Анализ
Требований к Модулям HSM

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Security Requirements Version 3.0 June 2016

Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Derived Test Requirements Version 3.0 June 2016

Evaluation Modules

- **Evaluation Module 1: Core Requirements**
- **A – Physical Security Requirements**
- **B – Logical Security Requirements**
- **C– Policy and Procedures**
- **Evaluation Module 2: Key-Loading Devices**
- **D – Key-Loading Devices**
- **Evaluation Module 3: Remote Administration**
- **E – Logical Security**
- **F– Devices with Message Authentication Functionality**
- **G – Devices with Key-Generation Functionality**
- **H – Devices with Digital Signature Functionality**
- **Evaluation Module 4: Device Management Security Requirements**
- **I – Device Security Requirements During Manufacturing**
- **J – Device Security Requirements Between Manufacturer and Point of Initial Deployment**

A – Physical Security Requirements

A1

- T**he 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.

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

:

A – Physical Security Requirements

A4

- There is no feasible way to determine any sensitive information by monitoring electro-magnetic emissions, power consumption, or any other internal or external characteristic without an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation.

A5

- Determination of any PCI-related cryptographic key resident in the device or used by the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation

Возможности нарушителя

- По разному определены возможности нарушителя в пределах контролируемой зоны (КЗ).
- В соответствии ТА4.5:
- The tester shall develop attack scenarios to defeat or circumvent the protection mechanisms against the monitoring of electro-magnetic emissions, power consumption, or any other internal or external characteristic available for monitoring, using attack scenarios
- Monitoring must be done **outside the protected areas of the device components (such as the device's tamper-protected casing)** and must investigate any data emanating from inside these device components
- *If the device is restricted to deployment in controlled environments, the following applies: The tester may drill out visible fasteners (e.g., screws, rivets, or press-fittings) to remove the cover or to create a gap between the covers or cover and housing* ***to insert probes.***
- .

Возможности нарушителя

Нарушитель может устанавливать зонды во все незащищенные от проникновения точки устройства. В том числе в физические интерфейсы считывателя ключей

Используемое оборудование

- **Специализированное оборудование стоимостью от 1 000 до 50 000 долларов США.**
  - Дорогие осциллографы с высоким разрешением, высокой частотой и глубокой буферизацией (> 1 ГГц, 1 ГГц, 16 бит и т. д.)
  - 3D-принтеры высокого разрешения
  - Фрезерные станки с высоким разрешением (например, для строгания)
  - Сложное программное обеспечение побочного канала, способное выполнять удаление шума и т.д
  - **Микрозонды для подключения к функциям на уровне кристалла, таким как линии шины на микросхемах**
  - Система сбоев EMFI
  - Высокочастотные / широкополосные электромагнитные пробники
  - Высокоскоростной логический анализатор 16/32 бит для захвата и анализа трафика
  - Выделенные электронные карты
  - Специализированные испытательные стенды
  - Анализаторы протокола
  - **Рабочая станция микрозонда**
  - Химический верстак
  - Лазерная шлифовка / резка

Attack Potential Factors

Factor	Range	Identification Phase	Exploitation Phase
Attack time	≤ 1 hour	0	0
	≤ 2 hours	1	1
	≤ 4 hours	1.5	1.5
	≤ 6 hours	2	2
	≤ 8 hours	3	3
	≤ 12 hours	4	4
	≤ 16 hours	4.5	4.5
	≤ 24 hours	5	5
	≤ 40 hours	5.5	5.5
	≤ 60 hours	6	6
	≤ 100 hours	6.5	6.5
	≤ 160 hours	7	7
	Beyond 160 hours	7.5	7.5

Attack Potential Factors

Factor	Range	Identification Phase	Exploitation Phase
Expertise	Layman	0	0
	Skilled	1	1
	Proficient	3	3
	Expert	4	4
Knowledge of the HSM	Public	0	0
	Restricted	2	2
	Sensitive	3	3
Access to the HSM per device required for the attack.	Mechanical sample	1	1
	Functional samples without working keys	2	2
	Functional sample with working keys and software	4	4
Equipment required for the attack	None	0	0
	Standard	1	1
	Specialized	3	3
	Bespoke	5	5
	Chip-level attacks	7	7

Attack Potential Factors

Factor	Range	Identification Phase	Exploitation Phase
Specific parts required	None	0	0
	Standard	1	1
	Specialized	3	3
	Bespoke	5	5

B – Logical Security Requirements

B1

- To ensure that the device is operating as designed**, the device runs self-tests when powered up and at least once per day** or 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.

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 firmware, and any changes thereafter, has been inspected and reviewed using a documented process that can be audited and is certified as being free from hidden and unauthorized or undocumented functions.

B4

- 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.

B – Logical Security Requirements

B4.1

- The firmware must support the authentication of applications loaded into the device consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.

B5

- The device provides secure interfaces that are kept logically separate by distinguishing between data and control for inputs and also between data and status for outputs.

B6

- The device must automatically clear or reinitialize its internal buffers that hold sensitive information prior to reuse of the buffer, including when:
- The transaction is completed,
- The device has timed out, or
- The device recovers from an error state.

B7

- Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.

B – Logical Security Requirements

B8

Key Form	Technique		
	Manual	Direct	Network
Plaintext keys	No	Yes	No
Plaintext key components	Yes	Yes	No
Enciphered keys/components	Yes	Yes	Yes

B9

- 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.

B10

- The device uses accepted cryptographic algorithms, modes, and key sizes.

B – Logical Security Requirements

B11

- The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support ANSI TR-31 key-derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.

B12

- 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.

B13

- 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 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.

B – Logical Security Requirements

B14

- 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 CSPs to components that could negatively impact security**.

B15

- 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.

B16

- The device includes cryptographic mechanisms to support secure logging of transactions, data, and events to enable auditing.

B – Logical Security Requirements

B17

- 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.

B18

- The operating system/firmware of the device must contain only the software (components and services) necessary for the intended operation. The operating system/firmware must be configured securely and run with least privilege.

B19

- The device has the ability to return its unique device ID.

B – Logical Security Requirements

B20

- **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

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.

G – Devices with Key-Generation Functionality

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 plaintext key except under dual control. Such dual control is enforced by means such as the following:
- The device requires that at least two passwords 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.

G – Devices with Key-Generation Functionality

G3

- The following operator functions (if available) require the use of special "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.**

I – Device Security Requirements During Manufacturing

The device manufacturer, subject to PCI payment brand site inspections, confirms the following. The PCI test laboratories will validate this information via documentation reviews. Any variances to these requirements will be reported to PCI for review. **However, this information will only be used for analysis at this time and will not impact whether a device receives an approval.**

I1

- 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.

I2

- 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.

I – Device Security Requirements During Manufacturing

I3

- The device is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Physical Security Requirements evaluation, and that unauthorized substitutions have not been made.

I4

- 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.

I5

- 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.

I – Device Security Requirements During Manufacturing

I6

- If 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.

I7

- 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.

I – Device Security Requirements During Manufacturing

I8

- **Controls exist over the repair process and the inspection/testing** process subsequent to repair to ensure that the device has not been subject to unauthorized modification.

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

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

  J1

- 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.

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

J2

- 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.

J3

- While in transit from the manufacturer's facility to the facility of initial deployment, the device is:
- **Shipped and stored in tamper-evident packaging; and/or**
- **Shipped and stored containing a secret that:**
  - Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and
  - Can be verified by the initial-key-loading facility, but that cannot feasibly be determined by unauthorized personnel.

J4

- 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.

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

J5

- If the manufacturer is in charge of initial key loading, the manufacturer must verify the authenticity of the device's security-related components.

J6

- 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.

J7

- Each device shall have a unique visible identifier affixed to it or should be identifiable using secure, cryptographically protected methods.

J8

- 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 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

Спасибо за внимание