
## Payment Card Industry (PCI)

# PIN Transaction Security (PTS) Point of Interaction (POI)

## Modular Security Requirements

Version 4.0

June 2013

# Document Changes

| Date | Version | Description |
|---|---|---|
| February 2010 | 3.x | RFC version |
| April 2010 | 3.0 | Public release |
| October 2011 | 3.1 | Clarifications and errata, updates for non-PIN POIs, encrypting card readers |
| February 2013 | 4.x | RFC version |
| June 2013 | 4.0 | Public release |

# Table of Contents

# About This Document

## Purpose

The purpose of this document is to provide vendors with a list of all the security requirements against which their product will be evaluated in order to obtain Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) device approval.

Version 3 introduced significant changes in how PCI will be evaluating PIN and non-PIN acceptance POI terminals. PCI no longer maintains three separate security evaluation programs (point-of-sale PIN entry device (PED), encrypting PIN pad (EPP), and unattended payment terminal (UPT)). Instead PCI provides and supports one set of modular requirements, which covers all product options.

This change was reflected in our renaming of this document to be the Modular Security Requirements.

The layout of the document was also changed to enable vendors to select the appropriate requirements that match the product they are submitting for evaluation.

This document supports the submission of products under the following categories:

- PED or UPT POI devices: Complete terminals that can be provided to a merchant “as-is” to undertake PIN-related transactions. This includes attended and unattended POS PIN-acceptance devices.
- Non-PIN acceptance POI devices evaluated for account data protection
- Encrypting PIN pads that require integration into POS terminals or ATMs. Overall requirements for unattended PIN-acceptance devices currently apply only to POS devices and **not** to ATMs.
- Secure components for POS terminals: These products also require integration into a final solution to provide PIN transactions. Examples are OEM PIN entry devices and secure (encrypting) card readers.

This version 4 additionally provides for:

- Submission by the vendor for assessment and publication on the PCI website of a user-available security policy addressing the proper use of the POI in a secure fashion, as further delineated in requirement B20.
- Greater granularity and robustness of the underlying PCI-recognized laboratory test procedures for compliance validation of a device to these requirements as detailed in the Derived Test Requirements.

## 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 Program Manual*) and the set may include:

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

Upon successful compliance testing by the laboratory and approval by the PCI SSC, the PCI PTS POI device (or a secure component) 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 "Evaluation Module Information" section of this document.

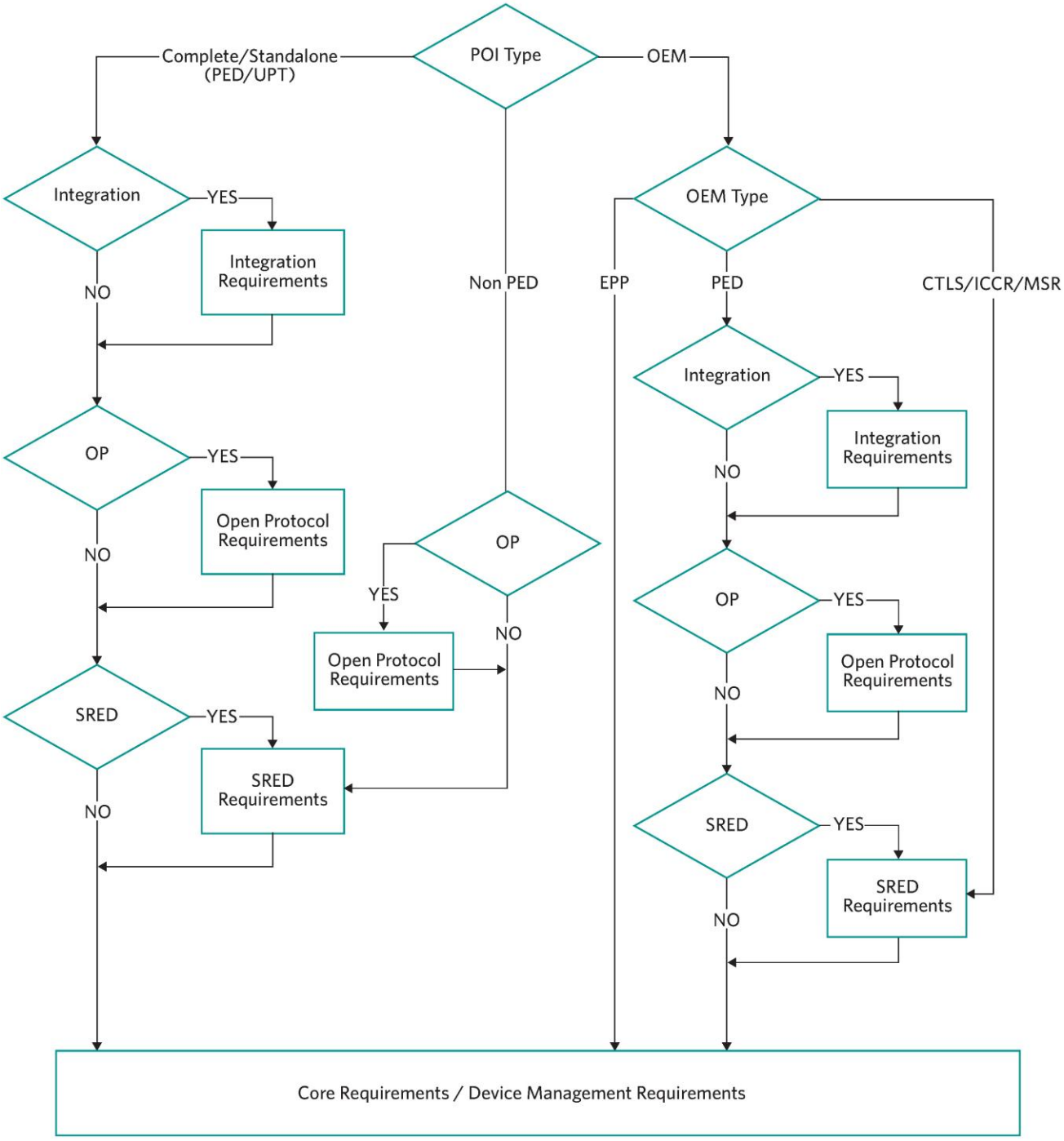
## Main Differences from Previous Version

This document is an evolution of the previous versions and supports a number of new features in the evaluation of POI devices:

- The reordering of the Core Physical Security Requirements
- The restructuring of the Open Protocols module
- The addition of a requirement for the vendor to provide a user-available security policy that will facilitate implementation of an approved POI device in a manner consistent with these requirements, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements

## PTS Approval Modules Selection

The graph below gives a preliminary view of which evaluation modules should apply, based on the product undergoing an evaluation. This only reflects applicability of modules. *Appendix B: Applicability of Requirements* makes further refinement at the requirement level.



# 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 POI devices. Thus, the requirements are not intended to eliminate the possibility of fraud, but to reduce its likelihood and limit its consequences.

## 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, and expertise and equipment required. Given the evolution of attack techniques and technology, the Associations will periodically review these amounts for appropriateness.

## Device Management

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

This document is only concerned with the device management for POI devices up to the point of initial key loading. Subsequent to receipt of the device at the initial key-loading facility, 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 the *PCI PIN Security Requirements*.

## Modular approach

The Council's PTS POI framework has taken a multifaceted modular approach:

- In support of modular device architectures offered by POI device vendors. These architectures are the result of the integration of several modules (often offered by third parties) that may include partial PIN entry features.
- Modular approvals, where a PIN entry device may be approved taking in consideration previously approved components.
- Offering evaluation modules (modular evaluation packages) that potentially optimize evaluation costs and time when laboratories are reviewing non-conventional architectures, conduct modular approvals or maintain existing approvals (changes in security components, etc.).

# Related Publications

The following references are applicable and related to the information in this manual.

| | |
|---|---|
| *Banking – Retail Financial Services Symmetric Key Management* | ANSI X9.24 |
| *Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms* | ANSI TR-31 |
| *Integrated Circuit Card Specification for Payment Systems – Book 2: Security and Key Management, Version 4.3, November 2011* | EMV 4.3 |
| *Identification Cards – Integrated Circuit Cards* | ISO 7816 |
| *Personal Identification Number (PIN) Management and Security* | ISO 9564 |
| *Banking – Key Management (Retail)* | ISO 11568 |
| *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 3: Block ciphers* | ISO/IEC 18033-3 |
| *Guidelines on Triple DES Modes of Operation*. | ISO TR 19038 |
| *Guideline for Implementing Cryptography In the Federal Government* | NIST SP 800-21 |
| *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* | NIST SP 800-22 |
| *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher* | NIST SP 800-67 |
| *PCI DSS v2.0* | PCI SSC |
| *PCI DSS Wireless Guidelines* | PCI SSC |
| *PCI PTS POI DTRs* | PCI SSC |
| *PCI PTS POI Evaluation Vendor Questionnaire* | PCI SSC |

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

# Required Device Information

This form is used by the vendor to provide details of the device to be submitted for evaluation.

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Device type claim** | **POS terminal containing a PIN entry device (select one):**<br>☐ Dedicated for PIN entry only ☐ UPT **(**Vending, AFD, Kiosk)<br>☐ Stand-alone POS terminal ☐ Other | | | | | | | | | | | | | | | | | | | | | | | | |
| | ☐ **Encrypting PIN pad (for ATM, Vending, AFD or Kiosk)** | | | | | | | | | | | | | | | | | | | | | | | | |
| | ☐ **Secure (encrypting) card reader** | | | | | | | | | | | | | | | | | | | | | | | | |
| | ☐ **Other secure component for PIN entry device** | | | | | | | | | | | | | | | | | | | | | | | | |
| | ☐ **Non-PED POI device** | | | | | | | | | | | | | | | | | | | | | | | | |
| **Manufacturer*:** | | | | | | | **Marketing Model Name/Number*:** | | | | | | | | | | | | | | | | | | |
| **Hardware Version Number*[A]:**<br>Use of "**x**" represents a request for field to be a variable | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| **Firmware/Software Version Number*:**<br>Use of "**x**" represents a request for field to be a variable | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| **Application Version Number*:** (if applicable) | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Version of *PCI PTS POI Security Requirements*:** | V4 | | | | | | **FAQ version:** | | | | | | | | | | | | | | | | | | |

| **Validation modules required (where applicable, please see Section C – Selection of Evaluation Modules):** | | **Yes** | **No** | **N/A** |
|---|---|---|---|---|
| | Core PIN Entry Security | ☐ | ☐ | ☐ |
| | POS Terminal Integration | ☐ | ☐ | ☐ |
| | Open Protocols | ☐ | ☐ | ☐ |
| | Secure Reading and Exchange of Data | ☐ | ☐ | ☐ |
| | Other | | | |

**Previously Approved Components Used* (if applicable)**

| **Vendor Name** | **Device Marketing/Model Name** | **PCI PTS Approval Number** | **Expiry Date** | **Product Type per PCI SSC Website** | **Other** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

***Continued on next page***

* Fields marked with an asterisk (*) will be used in the *PCI SSC Approved PIN Transaction Security Devices Approval List*.

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

| Device Photos | |
|---|---|
| **Photo(s) of device or component (if applicable) *** *Photos must show information for a Device Form Factor as noted in the Program Guide* | *Please attach a photo(s) of the terminal under evaluation, 320x320 pixels.* |

# Optional Use of Variables in the 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 POI 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 Information

## *POS Terminal Integration and Core Requirements Modules*

*Fields marked with an asterisk (*) will be used in the* PCI SSC Approved PIN Transaction Security Devices List.

| | | | |
|---|---|---|---|
| * | **PIN Support** | ☐ | N/A (explain) |
| | | ☐ | Offline only |
| | | ☐ | Offline and Online |
| | | ☐ | Online only |
| * | **Key Management** | ☐ | N/A (explain) |
| | | ☐ | DUKPT |
| | | ☐ | Fixed |
| | | ☐ | MK/SK |
| * | **PIN Entry Technology** | ☐ | N/A (explain) |
| | | ☐ | Physical (Hard) Keys |
| | | ☐ | Touch screen |
| | | ☐ | Other |
| * | **Prompt Control** | ☐ | N/A (explain) |
| | | ☐ | Acquirer-controlled |
| | | ☐ | Terminal manufacturer-controlled |
| | | ☐ | Other (explain) |
| * | **Other Functions Provided** | ☐ | Display |
| | | ☐ | CTLS |
| | | ☐ | ICCR |
| | | ☐ | MSR |
| | | ☐ | OP |
| | | ☐ | SRED |

## *Open Protocols Module – Protocol Declaration Form*

*Fields marked with an asterisk (*) will be used in the* PCI SSC Approved PIN Transaction Security Devices List*.*

| | | | |
|---|---|---|---|
| | **Link Layer Protocols** | ☐ | Yes |
| | | ☐ | No |
| | | ☐ | N/A |
| | | Name | |
| | **IP Protocols** | ☐ | Yes |
| | | ☐ | No |
| | | ☐ | N/A |
| | | Name | |
| | | Number | |
| | **Security Protocols** | ☐ | Yes |
| | | ☐ | No |
| | | ☐ | N/A |
| | | Name | |
| | **IP Services** | ☐ | Yes |
| | | ☐ | No |
| | | ☐ | N/A |
| | | Name | |
| | | Port Number | |

## *Secure Reading and Exchange of Data Module*

*Fields marked with an asterisk (*) will be used in the* PCI SSC Approved PIN Transaction Security Devices List*.*

| | | | |
|---|---|---|---|
| | **Does the terminal utilize secure reading and exchange of data?** | ☐ | Yes |
| | | ☐ | No |
| | | ☐ | N/A (explain) |

# Evaluation Module Groupings

In order to allow evaluation flexibility and support business needs of vendors, requirements were grouped in to a series of sets as illustrated in the following table. The laboratory will provide the necessary guidance for the selection of the evaluation modules.

| Evaluation Module | Requirements Set | Remarks |
|---|---|---|
| **1: Core Requirements** | Physical and logical Security | The core logical and physical requirements of PIN-acceptance POI devices |
| **2: POS Terminal Integration** | POS Terminal Integration | The PCI PTS POI approval framework is oriented to the evaluation of integrated PIN entry devices (i.e., device where PIN entry functionality is in a secure logical and physical perimeter).<br><br>However, it allows the re-use of previously approved individual components or their combinations (card readers, display, keypads, or secure processors) into the approval process of integrated PIN entry devices.<br><br>The POS Terminal integration Evaluation Module ensures that the integration of previously approved components does not impair the overall security as stated in the security requirements. This module also supports the cost-effective maintenance of components.<br><br>This module includes security management requirements applicable to the integrated device. |
| **3: Open Protocols** | Open Protocols | A set of requirements that ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities. |
| **4: Secure Reading and Exchange of Data** | Requirements in support of cardholder account data encryption | A set of requirements that ensures cardholder data is protected. |
| **5: Device Management** | Device Management (Manufacturing and initial key loading) | Life cycle requirements for POIs and their components up until the point of initial key loading. The information is not currently validated, but is still required for vendors to complete. |

# Evaluation Module 1: Core Requirements

## A – Core Physical Security Requirements

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

| 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 by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader[B]; **and**<br>***Note:*** *The replacement of both the front and rear casings shall be considered as part of any attack scenario. All attacks shall include a minimum of ten hours' attack time for exploitation.* | ☐ | ☐ | ☐ |
| **A2** | Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms. | ☐ | ☐ | ☐ |
| **A3** | The security of the device is not compromised by altering:<br>▪ Environmental conditions<br>▪ Operational conditions<br>*(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)* | ☐ | ☐ | ☐ |
| **A4** | Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation[C]. | ☐ | ☐ | ☐ |

[B] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **A5** | There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring—even with the cooperation of the device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation[C]. | ☐ | ☐ | ☐ |
| **A6** | Determination of any PIN-security-related cryptographic key resident in 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[C]. | ☐ | ☐ | ☐ |
| ***Note:*** *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.*<br>▪ *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.*<br>▪ *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.*<br>▪ *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.* | | | | |
| **A7** | The unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation[C]. | ☐ | ☐ | ☐ |
| **A8** | The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder. | ☐ | ☐ | ☐ |
| **A9** | It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation[C]. | ☐ | ☐ | ☐ |

[C] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **A10** | Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation[C]. | ☐ | ☐ | ☐ |
| **A11** | If PIN entry is accompanied by audible tones, the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit. | ☐ | ☐ | ☐ |

# B – Core Logical Security Requirements

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

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **B1** | The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours. | ☐ | ☐ | ☐ |
| **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 the clear-text PIN or other sensitive data. | ☐ | ☐ | ☐ |
| **B3** | The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions. | ☐ | ☐ | ☐ |
| **B4** | If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted. | ☐ | ☐ | ☐ |
| **B4.1** | The firmware must support the authentication of applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4. | ☐ | ☐ | ☐ |
| **B5** | The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks. | ☐ | ☐ | ☐ |
| **B6** | Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button.<br>The device must automatically clear its internal buffers when either:<br>▪ The transaction is completed, or<br>▪ The device has timed out waiting for the response from the cardholder or merchant. | ☐ | ☐ | ☐ |
| **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. | ☐ | ☐ | ☐ |

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **B8** | To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode. | ☐ | ☐ | ☐ |
| **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 it is generating numbers sufficiently unpredictable. | ☐ | ☐ | ☐ |
| **B10** | The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination. | ☐ | ☐ | ☐ |
| **B11** | The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle. | ☐ | ☐ | ☐ |
| **B12** | The PIN-encryption technique implemented in the device is a technique included in ISO 9564. | ☐ | ☐ | ☐ |
| **B13** | It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the device.<br>The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values. | ☐ | ☐ | ☐ |
| **B14** | There is no mechanism in the device that would allow the outputting of a private or secret clear-text key or clear-text PIN, 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. | ☐ | ☐ | ☐ |
| **B15** | The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations. | ☐ | ☐ | ☐ |

***Note:*** *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.*

- *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.*
- *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.*
- *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **B16** | All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation[4] to circumvent. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented. | ☐ | ☐ | ☐ |
| **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 of the device including, but not limited to, modifying data objects belonging to another application or the OS. | ☐ | ☐ | ☐ |
| **B18** | The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege. | ☐ | ☐ | ☐ |
| **B19** | The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal. | ☐ | ☐ | ☐ |
| **B20** | A user-available security policy from the vendor addresses the proper use of the POI 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 POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy. | ☐ | ☐ | ☐ |

[4] As defined in Appendix B of the *PCI PTS POI DTRs.*

## C – Online PIN Security Requirement

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **C1** | If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the device prohibits unauthorized key replacement and key misuse. | ☐ | ☐ | ☐ |

## D – Offline PIN Security Requirements

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **D1** | It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation[E], nor is it possible for both an ICC card and any other foreign object to reside within the card insertion slot.<br>***Note:*** *All attacks shall include a minimum of ten hours' attack time for exploitation.* | ☐ | ☐ | ☐ |
| **D2** | The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable. | ☐ | ☐ | ☐ |
| **D3** | The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder. | ☐ | ☐ | ☐ |

[E] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **D4** | PIN protection during transmission between the device encrypting the PIN and the ICC reader (at least **two** must apply): | | | |
| | If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be:<br>▪ An enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.<br>▪ A plaintext PIN, the PIN block shall be enciphered from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.<br>If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be:<br>▪ An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.<br>▪ A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564. | ☐ | ☐ | ☐ |

# Evaluation Module 2: POS Terminal integration

## E – POS Terminal Integration Security Requirements

The PCI PTS POI approval framework is oriented to the evaluation of complete PIN-acceptance POI devices (i.e., devices where PIN entry functionality is a secure logical and physical perimeter).

However it also allows the re-use of previously approved individual components or their combinations (card readers, display, keypads, or secure processors) into the approval process of integrated PIN entry devices.

The POS Terminal Integration Evaluation Module ensures that the integration of previously approved components does not impair the overall security as stated in the security requirements. This module also supports the cost effective maintenance of components.

This module includes security management requirements applicable to the integrated device and is applicable anytime previously approved components are combined that will result in a device meeting a PTS approval class.

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

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| | **Configuration Management** | | | |
| **E1** | Any secure component integrated into a PIN entry POI terminal submitted for evaluation has a clearly identified physical and logical security perimeter (related to PIN entry and card-reading functions). | ☐ | ☐ | ☐ |
| | **Integration of PIN Entry Functions** | | | |
| **E2.1** | The logical and physical integration of a PCI-approved secure component (or components) into a PIN entry POI terminal must not impact the overall PIN protection level. | ☐ | ☐ | ☐ |
| **E2.2** | The PIN pad (PIN entry area) and the surrounding area must be designed and engineered in such a way that the complete device does not facilitate the fraudulent placement of an overlay over the PIN pad.<br>An overlay attack must require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation[F]. | ☐ | ☐ | ☐ |

[F] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| | **Integration into a POS Terminal** | | | |
| **E3.1** | The logical and physical integration of an approved secure component into a PIN entry POI terminal does not create new attack paths to the PIN. | ☐ | ☐ | ☐ |
| **E3.2** | The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack). | ☐ | ☐ | ☐ |
| **E3.3** | There is a clear logical and/or physical segregation between secure components and non-secure components integrated into the same device. | ☐ | ☐ | ☐ |
| ***Note:*** *If the POI device has a keypad that can be used to enter non-PIN data, the device must meet at least one of the following: A7, B16, or E3.4.*<br>▪ *A7 applies to any components or paths containing plaintext display signals between the cryptographic processor and display unit.*<br>▪ *B16 applies to devices that allow for updates of prompts or use cryptography to communicate with a display, whether performed by the vendor or the acquirer.*<br>▪ *E3.4 is appropriate for unattended devices that do not meet any of the aforementioned.* | | | | |
| **E3.4** | The POI (application) must enforce the correspondence between the display messages visible to the cardholder and the operating state (i.e., secure or non-secure mode) of the PIN entry device, e.g., by using cryptographic authentication.<br>If commands impacting the correspondence between the display messages and the operating state of the PIN entry device are received from an external device (e.g., a store controller), the commands enabling data entry must be authenticated.<br>The alteration of the correspondence between the display messages visible to the cardholder and the operating state of the PIN entry device cannot occur without requiring an attack potential of at least 18 per POI for identification and initial exploitation with a minimum of 9 for exploitation[G]. | ☐ | ☐ | ☐ |
| **E3.5** | The PIN-accepting POI terminal must be equipped with only one payment card PIN-acceptance interface, e.g., a keyboard. If another interface is present which can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry, e.g., it must not have numeric keys, or it is not possible to use it otherwise for numeric entry or it is controlled in a manner consistent with B16. | ☐ | ☐ | ☐ |

[G] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| | **Removal Requirements** | | | |
| **E4.1** | The device is protected against unauthorized removal. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation[l]. | ☐ | ☐ | ☐ |
| **E4.2** | The vendor documents, maintains and makes available to integrators details on how to implement the protection system against unauthorized removal. | ☐ | ☐ | ☐ |
| **E4.3** | For each embedded device, the protection system against unauthorized removal is properly implemented as documented by the embedded device manufacturer. | ☐ | ☐ | ☐ |

# Evaluation Module 3: Open Protocols

## F – Discovery

The vendor must complete the following Security Compliance Statements concerning physical and logical interfaces.

This table must be completed considering all open protocol interfaces **in its entirety.** Answer "Yes" if **all** the options declared in the *Open Protocols Module – Protocol Declaration Form* are meet these security requirements.

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **F1** | A**ll** public domain protocols and interfaces available on the platform are clearly identified in the *Open Protocols Module – Protocol Declaration Form*. | ☐ | ☐ | ☐ |

# G – Vulnerability Assessment

The vendor must complete the following Security Compliance Statements concerning the Vulnerability Assessment.

This table must be completed considering the vulnerability assessment **in its entirety**. Answer "Yes" if **all** the options declared in the *Open Protocols Module – Protocol Declaration Form* meet these security requirements.

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **G1** | The platform vendor has vulnerability assessment procedures and documentation for each protocol and interface listed in F1 of the Open *Protocols Module – Protocol Declaration Form*. | ☐ | ☐ | ☐ |
| **G2** | The device has undergone a vulnerability assessment to ensure that the protocols and interfaces list in F1 do not contain exploitable vulnerabilities. | ☐ | ☐ | ☐ |
| | a) The vulnerability assessment is supported by a documented analysis describing the security of the protocols and interfaces. | | | |
| | b) The vulnerability assessment is supported by a vulnerability survey of information available in the public domain. | | | |
| | c) The vulnerability assessment is supported by testing. | | | |
| **G3** | The platform vendor has vulnerability disclosure measures in place for the device. | ☐ | ☐ | ☐ |
| | a) The vulnerability-disclosure measures are documented. | | | |
| | b) The vulnerability-disclosure measures ensure a timely distribution of information about newly found vulnerabilities. This information includes identification, description, and assessment of the vulnerabilities. | | | |
| | c) The vulnerability-disclosure measures ensure a timely distribution of mitigation measures. | | | |

# H – Vendor Guidance

The vendor must complete the following Security Compliance Statements concerning the Vendor Guidance.

This table must be completed considering the vendor guidance **in its entirety**. Answer "Yes" if **all** the open protocols and interfaces declared in the *Open Protocols Module – Protocol Declaration Form* meet these security requirements.

**Table H: Vendor Guidance in its Entirety**

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **H1** | The device has security guidance that describes how protocols and services must be used for each interface that is available on the platform identified in the *Open Protocols Module – Protocol Declaration Form*. | ☐ | ☐ | ☐ |
| **H2** | The device has guidance that describes the default configuration for each protocol and services for each interface that is available on the platform | ☐ | ☐ | ☐ |
| **H3** | The device has guidance for key management describing how keys and certificates must be used. | ☐ | ☐ | ☐ |
| | a) The key-management guidance is at the disposal of internal users, and/or of application developers, system integrators, and end-users of the platform. | | | |
| | b) Key-management security guidance describes the properties of all keys and certificates that can be used by the platform. | | | |
| | c) Key-management security guidance describes the responsibilities of the platform vendor, application developers, system integrators, and end-users of the platform. | | | |
| | d) Key-management security guidance ensures secure use of keys and certificates. | | | |

# I – Operational Testing

The vendor must complete the following Security Compliance Statements concerning operational testing of the device.

This table must be completed considering the operational testing **in its entirety**. Answer "Yes" if **all** the open protocols and interfaces declared in the *Open Protocols Module – Protocol Declaration Form* meet the security requirement.

**Table I: Operational Testing in their Entirety**

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **I1** | The device has **all** the security protocols that are available on the platform clearly identified in the *Open Protocols Module – Protocol Declaration Form*. | ☐ | ☐ | ☐ |
| **I2** | The device is able to provide confidentiality of data sent over a network connection. | ☐ | ☐ | ☐ |
| | a) Encryption mechanism utilizes key sizes appropriate for the algorithm(s) in question. | | | |
| | b) Encryption is provided by using keys that are established in a secure manner using appropriate key-management procedures, such as those listed in NIST SP800-21, *Guidelines for Implementing Cryptography*. | | | |
| **I3** | The device is able to provide the integrity of data that is sent over a network connection. | ☐ | ☐ | ☐ |
| | a) Integrity is provided by a MAC as defined in ISO 16609, or by a digital signature. | | | |
| | b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. | | | |
| | c) Examples of appropriate algorithms and minimum key sizes are stated in Appendix D of the *PCI PTS POI DTRs.* | | | |
| **I4** | The device uses a declared security protocol to authenticate the server. | ☐ | ☐ | ☐ |
| | a) Server authentication utilizes key sizes appropriate for the algorithm(s) in question. | | | |
| | b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. | | | |
| | c) The platform is able to verify the validity of the public keys it receives. | | | |
| | d) The platform is able to verify the authenticity of the public keys it receives. | | | |

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **I5** | The device is able to detect replay of messages, and enables the secure handling of the exceptions. | ☐ | ☐ | ☐ |
| **I6** | The platform implements session management. | ☐ | ☐ | ☐ |
| | a) The platform keeps track of all connections and restricts the number of sessions that can remain active on the platform to the minimum necessary number. | | | |
| | b) The platform sets time limits for sessions and ensures that sessions are not left open for longer than necessary. | | | |

## J – Maintenance

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **J1** | The platform vendor maintains guidance describing configuration management for the platform | ☐ | ☐ | ☐ |
| | a) The guidance is at the disposal of internal users, and/or of application developers, system integrators and end-users of the platform. | | | |
| | b) The guidance covers the complete platform; including firmware, applications, certificates and keys. | | | |
| | c) The guidance covers the complete life cycle of the platform from development, over manufacturing, up to delivery and operation. | | | |
| | d) The security guidance ensures that unauthorized modification is not possible. | | | |
| | e) The security guidance ensures that any modification of a PTS-approved platform that impacts platform security, results in a change of the platform identifier. | | | |
| **J2** | The platform vendor has maintenance measures in place. | ☐ | ☐ | ☐ |
| | a) The maintenance measures are documented. | | | |
| | b) The maintenance measures ensure timely detection of vulnerabilities that apply to the device by periodical execution of a vulnerability assessment that includes activities such as: analysis, survey of information available in the public domain, and testing. | | | |
| | c) The maintenance measures ensure timely assessment and classification of newly found vulnerabilities. | | | |
| | d) The maintenance measures ensure timely creation of mitigation measures for newly found vulnerabilities that may impact platform security. | | | |
| **J3** | Deployed platforms can be updated, and the platform vendor maintains guidance describing how the update mechanism is to be used. | ☐ | ☐ | ☐ |
| **J4** | The update mechanism ensures confidentiality, integrity, server authentication, and protection against replay by using an appropriate and declared security protocol. If the device allows software and/or configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted. | ☐ | ☐ | ☐ |

# Evaluation Module 4: Secure Reading and Exchange of Data (SRED)

This module defines requirements for cardholder account data protection.

## K – Account Data Protection

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| | **Generic Security Requirements** | | | |
| **K1** | All account data is either encrypted immediately upon entry or entered in clear-text into a secure device and processed within the secure controller of the device. | ☐ | ☐ | ☐ |
| **K1.1** | The device protects all account data upon entry (consistent with A10 for magnetic stripe data and D1 for Chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation[H].<br><br>***Note:*** *MSRs and ICCRs must meet the attack potentials stipulated in DTRs A10 and D1 respectively.* | ☐ | ☐ | ☐ |
| **K1.2** | Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms. | ☐ | ☐ | ☐ |
| **K2** | The logical and physical integration of an approved secure card reader into a PIN entry POI terminal does not create new attack paths to the account data. The account data is protected (consistent with A2) from the input component to the secure controller of the device. | ☐ | ☐ | ☐ |
| **K3** | Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation.[H] | ☐ | ☐ | ☐ |
| **K3.1** | Public keys must be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorized modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation.[H] | ☐ | ☐ | ☐ |
| **K4** | All account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (e.g., AES, TDES) and should use ANSI X9 or ISO-approved modes of operation. | ☐ | ☐ | ☐ |

[H] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **K5** | If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device. | ☐ | ☐ | ☐ |
| **K6** | The device supports data origin authentication of encrypted messages. | ☐ | ☐ | ☐ |
| **K7** | Secret and private keys that reside within the device to support account data encryption are unique per device. | ☐ | ☐ | ☐ |
| **K8** | Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted.<br>The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values. | ☐ | ☐ | ☐ |
| **K9** | If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied. | ☐ | ☐ | ☐ |
| **K10** | The firmware, and any changes thereafter, have been inspected and reviewed consistent with B3. | ☐ | ☐ | ☐ |
| **K11.1** | The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4. | ☐ | ☐ | ☐ |
| **K11.2** | The vendor must provide clear security guidance consistent with B2 and B6 to all application developers to ensure:<br>▪ That it is not possible for applications to be influenced by logical anomalies which could result in clear text data being outputted whilst the terminal is in encrypting mode.<br>▪ That account data is not retained any longer, or used more often, than strictly necessary. | ☐ | ☐ | ☐ |
| **K12** | If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted. | ☐ | ☐ | ☐ |
| **K13** | The device's functionality shall not be influenced by logical anomalies consistent with B2. | ☐ | ☐ | ☐ |
| **K14** | If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), then requirements specified in DTR Module 3: Open Protocols Requirements have been met. | ☐ | ☐ | ☐ |

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **K15** | When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication. | ☐ | ☐ | ☐ |
| **K15.1** | When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device. | ☐ | ☐ | ☐ |
| **K15.2** | Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary. | ☐ | ☐ | ☐ |
| **K16** | If the device is capable of generating surrogate PAN values to be outputted outside of the device, it is not possible to determine the original PAN knowing only the surrogate value. | ☐ | ☐ | ☐ |
| **K16.1** | If using a hash function to generate surrogate PAN values, input to the hash function must use a salt with minimum length of 64-bits. | ☐ | ☐ | ☐ |
| **K16.2** | If using a hash function to generate surrogate PAN values, the salt is kept secret and appropriately protected. Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per device for identification and initial exploitation with a minimum of 8 for exploitation[I]. | ☐ | ☐ | ☐ |
| **K17** | The key-management techniques implemented in the device are consistent with B11. | ☐ | ☐ | ☐ |
| **K18** | The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination. | ☐ | ☐ | ☐ |
| **K19** | Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data.<br>(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.) | ☐ | ☐ | ☐ |
| **K20** | If the device supports multiple applications, it must enforce the separation between applications consistent with B17. | ☐ | ☐ | ☐ |

[I] As defined in Appendix B of the *PCI PTS POI DTRs.*

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **K21** | The following features of the device's operating system must be in place:<br>▪ The operating system of the device must contain only the software (components and services) necessary for the intended operation.<br>▪ The operating system must be configured securely and run with least privilege.<br>▪ The security policy enforced by the device must not allow unauthorized or unnecessary functions.<br>▪ API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed). | ☐ | ☐ | ☐ |
| **K22** | 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, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data. | ☐ | ☐ | ☐ |
| **K23** | Sensitive services are protected from unauthorized use consistent with B8. | ☐ | ☐ | ☐ |

# Evaluation Module 5: Device Management Security Requirements

## L – 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 do not currently validate this information; however, the vendor is still required to complete these forms and the information will be reported to PCI for review and, if necessary, corrective action:

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **L1** | Change-control procedures are in place so that any intended security-relevant change to the physical or functional capabilities of the device causes a re-certification of the device under the applicable Security Requirements of this document. | ☐ | ☐ | ☐ |
| **L2** | The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing life cycle–e.g., by using dual control or standardized cryptographic authentication procedures. | ☐ | ☐ | ☐ |
| **L3** | The device is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Core PIN Entry and/or POS Terminal Integration Security Requirements evaluation, and that unauthorized substitutions have not been made. | ☐ | ☐ | ☐ |
| **L4** | 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. | ☐ | ☐ | ☐ |
| **L5** | 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. | ☐ | ☐ | ☐ |
| **L6** | If the device will be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the device during manufacturing, then this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device under dual control to ensure that it is not disclosed during installation. | ☐ | ☐ | ☐ |

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **L7** | Security measures are taken during the development and maintenance of POI 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 POI 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 POI security-related components. The evidence shall justify that the security measures provide the necessary level of protection to maintain the integrity of the POI security-related components. | ☐ | ☐ | ☐ |
| **L8** | 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. | ☐ | ☐ | ☐ |

# M – Between Manufacturer and Facility of Initial Key Loading or Facility 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 do not currently validate this information; however, the vendor is still required to complete these forms and the information will be reported to PCI for review, and if necessary corrective action.

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **M1** | The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI.<br><br>Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time.<br><br>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. | ☐ | ☐ | ☐ |
| **M3** | While in transit from the manufacturer's facility to the initial key-loading facility, the device is:<br>▪ Shipped and stored in tamper-evident packaging; and/or<br>▪ Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel. | ☐ | ☐ | ☐ |
| **M4** | The device's development security documentation must provide means to the initial key-loading facility to assure the authenticity of the TOE's security relevant components. | ☐ | ☐ | ☐ |
| **M5** | If the manufacturer is in charge of initial key loading, then the manufacturer must verify the authenticity of the POI security-related components. | ☐ | ☐ | ☐ |

| Number | Description of Requirement | Yes | No | N/A |
|---|---|---|---|---|
| **M6** | If the manufacturer is not in charge of initial key loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components. | ☐ | ☐ | ☐ |
| **M7** | Each device shall have a unique visible identifier affixed to it. | ☐ | ☐ | ☐ |
| **M8** | The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire life cycle of the POI security-related components and of the manner in which those components are integrated into a single POI, e.g.:<br>▪ Data on production and personalization<br>▪ Physical/chronological whereabouts<br>▪ Repair and maintenance<br>▪ Removal from operation<br>▪ 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 | | | |
|---|---|---|---|
| Manufacturer: | | | |
| Address 1: | | | |
| Address 2: | | | |
| City: | | State/Province: | |
| Country: | | Mail Code: | |
| Primary Contact: | | | |
| Position/Title: | | | |
| Telephone No: | | Fax: | |
| E-mail Address: | | | |
| Website: | | | |

# Compliance Declaration Statement – Form B

| Compliance Declaration | |
|---|---|
| **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 PIN entry device is:

☐ In full compliance with the standards set forth above in the Manufacturer Self-Assessment Form.

☐ Not in full compliance with the standards set forth above in the Manufacturer Self-Assessment Form as indicated in the attached Exception Form (*Form C*).

| | |
|---|---|
| | |
| *Signature* ↑ | *Date* ↑ |
| | |
| *Printed Name* ↑ | *Title* ↑ |

Attach to this form a device-specification sheet that highlights the device characteristics, including photos of the device. 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

| | |
|---|---|
| **Manufacturer:** | |
| **Model Name and Number:** | |

**INSTRUCTIONS:**

*For any statement 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. Seven functionalities have been identified, as shown below.

| Functionality | Description |
|---|---|
| **PIN Entry** | This is the functionality present for any device under test that captures the PIN from the cardholder and turns it into information. No assumption is made upon the format; this could be a PIN block, but also cover partial PIN information such as a digit, if this partial information is going to form a PIN during a legitimate transaction. |
| **Keys** | This functionality is considered whenever the device under evaluation contains—even temporarily—keys involved in PIN security. Under the scope of this functionality are the secret keys of symmetric algorithms, the private keys of asymmetric algorithms, and the public keys of asymmetric algorithms (with the limitation of scope to their integrity and authenticity). |
| **Card Reader** | This functionality applies whenever a device under evaluation has the capability to capture card data, irrespective of the technology being used (i.e., it encompasses both the magnetic stripe and smart card readers). This is further broken down into ICCR and MSR functionality. |
| **Feedback to cardholder** | Each time a device under evaluation implements any way of possibly giving feedback to the cardholder during its PIN-based transaction, it applies to this functionality. This includes but is not limited to auditory and visible feedback (i.e., displays). |
| **Terminal is a module** | If the device under evaluation is designed to be integrated into equipment, then it applies for “terminal is a module” functionality. Modules are also referred to as OEM equipment. |
| **Terminal is compound** | A device under evaluation is said to be compound whenever it incorporates one or more modules, in order to cover one or several of the aforementioned functionalities. Being a compound device does not preclude the applicability of “terminal is a module” functionality. Both functionalities are independent. |
| **Terminal implements TCP/IP stack** | A device under evaluation implements a TCP/IP stack and associated open protocols. |

# 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" from the functionality column to the baseline column. "x" stands for "applicable," in which case the requirement must be considered for vendor questionnaire and possibly evaluation.

| Requirement | PIN Entry | Keys | ICCR | MSR | Feedback to cardholder | Device is a module | Device is compound | Implements TCP/IP stack | Protects account data | Conditions |
|---|---|---|---|---|---|---|---|---|---|---|
| **Core Requirements Modules** | | | | | | | | | | |
| **Core Physical Security Requirements** | | | | | | | | | | |
| A1 | x | | | | | | | | | |
| A2 | x | x | | | | | | | | |
| A3 | x | x | | | | | | | | |
| A4 | x | x | | | | | | | | |
| A5 | x | | | | | | | | | |
| A6 | | x | | | | | | | | |
| A7 | | | | | x | | | | | |
| A8 | x | | | | | | | | | *If keypad that can be used to enter non-PIN data.* |
| A9 | | | | x | | | | | | |
| A10 | | | x | | | x | | | | |
| A11 | x | | | | x | | | | | |

| Requirement | PIN Entry | Keys | ICCR | MSR | Feedback to cardholder | Device is a module | Device is compound | Implements TCP/IP stack | Protects account data | Conditions |
|---|---|---|---|---|---|---|---|---|---|---|
| **Core Logical Security Requirements** | | | | | | | | | | |
| B1 | x | x | | | | | | x | x | |
| B2 | x | x | | | | | | | | |
| B3 | x | x | | | | | | | | |
| B4 | x | x | | | | | | | | |
| B4.1 | x | x | | | | | | | | |
| B5 | x | | | | | | | | | |
| B6 | x | | | | | | | | | |
| B7 | x | x | | | | | | | | |
| B8 | x | x | | | | | | | | |
| B9 | | x | | | | | | x | x | |
| B10 | x | | | | | | | | | |
| B11 | | x | | | | | | | | |
| B12 | x | x | | | | | | | | |
| B13 | | x | | | | | | | | |
| B14 | x | x | | | | | | | | |
| B15 | x | | | | | | | | | |
| B16 | | | | | x | | | | | *If keypad that can be used to enter non-PIN data.* |
| B17 | x | | | | | | | | | |
| B18 | x | | | | | | | | | |
| B19 | | | x | x | | x | | | | |
| B20 | x | x | x | x | x | x | x | x | x | |
| **Additional Online Requirement** | | | | | | | | | | |
| C1 | | x | | | | | | | | |
| **Additional Offline Requirements** | | | | | | | | | | |
| D1 | | | x | | | | | | | |
| D2 | | | x | | | | | | | |

| Requirement | PIN Entry | Keys | ICCR | MSR | Feedback to cardholder | Device is a module | Device is compound | Implements TCP/IP stack | Protects account data | Conditions |
|---|---|---|---|---|---|---|---|---|---|---|
| D3 | | | x | | | | | | | |
| D4 | | | x | | | | | | | |

| Requirement | PIN Entry | Keys | ICCR | MSR | Feedback to cardholder | Device is a module | Device is compound | Implements TCP/IP stack | Protects account data | Conditions |
|---|---|---|---|---|---|---|---|---|---|---|
| **POS Terminal Integration Requirements** | | | | | | | | | | |
| E1 | x | x | x | | x | x | x | x | x | Always applicable |
| E2.1 | x | | | | | | x | | | |
| E2.2 | x | | | | | | x | | | |
| E3.1 | | | | | | | x | | | |
| E3.2 | | | x | | | x | x | | | |
| E3.3 | x | | | | | | x | | | |
| E3.4 | x | | | | x | | x | | | *If keypad that can be used to enter non-PIN data.* |
| E3.5 | x | | | | | | x | | | |
| E4.1 | x | | x | | | x | | | | |
| E4.2 | x | | x | | | x | | | | |
| E4.3 | | | | | | | x | | | |
| **Open Protocols Security Module** | | | | | | | | | | |
| All | | | | | | | | x | | All requirements applicable |
| **Secure Reading and Exchange of Data Module** | | | | | | | | | | |
| All | | | | | | | | | x | All requirements applicable |

| Requirement | PIN Entry | Keys | ICCR | MSR | Feedback to cardholder | Device is a module | Device is compound | Implements TCP/IP stack | Protects account data | Conditions |
|---|---|---|---|---|---|---|---|---|---|---|
| **Device Security Requirements** | | | | | | | | | | |
| **During Manufacturing** | | | | | | | | | | |
| L1 | x | x | x | x | x | x | x | x | x | |
| L2 | x | x | x | x | x | x | x | x | x | |
| L3 | x | x | x | x | x | x | x | x | x | |
| L4 | x | x | x | x | x | x | x | x | x | |
| L5 | x | x | x | x | x | x | x | x | x | |
| L6 | x | x | x | x | x | x | x | x | x | |
| L7 | x | x | x | x | x | x | x | x | x | |
| L8 | x | x | x | x | x | x | x | x | x | |
| **Between Manufacturing and Initial Key Loading** | | | | | | | | | | |
| M1 | x | x | x | x | x | x | x | | x | |
| M2 | x | x | x | x | x | x | x | | x | |
| M3 | x | x | x | x | x | x | x | | x | |
| M4 | x | x | x | x | x | x | x | | x | |
| M5 | x | x | x | x | x | x | x | | x | |
| M6 | x | x | x | x | x | x | x | | x | |
| M7 | x | x | x | x | x | x | x | | x | |
| M8 | x | x | x | x | x | x | x | | x | |

# Glossary

| Term | Definition |
|---|---|
| **Account Data** | At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code. Other transaction-relevant information may be included at the vendor's discretion.<br><br>***Note:*** *Encrypted, truncated, masked and hashed PAN data (with salt) may be outputted outside of the device.* |
| **Accountability** | The property that ensures that the actions of an entity may be traced uniquely to that entity. |
| **Active Erasure** | The intentional clearing of data from storage through a means other than simply removing power (e.g. zeroization, inverting power). |
| **Advanced Encryption Algorithm (AES)** | The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). |
| **Application** | Application is considered to be any code in the device that does not impact compliance to these security requirements. |
| **Authentication** | The process for establishing unambiguously the identity of an entity, process, organization, or person. |
| **Authorization** | The right granted to a user to access an object, resource, or function. |
| **Authorize** | To permit or give authority to a user to communicate with or make use of an object, resource, or function. |
| **Check Value** | A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible. Check values shall not allow the determination of the secret key. |
| **Ciphertext** | An encrypted message. |
| **Clear-text** | See *Plaintext.* |
| **Compromise** | In cryptography, the breaching of secrecy and/or security.<br><br>A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material). |

| Term | Definition |
|---|---|
| **Cryptographic Key Component (Key Component)** | One of at least two parameters having the characteristics (for example, format, randomness) of a cryptographic key that is combined with one or more like parameters—for example, by means of modulo-2 addition—to form a cryptographic key. Throughout this document, "key component" may be used interchangeably with "secret share" or key "fragment." |
| **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 encrypting and decrypting data. |
| **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 Controller** | The device controller may be integrated in either the EPP or the ICCR; or it may be a separate module, possibly PC-operated by a standard operating system. In the latter case, the device controller may contain a cryptographic module if used for PIN re-encryption. |
| **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. |
| **DTR** | Derived Test Requirement |
| **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. |
| **Electromagnetic Emanations (EME)** | An intelligence-bearing signal that, 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 using previously encrypted data blocks. |
| **Electronic Key Entry** | The entry of cryptographic keys into a security cryptographic device in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered. |
| **EM** | Electro-magnetic |

| Term | Definition |
|---|---|
| **Encipher** | See *Encrypt.* |
| **Encrypt** | The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext—i.e., the process of transforming plaintext into ciphertext to hide the information content of the data. |
| **Encrypted Key (Ciphertext Key)** | A cryptographic key that has been encrypted with a key-encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key. |
| **Encrypting PIN Pad (EPP)** | A device for secure PIN entry and encryption in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (e.g., an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell.<br>Encrypting PIN pads require integration into UPTs or ATMs. |
| **Encryption** | See *Encrypt.* |
| **Entropy** | The uncertainty of a random variable. |
| **Evaluation Laboratory** | Independent entity that performs a security evaluation of the POS terminal against the PCI Security Requirements. |
| **Evaluation Module** | Evaluation package corresponding to a well-defined set of requirements. |
| **Firmware** | For purposes of these requirements, firmware is considered to be any code within the device that provides security protections needed to comply with device security requirements or can impact compliance to these security requirements. Firmware may be further segmented by code necessary to meet Core, OP or SRED.<br>Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware. |

| 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.<br>Approved hash functions satisfy the following properties:<br>1) One-way: It is computationally infeasible to find any input that maps to any pre-specified output.<br>2) Collision-resistant: It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output.<br>It may be used to reduce a potentially long message into a "hash value" or "message digest" 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. |
| **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. |
| **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 organizations. |
| **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 criteria for composite evaluations, attack paths, attack quotations, and methodology. |
| **KEK** | See *Key-Encrypting Key.* |
| **Key** | See *Cryptographic 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.* |

| Term | Definition |
|---|---|
| **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-encrypting (encipherment or exchange) Key (KEK)** | A cryptographic key that is used for the encryption or decryption of other keys. |
| **Key Establishment** | The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport. |
| **Key Fragment** | See *Cryptographic Key Component.* |
| **Key Generation** | Creation of a new key for subsequent use. |
| **Key Instance** | The occurrence of a key in one of its permissible forms, that is, plaintext key, key components and enciphered key. |
| **Key Loading** | Process by which a key is manually or electronically transferred into a secure cryptographic device. |
| **Key Management** | The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving. |
| **Key Pair** | Two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; the other, termed the private key, is expected to be restricted so that it is known only to the appropriate entities. |
| **Key Replacement** | Substitution of 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 (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 Storage** | Holding of the key in one of the permissible forms. |
| **Key Termination** | Occurs when a key is no longer required for any purpose and all copies of the key and information required to regenerate or reconstruct the key have been deleted from all locations where they ever existed. |
| **Key Transport** | A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected. |
| **Key Usage** | Employment of a key for the cryptographic purpose for which it was intended |

| Term | Definition |
|---|---|
| **Key variant** | A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key. |
| **Manual Key Entry** | The entry of cryptographic keys into a secure cryptographic device, using devices such as buttons, thumb wheels, or a keyboard. |
| **Masking** | Method of concealing a segment of data when displayed. At most the first six and last four digits of a PAN can be displayed by the device**.** |
| **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. |
| **Merchant** | An entity that uses at the point of sale a PCI PTS approved POI PIN-acceptance device as part of a card-acceptance contract with an acquiring bank. |
| **Message Authentication Code (MAC)** | A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data (example: a hash-based message authentication code). |
| **Non-Reversible Transformation** | See *Irreversible Transformation.* |
| **OEM Card Reader** | A self-contained, secure chip, or hybrid card reader, which requires integration into UPTs. |
| **OEM PED** | A self-contained point-of-sale POI device containing a PIN pad, display and/or card reader, which requires integration into a final casing. Generally used in UPTs. |
| **Opaque** | Impenetrable by light (i.e., light within the visible spectrum of wavelength range of 400nm to 750nm); neither transparent nor translucent within the visible spectrum. |
| **Overlay** | Any additional covering including a fake keypad, placed by fraudsters on top of a genuine PIN entry keypad and generally similar in shape and color, The placement of an overlay may also serve the purpose of concealing other attacks. |
| **PAN** | Acronym for "primary account number" and also referred to as "account number." Payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. |
| **Password** | A string of characters used to authenticate an identity or to verify access authorization. |

| Term | Definition |
|---|---|
| **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. |
| **PIN Entry Device (PED)** | A complete terminal that can be provided to a merchant "as is" to undertake PIN-related transactions. This may include either attended or unattended POS POI terminals. |
| **Plaintext** | The intelligible form of an encrypted text or of its elements. |
| **Plaintext Key** | An unencrypted cryptographic key, used in its current form. |
| **Point of Interaction (POI)** | An electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in an acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC and/or magnetic-stripe card-based payment transactions. |
| **POS POI Terminal** | A general description of any terminal used to perform a card-based payment transaction. This may or may not require a PIN to confirm cardholder authentication. |
| **Private Key** | A cryptographic key, used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public.<br>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. |
| **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.<br>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.<br><br>A system based on asymmetric cryptographic techniques can be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system.<br><br>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 transformations are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and, where used, the four elementary transformations and the corresponding keys should be kept separate. See *Asymmetric Cryptographic Algorithm.* |
| **Random** | The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware-based "noise" mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable. |
| **RNG** | Random number generator |
| **ROM** | Read-only memory |
| **RSA Public Key Cryptography** | Public-key cryptosystem that can be used for both encryption and authentication. |
| **Salt** | 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 (Secret) Share* |

| Term | Definition |
|---|---|
| **Secure Components (for POI Terminals)** | Products which incorporate security mechanisms for PIN and account data handling and processing, and require integration into a complete terminal, such as OEM PIN entry devices and IC card readers. |
| **Secure Controller** | A secure microprocessor or security protected microprocessor within the terminal, used to manage cardholder data amongst other functions. |
| **Secure Cryptographic Device** | A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms. |
| **Secure Cryptoprocessor** | A secure cryptoprocessor is a dedicated computer on a chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures that give it a degree of tamper resistance. |
| **Secure Key Loader** | A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module. |
| **Security Policy** | A description of how the specific module meets these security requirements, including the rules derived from this standard and additional rules imposed by the vendor. |
| **Sensitive Authentication Data** | Security-related information (card validation codes/values, full track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. |
| **Sensitive (Secret) Data (Information)** | Sensitive data includes but is not restricted to the cardholder PIN, all secret keying material, design characteristics, status information, and other functions that allow access to secure areas within the terminal. |
| **Sensitive Functions** | Sensitive functions are those functions that process sensitive data such as cryptographic keys and PINs. |
| **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. |
| **Service Module** | A module providing for non-cardholder activities and oriented towards service or maintenance related functions and may consist of:<br>▪ A service keyboard (SK),<br>▪ A service display (SD), and<br>A service data exchange support (SDE), which may consist of a card reader, a floppy disk drive, a USB interface or the like. |

| 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. |
| **Single-Length Key** | A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm. |
| **SK** | Session key |
| **Split Knowledge** | A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. |
| **SSL** | Secure Sockets Layer |
| **Surrogate PAN** | A unique, non-PCI relevant replacement value for a PAN. It must not be possible (except by chance) to recover the original PAN knowing only the surrogate value. |
| **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. Because merchants and cardholders are not trained to identify tamper-evidence and it is not expected that there will be frequent inspections by a trained inspector, any tamper evidence must be very strong. The typical uninformed cardholder and merchant must be able to easily recognize that the device has been tampered with. |
| **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.* |
| **Terminal Vendor** | Organization that submits for evaluation a POI device to the PCI PTS framework. |

| 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. |
| **Truncation** | Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. |
| **Unattended Payment Terminal (UPT)** | A POS POI device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as:<br>▪ Automated fuel dispensers<br>▪ Kiosks<br>▪ Self-service devices – ticketing/vending or car parking terminals |
| **Unprotected Memory** | Data retained within components, devices, and recording media that reside outside the cryptographic boundary of a secure cryptographic device. |
| **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. |
| **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.* |
| **Zeroize** | The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data. |