming or in-circuit testing features of the processing elements of the device cannot be re-enabled (either temporarily or permanently).
9	Any assistance and/or materials that will be provided to the evaluating test house to facilitate robust and efficient testing.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

B – Logical Security Characteristics

Section B1

#	If the answer to B1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The set of relevant device components undergoing self-tests.
2	All self-tests performed by the relevant device components, including validation of any register settings relied upon for the security of the device.
3	How initial machine code is loaded and executed by the processing elements, and how any subsequent firmware modules are loaded and executed, up to and including software modules used.
4	The algorithms and key sizes used to perform self-test functions.
5	The methods implemented to authenticate the cryptographic keys to ensure they have not been modified after loading.
6	Any self-test functions implemented by the built-in functions of the security processing elements and what sources of information and testing have been used to validate that these processes are in place.
7	The response of the device to a self-test failure for each type of component.
8	The types of events that initiate self-tests for each type of test.
9	The types of events that initiate a device reset, including elapsed time.
10	In detail, each self-test performed by the device on power-up and periodically during operation. Which of the techniques are consistent with FIPS PUB 140-2?

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
11	How the self tests are performed, either how periodic tests are induced or how continuous testing is implemented.
12	If applicable, how frequently the periodic self-tests are executed.
13	The conditional tests performed by the device. Which of the techniques is consistent with FIPS PUB 140-2?
14	How the conditional self-tests are induced.
15	The status provided by the device when power-up, periodic, and conditional self-tests execute successfully.
16	The actions of the device on a failure of each self-test
17	The algorithms used to perform the power-on firmware authenticity and integrity test. If the device supports firmware load, describe the firmware-load test, including the algorithms used.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B2

#	If the answer to B2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All logical and physical interfaces provided by the device and how each of those interfaces is configured to accept commands.
2	The testing The testing/fuzzing performed on each of the interfaces.
3	The languages in which the device's source code is written and the type and configuration of the operating system(s) used for each of the security processing elements.
4	All command interpreters within the HSM software that implement commands that can be invoked from the host system.
5	Which commands are accepted by the affected device components.
6	How the commands are segregated by the device modes.
7	The type of parameter and data checking performed to prevent the device from outputting sensitive data such as PINs due to the supplying of incorrect parameters or data..
8	Why the functionality is not influenced by logical anomalies.
9	Any tests that have been performed to ensure the functionality is not influenced by logical anomalies. Provide a rationale why the test coverage is sufficient**.**
10	How sensitive information is prevented from being outputted in clear text.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
11	Whether the device is designed to allow non-firmware applications to be executed If yes, can the non-firmware perform functions such as PIN processing, cryptographic key operations, prompt control, etc.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B3

#	If the answer to B3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The documented software-development process that details how firmware must be written, reviewed, and tested to ensure the software is free from security vulnerabilities.
2	The details of the audit trail that allows the certification of the firmware as being free from hidden and unauthorized or undocumented functions.
3	The compiler settings used in order to maximize the mitigation of known vulnerabilities.
4	The tools used for software/firmware source control.
5	The tools/methods used during source code reviews as part of the firmware-verification audit.
6	The sources of public vulnerabilities disclosure checked during the firmware-verification audit.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B4

#	If the answer to B4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Which components of the device allow updates of firmware and/or software.
2	Whether different parts of the firmware can be updated separately and how are the different firmware images/packages differentiated.
3	The methods used for initial firmware loading and, if different, the methods used for updates.
4	The mechanisms used and the device components affected by the firmware/software update.
5	The cryptographic algorithms and keys used for firmware authentication.
6	How any public or private secret keys are loaded into the device during manufacturing.
7	The device's response if firmware to be updated cannot be authenticated.
8	How the firmware/software is deleted if rejected.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B4.1

#	If the answer to B4.1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Which components of the device allow applications to be loaded.
2	How application updates are differentiated from firmware updates.
3	What cryptographic algorithms and key sizes are used for application authentication.
4	The device's response if the application cannot be authenticated.
5	How the application is deleted if rejected.
6	Which components of the device allow software application/configuration updates.
7	The mechanisms used and the device components affected by the updates.
8	The cryptographic algorithms and key sizes used for software application/configuration authentication.
9	The device's response if software application/configuration to be updated cannot be authenticated.
10	How the software application/configuration update is deleted if rejected.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B5

#	If the answer to B5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the device's data input, data output, control input, and status output interfaces are kept logically separate.
2	All data that is passed in and out of each logical interface.
3	The device's response to erroneous commands.
4	The device's response to erroneous data.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B6

#	If the answer to B6 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The data that is automatically cleared from the device's internal buffers when a transaction is completed.
2	The location of all buffers that are cleared.
3	The process used to clear the buffers.
4	What is the time-out period for the device.
5	The action taken by the device upon time-out.
6	The optimization options/flags included in the compiler options.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B7

#	If the answer to B7 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All of the administration services provided by the device (or make reference to a document that contains this information).
2	Which services require the assistance of two separately authenticated operators or a single authenticated operator.
3	The sensitive functions provided by the device. *Examples are key loading or the definition and maintenance of user roles.*
4	How the device controls the access and use of sensitive functions.
5	The authentication method used to access sensitive services.
6	Whether an external device is used to authenticate to the device to access sensitive services and its protections. Yes ☐ No ☐
7	How the authentication data used to access sensitive services in the device reader is protected, as it is input/output via the interface.
8	Which of the following is true for the data referred to in 7 above: ☐ Data inputs cannot be discerned from any displayed characters. ☐ Data inputs cannot be discerned by monitoring audible or electro-magnetic emissions. ☐ Sensitive data is cleared from internal buffers upon exiting a secure mode.
9	The interface used to authenticate to access sensitive services.
10	The rationale for the value chosen for the limit on the number of function calls (services). Also, describe how the limit minimizes the risks from unauthorized use of sensitive functions.
11	The rationale for the chosen time limit. Also, describe how the time limit minimizes the risks from unauthorized use of sensitive functions.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B7 in the *PCI HSM Modular Security Requirements* was "YES," describe:	
12	Whether, when the limits are exceeded, the device requires the operators to re-authenticate. Yes ☐ No ☐	
13	The measures that ensure that entering or existing sensitive services do not reveal or otherwise affect sensitive information**.**	
14	The management of any data used for authentication. *Examples of authentication data are passwords, cryptographic keys, and hardware tokens*. Include:	
	▪ The number of devices that share the same keys or passwords.	
	▪ Cryptographic algorithms used for authentication, if applicable.	
	▪ Data size (key or password length).	
	▪ How authentication data is distributed to legitimate users.	
	▪ How authentication data can be updated.	
15	For each of the implemented authentication techniques, provide a calculation for the associated probability that a random attempt will succeed.	
16	For each of the implemented authentication techniques, provide a calculation for the associated probability that for multiple attempts within a one-minute period, a random attempt will succeed.	
17	The device's response to false authentication data.	
18	All methods used to load cryptographic keys into device.	
19	The authorized methods for accessing and manipulating CSPs.	

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B8

#	If the answer to B8 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All CSP components that are entered or output using split-knowledge/dual-control procedures. Indicate how many components each CSP is split into and how many components are required to reconstruct the original CSP.
2	If knowledge of *n* components is required to reconstruct the CSP, the rationale stating how the knowledge of any *n*-1 components contains no other information about the original CSP other than the length.
3	The implemented CSP component-entry/output techniques (manual, direct, device).
4	How the CSP components are entered into the device without traveling through any enclosing or intervening systems.
5	Whether the device supports split knowledge/dual control CSP component-entry/output procedures via a network connection.
6	All keys that are entered or output in enciphered form and the algorithm used to encipher each key.
7	All keys that are entered or output in plaintext form.
8	The implemented plaintext key-entry/output techniques and how the keys are directly entered into the device without traveling through any intervening systems.
9	Whether the device supports the manual or network techniques for plaintext key entry/output procedures.
10	What mechanisms are in place to record audit information.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B8 in the *PCI HSM Modular Security Requirements* was "YES," describe:
11	Each combination of key-exchange technique and key-storage mechanism supported by the device (e.g., ANSI TR-31).
12	If applicable, the secure device or interface used for the loading of clear-text cryptographic data.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B9

#	If the answer to B9 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The implementation of the random number generator, including any seed values used, hardware systems, and software-based, deterministic pseudo random number generators (DPRNG).
2	Any standards the RNG(s) and/or PRNG(s) have been designed to comply with.
3	For each type of CSP generated by the device, indicate the RNG and/or PRNG used.
4	How cryptographic key components and other CSPs are generated using a random or pseudo-random process, such that it is not possible to predict any secret value or determine that certain values are more probable than others from the total set of all the possible values.
5	The tests performed by the TOE itself to check that the RNG works properly.
6	The tests performed by the vendor to check that the RNG works properly.
7	How the random number generator is used to protect or produce sensitive data i.e., list all functionality that make use of the RNG to protect/generate sensitive data.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B10

#	If the answer to B10 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All algorithms implemented within the device, their associated key sizes, and the modes used (e.g., TDES CBC, RSA PKCS #1 v2.1).
2	How each algorithm is used**.**
3	All security protocols (e.g., SSL, TLS, IPsec, etc.) supported by the device.
4	The combination of algorithms (e.g., cipher suites) supported for each protocol.
5	All prior algorithm certifications and/or test results. (Please provide certificates, letters of approval, or test reports.)
6	Any relevant documentation, such as security-evaluation reports, schematics, data sheets, vendor test procedures and test reports about the encryption algorithm, padding mechanism, and mode of operation being used.
7a	The credentials of the expert reviewer that assessed the security of the mode of operation used by the encryption algorithm (if a non-standardized mode of operation is in use).
7b	How the expert reviewer is independent to the vendor**.**

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B11

#	If the answer to B11 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The key management techniques i.e., fixed key, master key/session key, or unique key per transaction (UKPT) used for PIN-protection.
2	Whether each key is used for only one cryptographic purpose. Yes ☐ No ☐ How is this enforced?
3	How keys are protected during key storage against unauthorized disclosure and substitution.
4	How key separation is ensured during key storage.
5	All cryptographic algorithms implemented by the device.
6	Whether the device has the ability to erase cryptographic keys. Yes ☐ No ☐
7	What keys may be erased.
8	The process used for erasure.
9	The circumstances under which keys are erased. Describe for all device states (power-on, power-off, sleep mode).
10	Any other data that may be erased along with the cryptographic keys. The circumstances under which such data may be erased.
11	The keys that are not erased.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B11 in the *PCI HSM Modular Security Requirements* was "YES," describe:	
12	How all keys present or otherwise used in the device are loaded, including who the key is generated by (e.g., acquirer or manufacturer) generates and whether the keys are loaded encrypted or as plaintext or as encrypted or plaintext components/secret shares.	
13	Whether there is a key-distribution technique present that uses an asymmetric algorithm with a public key for the exchange of symmetric secret keys, and address each of the following regarding this key-distribution technique:	
	▪ The technique utilizes a random/pseudo-random key-generation process such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others.	Yes ☐ No ☐ N/A ☐
	▪ Is the random source tested in a suitable manner before key generation?	Yes ☐ No ☐
	▪ How the authenticity of public keys is ensured.	
	▪ Whether there is a certificate hierarchy.	Yes ☐ No ☐
	▪ How certificates (signed public keys of the key-exchange partners) are generated—i.e., who signs?	
	▪ Whether there is mutual device authentication.	Yes ☐ No ☐
	▪ If certificates are used, how they are tested and accepted or rejected.	
	▪ Whether there is a secure formatting and padding of the message used containing the symmetric secret key.	Yes ☐ No ☐
	▪ Whether the correctness of the message structure is tested by the receiver.	Yes ☐ No ☐
14	How the authenticity of origin is ensured—e.g., is the signature of the exchange message tested?	
	▪ The reaction of the device if an authenticity test fails.	
	▪ The effective key length(s) that is/are utilized for all the cryptographic algorithm(s) in question.	
	▪ Whether the chosen key length is appropriate for the algorithm and its protection purpose.	Yes ☐ No ☐
	▪ For the algorithm(s) used, the key size(s) used as denoted in Appendix D of the DTRs.	
15	The hashing algorithm(s) that are used.	
16	The purpose of their usage(s).	

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B11 in the *PCI HSM Modular Security Requirements* was "YES," describe:
17	Whether single component keys can be loaded and the algorithm used to encrypt them during key entry.
18	All storage and usage locations for each key ever present in or used by the device.
19	Each combination of key-exchange technique and key-storage mechanism supported by the device (e.g., ANSI TR-31).
20	How keys stored or used by the device are generated.
21	Whether the device uses any key-derivation method. Yes ☐ No ☐
	If **"YES,"** describe the method.
22	Whether any key is calculated as a variant of another key. Yes ☐ No ☐
	If **"YES,"** describe how the variant(s) are protected at an equivalent or greater level of security as the original key(s).

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B12

#	If the answer to B12 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The device's behavior when cryptographic keys are lost.
2	How the device fails in a secure manner when the cryptographic keys are rendered invalid.
3	Any status provided by the device when cryptographic keys rendered invalid.
4	How the device determines that a key has been rendered invalid.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B13

#	If the answer to B13 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the device ensures that cryptographic keys are only used for a single cryptographic function.
2	How the device ensures that cryptographic keys are only used for an intended purpose, and indicate which of the following methods are supported: ☐ Physical segregation ☐ Storing keys enciphered under a KEK dedicated to encipherment of a specific type of key ☐ Modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage, e.g., key tags.
3	For every key used for PIN encryption, indicate what type of data can be encrypted or decrypted.
4	How encrypted PIN data is distinguished from all other data encrypted or plaintext.
5	All key-encrypting keys.
6	What data can be encrypted using key-encrypting keys.
7	How this data is distinguished from all other data.
8	How encrypted keys are distinguished from all other data.
9	How does the device enforce that a key is only used for one purpose.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B14

#	If the answer to B14 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Whether there is a mechanism that will allow the output of plaintext secret or private cryptographic keys or plaintext PIN. Yes ☐ No ☐ If yes, describe the mechanism.
2	How the outputting of plaintext keys and plaintext PINs is prevented.
3	The locations within the device wherein cryptographic keys may exist in plaintext.
4	Under what circumstances a plaintext key may be transferred from each of the above locations to another location within the device.
5	How the encryption of a key or PIN under a key that might itself be disclosed is prevented.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B15

#	If the answer to B15 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The PIN-block formats supported by the device.
2	The PIN block translations that are supported by the device
3	Whether PIN block translations between PIN blocks that contain the real PAN and PIN blocks that contain tokens are supported, and if so, what translations are supported and which prevented
4	The method used by the device to ensure that journaled transaction messages do not contain a plaintext PIN.
5	All key-encryption keys and associated algorithms.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B16

#	If the answer to B16 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The device's logging mechanism, and list the data and events logged.
2	How the log data is protected from unauthorized modification, substitution, and deletion.
3	The method used to provide a time stamp for audit events.
4	The dual-control mechanism for deletion if logs are stored internally.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B17

#	If the answer to B17 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Whether the device support multiple applications. Yes ☐ No ☐
	If yes, provide a list of these applications, and identify those with security impact.
	If yes, describe how the separation between applications with security impact and those without security impact is enforced.
2	For each security-relevant application, list by groups, the data objects and their location.
3	Which mechanism(s) ensure that code and data objects of different applications/firmware are kept separate.
4	What mechanisms exist within the device that allow for the execution of non-ROM based configuration or program data (e.g., processors, micro-controllers, FPGAs, etc.).
5	Whether the device relies upon the use of different processors to provide for the separation between the firmware and any applications and, if so, the method of communications provided between these processors, including any physical interface and API(s).
6	The mechanisms provided to prevent the execution of memory used to hold data objects.

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

#	If the answer to B17 in the *PCI HSM Modular Security Requirements* was "YES," describe:
7	If the device allows customers or integrators to install additional applications, how the device's design prevents the embedded application from:
	▪ Having access to the top-level master keys that protect the working keys—i.e., it cannot extract or modify the top-level master key.
	▪ Having access to operator or security officer functions, and so cannot change security configurations or change privileges.
	▪ Introducing new primitive cryptographic functions (although it can use these to implement new composite functionality).
8	How the embedded application is separated from the approved device functionality by an internal security boundary that prevents embedded applications from obtained any elevated privilege or access to any data belonging to other embedded or host side applications.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B18

#	If the answer to B18 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Whether the device implements a commercial operating system, custom operating system, function executive, or other mechanism. If the device uses a commercial operating system, note the name and version of this system.
2	The method of ensuring that the operating system contains only the components and the services necessary for the intended operation.
3	The procedures used for maintenance and updates of the operating system.
4	The rationale for why the method used to enforce least privilege is effective.
5	The rationale for why all the components and services in the configuration list are necessary.
6	The security policy enforced by the device to not allow unauthorized or unnecessary functions.
7	The API functionality and commands that exist and are either (i) identified as required to support specific functionality, or (ii) disabled/removed.
8	The rationale for why it is infeasible to remove API functionality and commands that are not necessary to support specific functionality.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B19

#	If the answer to B19 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The format of the device's unique device ID.
2	How the unique device ID can be obtained from the device.
3	How the unique device ID is assigned.
4	Whether it is possible to change the device's unique device ID. Yes ☐ No ☐ If yes, provide a description.
5	How exactly the device is uniquely identified using cryptographic methods.
6	What acceptable algorithms are used for uniquely identifying the device through cryptographic means.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section B20

#	If the answer to B20 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Describe the differences between PCI and non-PCI mode, including (but not limited to) services/functions available, algorithms, PIN translations, and key input or output:
2	Describe the process/commands for switching between PCI and non-PCI mode.
	▪ If remote (over a network such as Ethernet or WiFi), what authentication and replay prevention mechanisms are used?
	▪ If direct (e.g., through serial or keypad on the device), what authentication mechanism is used?
3	How the device prevents keys from being shared between PCI and non-PCI mode (zeroization or isolation).
4	How the device indicates that it is in PCI or non-PCI mode.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

C – Policy and Procedures

Section C1

#	If the answer to C1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Whether the security policy is available to potential customers. Yes ☐ No ☐
2	How changes to the security policy document are controlled.
3	The roles supported by the device.
	The services available for each role.
4	How the device is configured to comply with the security policy.
5	Whether the device supports PIN translation. Yes ☐ No ☐
	If so, what formats does it support and what translations to/from does it support?

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Evaluation Module 2: Key-Loading Devices

D – Key-Loading Devices

Section D1

#	If the answer to D1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The generation of asymmetric key pairs by the device.
2	The generation of secret keys by the device.
3	The protection of private or secret key or its precursors from being observed in clear text during the generation process.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section D2

#	If the answer to D2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The generation of asymmetric keys pairs not used by the device
2	The generation of symmetric keys not used by the device.
3	The transfer of symmetric keys or asymmetric key pairs, including the deletion of all related secret or private seed elements.
4	The device's process of deleting all related secret and private seed elements.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section D3

#	If the answer to D3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The key-transfer process used by the device
2	The information present in the device after the key transfer.

Comments:

Section D4

#	If the answer to D4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Each of the components of the device, including the transfer process between the components that define the device.
2	The characteristics that prevent a cryptographic key in a device component to be loaded into a component providing lower security.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section D5

#	If the answer to D5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the device responds to attempts to modify the device's functional capbilities once cryptographic keys are loaded to it.
2	Why the response cannot be circumvented.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Evaluation Module 3: Remote Administration

E – Logical Security

Section E1

#	If the answer to E1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The device initialization process.
2	The process for loading keys and other relevant material into the device during initialization.
3	The process for putting the device into operational service after initialization.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section E2

#	If the answer to E2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	All operator functions of the device.
2	All operator functions that are permitted when the device is in a sensitive state.
3	The process of disabling or enabling device functions.
4	The process of changing passwords or other authentication data in the device.
5	Authentication data that enables the device to enter sensitive service.
6	The secure operator interface and mechanism used to enter the sensitive state.
7	How the secure operator interface ensures that it cannot be inadvertently left in a sensitive state.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

F – Devices with Message Authentication Functionality

Section F1

#	If the answer to F1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the message authentication device is manually activated.
2	How the identity of the key used is displayed on the device.
3	How the device only outputs a confirmation or denial of a MAC provided for verification, and never the plaintext-computed MAC.

Comments:

Section F2

#	If the answer to F2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The length of the MAC being generated or verified.
2	How the MAC being generated or verified is in accordance with ISO 16609.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section F3

#	If the answer to F3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The MAC generation and verification techniques.
2	How the techniques are in accordance with ISO 16609.

Comments:

Section F4

#	If the answer to F4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The message authentication device use of unidirectional MAC keys.
2	Each MAC function for each MAC key

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

G – Devices with Key-Generation Functionality

Section G1

#	If the answer to G1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the device is protected from unauthorized removal from its operational location. List all deterrents available to the device.

Comments:

Section G2

#	If the answer to G2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The means provided by the device to output any plaintext key.
2	How the device enforces the use of dual control for plaintext key outputting.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section G3

#	If the answer to G3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The functions that require the use of "special sensitive states."
2	How the special "sensitive" state is entered.

Comments:

Section G4

#	If the answer to G4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Any proprietary functions and how they are totally equivalent to a series of standard and approved functions.
2	How the proprietary functions are limited to use of specific keys.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

H – Devices with Digital Signature Functionality

Section H1

#	If the answer to H1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the asymmetric private and public key pair is generated within the digital signature device.
2	How the asymmetric private key can be exported (if applicable) outside the original digital signature device under control for backup and archival purposes.
3	The mechanisms for the control of the use of the private key.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section H2

#	If the answer to H2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The binding between the public key and the identity of the owner of the private key.
2	The use of public key certificates, and where the public key certificate was obtained from an authorized certificate authority.
3	Other equivalent mechanisms to irrefutably determine the identity of the owner of the corresponding private key.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Evaluation Module 4: Device Management Security Requirements

I – Device Management Security Requirements during Manufacturing

Section I1

#	If the answer to I1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How change control procedures ensure that any intended change to the physical or functional capabilities of the device causes a re-certification of the device under these requirements.
2	If and how the change control process differs for changes that purely rectify errors or faults in software that do not remove, modify, or add functionality.

Comments:

Section I2

#	If the answer to I2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life cycle. Include all dual control or standardized cryptographic authentication procedures.
2	How the protected firmware is validated before use.
3	The change management process for updating validated firmware.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section I3

#	If the answer to I3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How the device is assembled in a manner that the components used in the manufacturing process are those components that were certified.
2	The process used to ensure that approved components are not swapped out during the manufacturing.

Comments:

Section I4

#	If the answer to I4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	How production software (e.g., firmware) is loaded to devices at the time of manufacture and how the principle of dual control is followed.
2	The process used to prevent unauthorized modifications and/or substitutions of software (e.g., firmware) during the manufacturing process.
3	How production software (e.g., firmware) is stored during manufacturing.
4	How production software (e.g., firmware) is transported to the manufacturing facility.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section I5

#	If the answer to I5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	Subsequent to production but prior to shipment from the manufacturer's or reseller's facility, how the device and any of its components are protected during storage.
2	The access controlled area or sealed tamper-evident packaging used to prevent unauthorized access to the device or its components.
3	The process for validating devices or their components prior to shipment to ensure they have not been tampered with.

Comments:

Section I6

#	If the answer to I6 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The process by which the device is authenticated at the facility of initial deployment if authentication is by means of secret information placed in the device during manufacturing.
2	How the secret information in each device is unique to the device and is unknown and unpredictable to any person.
3	How secret information is installed in each device to ensure that it is not disclosed during installation.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section I7

#	If the answer to I7 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The security measures taken during the development and maintenance of device's security-related components.
2	The process used to maintain and develop 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.
3	The documented and approved processes that provide evidence that security measures are followed during the development and maintenance of the device's security-related components.
4	What evidence validates that the security measures provide the necessary level of protection to maintain the integrity of the device's security-related components.

Comments:

Section I8

#	If the answer to I8 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The specific controls over the repair process.
2.	The process used for inspection and testing subsequent to repair to ensure that the device has not been subject to unauthorized modification.
3	The process for resetting the tamper mechanisms.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

J – Device Management Security Requirements between Manufacturer and Facility of Initial Deployment

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

Section J1

#	If the answer to J1 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The process and tamper-detection security features that protect the device from unauthorized modification.
2	The customer documentation that provides instruction on validating the authenticity and integrity of the device.
3	The controls for shipping devices from manufacturer's facility to the facility of initial deployment.
4	The auditable controls that account for the location of every device at every point in time.
5	Where multiple parties are involved in organizing the shipping, the responsibility of each party to ensure that the shipping and storage they are managing are compliant with this requirement.
6	How the device is shipped from the manufacturer's facility to the facility of initial deployment and stored en route under auditable controls.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section J2

#	If the answer to J2 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The procedures for the transfer of accountability for the device directly from the manufacturer to the facility of initial deployment.
2	Where the device is shipped via intermediaries such as resellers; and the process for accountability with the intermediary from the time at which they received the device until the time it is received by the next intermediary or the point of initial deployment.

Comments:

Section J3

#	If the answer to J3 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The end-to-end transit procedures for shipping devices from the manufacturer's facility to the initial key-loading facility.
2	The procedures for detecting physical or functional alteration attempts to the device that may have occurred while the device was in transit from the manufacturer's facility to the initial key-loading facility.
3	The controls used to ensure the device is shipped and stored containing a secret that (i) is immediately and automatically erased if any physical or functional alteration to the device is attempted, (ii) can be verified by the initial key-loading facility, but (iii) cannot feasibly be determined by unauthorized personnel.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section J4

#	If the answer to J4 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The device's development security documentation that provides information to the initial key-loading facility to assure the authenticity of the TOE's security-relevant components.

Comments:

Section J5

#	If the answer to J5 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The process for validating the authenticity of the device's security-related components if the manufacturer is in charge of initial key loading.

Comments:

Section J6

#	If the answer to J6 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The procedures provided to the initial key-loading facility to verify the authenticity of the device's security-related components if the manufacturer is not in charge of initial key loading.

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Section J7

#	If the answer to J7 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The affixed visible identifier unique to each device.

Comments:

Section J8

#	If the answer to J8 in the *PCI HSM Modular Security Requirements* was "YES," describe:
1	The manual that provides instructions for the operational management of the device.
2	The instructions for recording the entire life cycle of the device's security-related components and of 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

Comments:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Annex A: DTR Templates

DTR TA1.11

Enumerate each of the circuit boards indicated in the device in the table below, providing, at a minimum:

PCB Designator	PCB Version	PCB purpose	Picture reference	Sensitive signals	Tamper-Detection Mechanisms

DTR TA1.14

Using vendor documentation for each tamper grid that is implemented, complete the details indicated in the table below, describing, at a minimum:

Tamper Grid Location	Physical Implementation	Size of Traces and Distance between Traces, Signals, or Layers	Number of Tamper-Detecting Signals	Method of Connection	Adjacent Signals?

DTR TA1.16

For each tamper switch used in the device, complete the details indicated in the table below, at a minimum.

Switch Location	Number Used in that Location	Physical Implementation	Size of Switch Contacts	Conductive Ink Protections	Additional Comments

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

DTR A2.5

Use the table below to detail the environmental protection features implemented by the device.

	Maximum Value	Minimum Value	Detecting Circuitry	Response
Voltage (Specify type)	Configured Value	Configured Value		
	Tested Value	Tested Value		
Temperature	Configured Value	Configured Value		
	Tested Value	Tested Value		

DTR TA3.4

In the following table, outline the locations of all types of sensitive information and functions, adding to those provided where other types of sensitive information exist within the device.

Sensitive Information	Storage area	Method of protection
Plaintext PINs		
Passwords		
Device Firmware		
Public keys		

DTR TB1.11

Complete the following table indicating the process used to authenticate the firmware images during each stage of the booting process.

Boot stage	Algorithms and Key Sizes Used for Authentication	Area/Code/Registers Authenticated	Method and Frequency of Re-authentication	Action Performed if Failed

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

DTRs TB4.6 and TB4.1.6

Complete the following table for each of the processing elements listed in DTR A3.

Processing/ Application or Firmware Element	Elements Used to Perform Authentication	Algorithms and Key Sizes Used for Firmware Authentication	Format of Authentication Block	Process Performed if Authentication Failed

DTR TB11.13

Complete the following table for all keys and key-management methods outlined in DTR B11.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Generated by:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)	How the key is identified by the device so that it is used only as intended

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Generated by:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)	How the key is identified by the device so that it is used only as intended

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Generated by:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)	How the key is identified by the device so that it is used only as intended

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Generated by:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)	How the key is identified by the device so that it is used only as intended

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Generated by:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/ acquirer/ vendor-specific/ other (describe)	How the key is identified by the device so that it is used only as intended

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Annex B: Device Diagrams and Test Reports

(Mandatory where specified in the preceding questions; optional for additional information)

Required Diagrams and Reports

If any of the Sections noted below were completed within the Questionnaire, attach requested diagrams or reports, as appropriate, in the areas designated below.

Section A1, Question 12:

Section A1, Question 16:

Section A1, Question 20:

Section A2, Question 9:

Section A4, Question 3:

Section A4, Question 4:

Section A4, Question 5:

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Device Diagrams (Optional)

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

Copyright 2012-2016 PCI Security Standards Council, LLC. All Rights Reserved.