Payment Card Industry (PCI)

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

Modular Security Requirements

Version 6.1

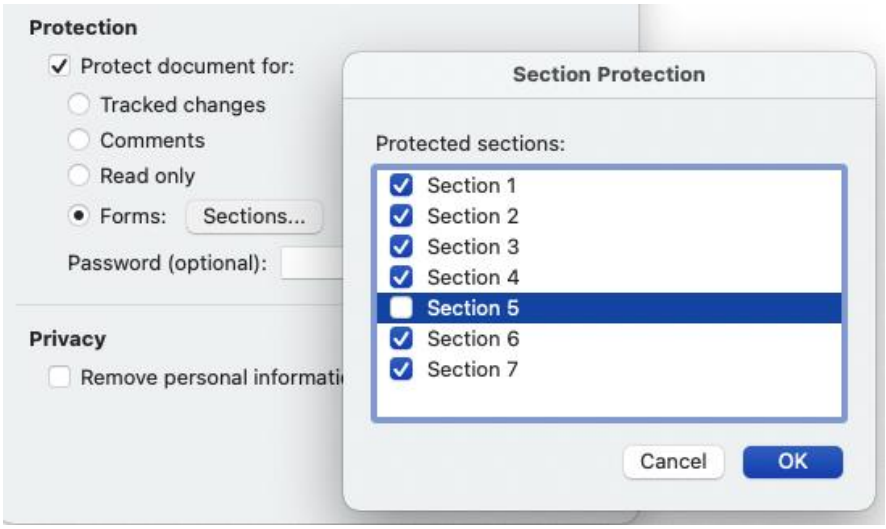
March 2022

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
July 2015	4.1a	Updates for errata and new core section J.
September 2015	4.1b	Updates for Device Management and Section J
November 2015	4.1c	Appendix A errata
June 2016	5.x	RFC Version
September 2016	5.0	Public release
March 2018	5.1	Modified D1 and Appendix B and added K24 for new SCRP approval class. Errata.
August 2019	6.x	Created new module structure
June 2020	6.0	Public Release
March 2022	6.1	Added requirement for unauthenticated wireless communications.

Note to Assessors

When protecting this document for use as a form, leave Section 5 (Device Photos) unprotected to allow for insertion of a device or component photos. Under “Tools / Protect Document,” select “Forms” then “Sections,” and un-check Section 5 as illustrated below.



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.

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 (EPPs) that require integration into POS terminals or ATMs.

  Note: *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, secure (encrypting) card readers (SCRs), and secure card readers – PIN (SCRPs).

Appendix B, "Applicability of Requirements," details which requirements apply based upon functionality.

This version 6 additionally provides for:

- The restructuring of the modules into:
  - Physical
  - Logical
  - Integration
  - Communications and Interfaces
  - Life Cycle
- The addition of new appendices in the Derived Test Requirements for:
  - Domain-Based Asset Flow Analysis
  - Evaluation Guidance for CPUs
- The migration of technical FAQs into either the Derived Test Requirements or the *Device Testing and Approval Program Guide.*

Scope of the Document

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

- Product samples
- Technical support documentation

Upon successful compliance testing by the laboratory and approval by the PCI SSC, the PCI PTS 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:

- Restructured modules into Physical, Logical, Communications and Interfaces, and Life Cycle while retaining the Integration Module.
- POI v6 firmware expires three years from the date of approval but shall not expire past the overall approval expiration of the device.
- POI v6 chipsets must provide support for ECC.
- Eliminated Removal Detection Requirements.
- Split requirement A1 into two separate requirements: 1) Tamper Detection Mechanisms 2) Protection of Sensitive Keypad Inputs.
- Split requirement A6 into two separate requirements: 1) Invasive Attacks for Cryptographic Keys 2) Non-invasive Attacks for Cryptographic Keys.
- Allow the inclusion of MSRs in SCRPs for use in SPoC solutions.
- Added tracking of Key Management for Account Data Encryption.

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 relative to attack potential. Virtually any physical barrier can be defeated with sufficient time and effort. Therefore, many of the requirements have minimum attack calculation values for the identification and initial exploitation of the device based upon factors such as attack time, expertise, and equipment required. Given the evolution of attack techniques and technology, PCI will periodically review these amounts for appropriateness.

Life Cycle

Life cycle 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 life cycle for POI devices up to the point of initial key loading for payment transaction keys (keys used by the acquiring organization) or at the facility of initial deployment. Subsequent to receipt of the device at the initial key-loading facility or at the facility of initial deployment, the responsibility for the device falls to the acquiring financial institution and its agents—e.g., merchants and processors—and is covered by the operating rules of the Participating 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.
- In modular approvals, where a PIN entry device may be approved taking in consideration previously approved components.
- In offering evaluation modules (modular evaluation packages) that potentially optimize both evaluation costs and time when laboratories review 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 document.

Publication Title	Reference
Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	ANSI X9.42
Key Establishment Using Integer Factorization Cryptography	ANSI X9.44
Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography	ANSI X9.63
Symmetric Key Cryptography for the Financial Services Industry – Wrapping of Keys and Associated Data	ANSI X9.102
Retail Financial Services – Requirements for Protection of Sensitive Payment Card Data Part 1: Using Encryption Methods	ANSI X9.119-1
Retail Financial Services – Requirements for Protection of Sensitive Payment Card Data – Part 2: Using Tokenization Methods	ANSI X9.119-2
Public Key Cryptography: The Elliptical Curve Digital Signature Algorithm (ECDSA)	ANSI X9.142
Retail Financial Services – Interoperable Secure Key Block Specification	ANSI X9.143
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ASC X9 TR 31
Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport	ASC X9 TR 34
Integrated Circuit Card Specification for Payment Systems – Book 2: Security and Key Management, Version 4.3, November 2011	EMV 4.3
Digital Signature Standard (DSS)	*FIPS PUB 186-5*
Identification Cards – Integrated Circuit Cards	ISO 7816
Personal Identification Number (PIN) Management and Security	ISO 9564
Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher	ISO 9797-1
Financial Services – Key Management (Retail)	ISO 11568
Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques	ISO 11770-2
Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers	ISO 11770-3

Publication Title	Reference
Financial Services – Secure Cryptographic Devices (Retail)	ISO 13491
Financial services – Requirements for message authentication using symmetric techniques	ISO 16609
Information Technology – Security techniques – Encryption algorithms – Part 1: General	ISO/IEC 18033-1
Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers	ISO/IEC 18033-3
Information Technology – Security techniques – Encryption algorithms – Part 5: Identity Based Ciphers	ISO/IEC 18033-5
Guidelines on Triple DES Modes of Operation	ISO TR 19038
Banking and related financial services – Key wrap using AES	ISO 20038
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 Block Cipher Modes of Operation: The CMAC Mode for Authentication	NIST SP 800-38B
Recommendation for Key Management, Part 1: General	NIST SP 800-57
Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	NIST SP 800-67
Recommendation for Random Number Generation Using Deterministic Random Bit Generators	NIST SP 800-90A Revision 1
Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	NIST SP 800-131A Revision 2
Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters	NIST SP 800-186
Payment Card Industry (PCI) Data Security Standard (DSS)	PCI SSC
Payment Card Industry (PCI) Data Security Standard Wireless Guidelines	PCI SSC
Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements	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.

<table>
<tr><th colspan="27">Device Details</th></tr>
<tr><td rowspan="6">Device type claim</td><td colspan="26">POS terminal containing a PIN entry device (select one):
☐ Dedicated for PIN entry only ☐ UPT (Vending, AFD, Kiosk)
☐ Stand-alone POS terminal ☐ Other</td></tr>
<tr><td colspan="26">☐ Encrypting PIN pad (for ATM, Vending, AFD, or Kiosk)</td></tr>
<tr><td colspan="26">☐ Secure (encrypting) card reader</td></tr>
<tr><td colspan="26">☐ Secure (encrypting) card reader PIN</td></tr>
<tr><td colspan="26">☐ Non-PED POI device</td></tr>
<tr><td colspan="26">☐ Other secure component for PIN entry device</td></tr>
<tr><td>Manufacturer*:</td><td colspan="12"></td><td colspan="2">Marketing Model Name/Number*:</td><td colspan="12"></td></tr>
<tr><td rowspan="3">Hardware Version Number*[A]:
Use of “x” represents a request for field to be a variable.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
<tr><td colspan="26">Additional versions:</td></tr>
<tr><td rowspan="3">Firmware/Software Version Number*:
Use of “x” represents a request for field to be a variable.</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
<tr><td colspan="26">Additional versions:</td></tr>
<tr><td>Application Version Number*: (if applicable)</td><td colspan="26"></td></tr>
<tr><td>Version of PCI PTS POI Security Requirements:</td><td colspan="11">v6</td><td colspan="3">FAQ version:</td><td colspan="12"></td></tr>
</table>

* 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,” page 8.

Device Details (continued)				
Validation modules required (where applicable, please see Evaluation Module Groupings):		**Yes**	**No**	**N/A**
	Physical	☐	☐	☐
	Logical	☐	☐	☐
	Integration	☐	☐	☐
	Communications and Interfaces	☐	☐	☐
	Life Cycle	Always Applicable:		

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**

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 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 Physical and Logical Security 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 – PIN Encryption**	☐	N/A (explain)
		☐	TDES – DUKPT
		☐	TDES – MK/SK
		☐	AES – DUKPT
		☐	AES – MK/SK
*	**Key Management – Account Data Encryption**	☐	N/A (explain)
		☐	TDES – DUKPT
		☐	TDES – MK/SK
		☐	AES – DUKPT
		☐	AES – MK/SK
		☐	Format-Preserving Encryption
*	**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 – 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 Requirements

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 to support business needs of vendors, requirements were grouped into 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: Physical and Logical Requirements	Physical and Logical Security	The logical and physical requirements of 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. 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. 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.
3: Communications and Interfaces	All Protocols and all interfaces on the device	A set of requirements that ensures POI devices using communication protocols and interfaces are secure, including determination that those using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities.
4: Life Cycle	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.

An "N/A" response to a requirement is acceptable in two cases:

First, if compliance is achieved by meeting another requirement option, if one exists.

Second, if the characteristics governed by the requirement are absent in the device. The evaluation laboratory will verify that all responses are appropriate.

Evaluation Module 1: Physical and Logical Requirements

A – 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 results 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.	☐	☐	☐
A2	There is no demonstrable way to disable or defeat the tamper mechanism/s and insert a sensitive key-press-disclosing bug. Keypads used for PIN entry require an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation, exclusive of the IC card reader, as defined in Appendix B. Keypads used for manual PAN entry, but not PIN entry—e.g., a non-PED—require an attack potential of at least 16 per device for identification, with a minimum of 8 points for initial exploitation.[B]	☐	☐	☐
A3	The security of the device is not compromised by altering: ▪ Environmental conditions ▪ Operational conditions *(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 unauthorized modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation, exclusive of the IC card reader, for identification and initial exploitation.[B]	☐	☐	☐

[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 initial exploitation.[C]	☐	☐	☐
A6	Determination of any PIN-security-related secret or private cryptographic keys resident in the device by penetration of the device requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for initial exploitation, as defined in Appendix B. Determination of any account-data-security-related secret or private cryptographic keys resident in the device by penetration of the device requires an attack potential of at least 26 points for identification and initial exploitation with a minimum of 13 for initial exploitation.[C]	☐	☐	☐
A7	Emanations from the device (including power fluctuations) cannot be feasibly used to recover PIN and/or SRED security-related cryptographic keys resident in the 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: A8, B15, or C2.4.* ▪ *A8 applies to any components or paths containing clear-text display signals between the cryptographic processor and display unit.* ▪ *B15 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.* ▪ *C2.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *If numerical key input is enabled, the display prompts should be controlled by the cryptographic processor.*			
A8	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 initial exploitation.[C]	☐	☐	☐
A9	The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.	☐	☐	☐

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

Number	Description of Requirement	Yes	No	N/A
A10	The device protects all account data upon entry for magnetic stripe or contactless data, and there is no method of accessing the clear-text account data to determine or modify the 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 initial exploitation.[D] ***Note:*** *Contact chip is addressed in A13. Manual PAN entry is addressed in A2.*	☐	☐	☐
A11	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.	☐	☐	☐
A12	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 from the input component to the secure controller of the device—i.e., it is not possible to insert a bug that would disclose sensitive data.	☐	☐	☐
A13	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 initial exploitation,[D] nor is it possible for both an IC card and any other foreign object to reside within the card-insertion slot. SCRPs shall require an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation.[D]	☐	☐	☐
A14	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. 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.	☐	☐	☐

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

B – 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 must support firmware updates. The device must cryptographically authenticate the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted. The update mechanism ensures security—i.e., integrity, mutual authentication, and protection against replay—by using an appropriate and declared security protocol when using a network connection.	☐	☐	☐
B2.1	The firmware must support the authentication of applications loaded onto the terminal consistent with B2.	☐	☐	☐
B2.2	The vendor must provide a defined and documented process containing specific details on how any signing mechanisms must be implemented. This must include any "turnkey" systems required for compliance with the management of display prompts, or any mechanisms used for authenticating any application code. This must ensure: ▪ The signing process is performed under dual control. ▪ All executable files are signed. ▪ Software is only signed using a secure cryptographic device—e.g., smartcard—provided by the terminal vendor.	☐	☐	☐
B3	The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols—e.g., asterisks. 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.	☐	☐	☐
B4	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. The device must automatically clear its internal buffers of full track data (or chip equivalent) and sensitive authentication data is cleared when either: ▪ The transaction is completed, or ▪ The device has timed out waiting for the response from the cardholder or merchant.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
B5	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords/authentication codes. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	☐	☐	☐
B6	To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit shall be imposed, after which the device is forced to return to its normal mode.	☐	☐	☐
B7	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.	☐	☐	☐
B8	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.	☐	☐	☐
B9	The key-management techniques implemented in the device conform to *ISO 11568* and/or *ANSI X9.24.* Key-management techniques must support key blocks as defined in DTR B9.	☐	☐	☐
B10	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.	☐	☐	☐
B11	The PIN-encryption technique implemented in the device is a technique included in *ISO 9564.*	☐	☐	☐
B12	It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key, account data encryption, data-encrypting key, or key-encrypting key contained in the device. The device must enforce that PIN encryption, account data encryption, data-encryption keys, and key-encipherment keys have different values.	☐	☐	☐
B13	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.	☐	☐	☐
B14	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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
	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: A8, B15, or C2.4.* ▪ *A8 applies to any components or paths containing clear-text display signals between the cryptographic processor and display unit.* ▪ *B15 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.* ▪ *C2.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *If numerical key input is enabled, the display prompts should be controlled by the cryptographic processor.*			
B15	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device. 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.	☐	☐	☐
B16	If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the device including, but not limited to, modifying data objects belonging to either another application or the OS.	☐	☐	☐
B16.1	If the device supports software with lesser security requirements or that is not developed by the vendor—e.g., applications—it must enforce segregation at least between different software security domains.	☐	☐	☐
B16.2	The vendor must provide clear security guidance consistent with D1 and B4 to all application developers to ensure: ▪ That it is not possible for applications to be influenced by logical anomalies which could result in clear-text data being outputted while the terminal is in encrypting mode. ▪ That account data is not retained any longer, or used more often, than strictly necessary. ▪ That SRED functions, where provided, are correctly implemented.	☐	☐	☐
B17	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.	☐	☐	☐
B18	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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
B19	The vendor must provide adequate documented security guidance for the integration of any secure component into a 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.	☐	☐	☐
B21	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: ▪ 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. ▪ A clear-text 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 clear text to the IC card) in accordance with ISO 9564. 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: ▪ An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card. ▪ A clear-text PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the clear-text PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.	☐	☐	☐
B22	If the device can 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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
Secure Reading and Exchange of Data				
B23	When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data except as described in DTR B23. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.	☐	☐	☐
B23.1	When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device.	☐	☐	☐
B24	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. Where a hash function is used to generate surrogate PAN values: ▪ Input to the hash function must use a salt with minimum length of 64 bits. ▪ 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 initial exploitation, as defined in Appendix B.	☐	☐	☐
B25	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.	☐	☐	☐
B26	Secure enablement tokens are required from the SPoC monitor system for operation of the SCRP.	☐	☐	☐

Evaluation Module 2: POS Terminal integration

C – 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
	Integration of PIN Entry Functions			
C1.1	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.	☐	☐	☐
C1.2	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. An overlay attack must require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for initial exploitation[E].	☐	☐	☐
	Integration into a POS Terminal			
C2.1	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.	☐	☐	☐
C2.2	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.	☐	☐	☐

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

Number	Description of Requirement	Yes	No	N/A
C2.3	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: A8, B15, or C2.4.* ▪ *A8 applies to any components or paths containing clear-text display signals between the cryptographic processor and display unit.* ▪ *B15 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.* ▪ *C2.4 is appropriate for unattended devices that do not meet any of the aforementioned.* *If numerical key input is enabled, the display prompts should be controlled by the cryptographic processor.*			
C2.4	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. 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. 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 initial exploitation[F].	☐	☐	☐
C2.5	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 B15.	☐	☐	☐

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

Evaluation Module 3: Communications and Interfaces

D – Communications and Interfaces

Number	Description of Requirement	Yes	No	N/A
D1	All protocols and all interfaces available on the device are accurately identified by the device vendor. The vendor has a complete and comprehensive understanding of how all protocols and interfaces present on the device interact. A**ll** public domain protocols and interfaces available on the device are clearly identified in the *Open Protocols – Protocol Declaration Form*.	☐	☐	☐
D2	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.	☐	☐	☐
D3	The device has security guidance that describes how protocols and services must be used for each interface that is accessible by the device applications.	☐	☐	☐
D4	The device has guidance that describes the default configuration for each protocol and services for each interface that is available on the device. Each interface and protocol on the device should be configured with secure default settings.	☐	☐	☐
D5	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 application developers, system integrators, and end-users of the device. b) Key-management security guidance describes the properties of all keys and certificates that can be used by the device. c) Key-management security guidance describes the responsibilities of the device vendor, application developers, system integrators, and end-users of the device. d) Key-management security guidance ensures secure use of keys and certificates, including certificate status —e.g., revoked —secure download, and roll-over of keys.	☐	☐	☐
D6	The device has all the security protocols that are available on the device clearly identified in the *Open Protocols – Protocol Declaration Form*. The device vendor provides documentation that describes the implementation and use of the security protocols that are available on the device.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
D7	As defined in the asset flow diagrams, 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 in the Federal Government* and *ISO 11568 Banking – Key Management (Retail).*	☐	☐	☐
D8	As defined in the asset flow diagrams, 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 E of the *PCI PTS POI DTRs.*	☐	☐	☐
D9	As defined in the asset flow diagrams, 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 device is able to verify the validity of the public keys it receives. d) The device is able to verify the authenticity of the public keys it receives. e) The device's trusted root certificate store shall contain only public key certificates from trusted CAs or else self-signed certificates verified by the acquirer.	☐	☐	☐
D10	As defined in the asset flow diagrams, the device is able to detect replay of messages and enables the secure handling of the exceptions.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
D11	As defined in the asset flow diagrams, the device implements session management. a) The device keeps track of all connections and restricts the number of sessions that can remain active on the device to the minimum necessary number. b) The device sets time limits for sessions and ensures that sessions are not left open longer than necessary.	☐	☐	☐
D12	Bluetooth communications must be secured against eavesdropping and man-in-the-middle attacks. ***Note:*** *If Bluetooth is used, D14 may alternatively be used.*	☐	☐	☐
D13	Wi-Fi communications must be securely configured. Protocols with known vulnerabilities must be disabled. ***Note:*** *If Wi-Fi is used, D14 may alternatively be used.*	☐	☐	☐
D14	Wireless communication interfaces which do not have specific security requirements, or have not met those requirements as listed, must be physically or cryptographically isolated. ***Note:*** *Where the security requirements in D12 and/or D13 for Bluetooth or Wi-Fi are not met, D14 must be met.*	☐	☐	☐

Evaluation Module 4: Life Cycle Security Requirements

E – During Manufacturing

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

The device manufacturer, subject to Participating Payment Brand site inspections, confirms the following. The PCI test laboratories will validate this information via documentation reviews, and by means of evidence that procedures are properly implemented and used. This information shall be included in the evaluation report to PCI.

Number	Description of Requirement	Yes	No	N/A
E1	Change-control procedures are in place so that any intended change to the physical or functional capabilities of the POI causes a re-certification of the device under the impacted security requirements of this document. Re-certification is not required for changes that purely rectify errors and faults in software in order to make it function as intended and do not otherwise remove, modify, or add functionality that impacts security. Approval of delta submissions is contingent on evidence of the ongoing change control and vulnerability management process.	☐	☐	☐
E2	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.	☐	☐	☐
E3	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.	☐	☐	☐
E4	The device is assembled in a manner that the hardware components used in the manufacturing process are those hardware components that were certified by the PIN Entry and/or POS Terminal Integration Security Requirements evaluation, and that unauthorized substitutions have not been made.	☐	☐	☐
E5	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.	☐	☐	☐
E6	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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
E7	The device must be authenticated at the key-loading facility or the facility of initial deployment by means of secret information placed in the device during manufacturing. This secret information is unique to each device, unknown and unpredictable to any person, and installed in the device. Secret information is installed under dual control to ensure that it is not disclosed during installation, or the device may use an authenticated public-key method. Authentication by secret information is mandatory in POI v6.	☐	☐	☐
E8	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.	☐	☐	☐
E9	Controls exist over the repair process at all POI vendor-authorized repair facilities, including the resetting of tamper mechanisms and the inspection/testing process subsequent to repair, to ensure that the device has not been subject to unauthorized modification.	☐	☐	☐
E10	The device vendor has internal policies and procedures that ensure the vendor maintains an effective process for detecting vulnerabilities that may exist within its device. This process is expected to be robust enough to include all interfaces defined in Requirement D1 and to detect vulnerabilities which may have not been publicly known during the last vulnerability assessment.	☐	☐	☐
E11	The device has undergone a vulnerability assessment to ensure that the protocols and interfaces list in D1 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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
E12	The device 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.	☐	☐	☐

F – 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 Participating Payment Brand site inspections, confirms the following. The PCI test laboratories will validate this information via documentation reviews and by means of evidence that procedures are properly implemented and used and that this information shall be included in the evaluation report to PCI.

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

Number	Description of Requirement	Yes	No	N/A
F1	The POI should be protected from unauthorized modification with tamper-detection security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI. 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 enroute under auditable controls that can account for the location of every POI at every point in time—such as the use of serialized tamper-evident packing for all devices with no tamper detection, in conjunction with thorough physical inspection (possibly including sampling of HW internals) upon reception. 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. In the absence of defined agreements stipulating otherwise, the POI vendor remains responsible.	☐	☐	☐
F2	Procedures are in place to transfer accountability for the device from the manufacturer to the facility of initial deployment. Where the device is shipped via intermediaries such as resellers, accountability will be with the intermediary from the time at which they receive the device until the time it is received by the next intermediary or the point of initial deployment. In the absence of defined agreements stipulating otherwise, the POI vendor remains responsible.	☐	☐	☐
F3	While in transit from the manufacturer's facility to the initial key-loading facility, the device is shipped and stored containing a secret that: ▪ Is immediately and automatically erased if any physical or functional alteration to the device is attempted, and ▪ Can be verified by the initial key-loading facility but cannot feasibly be determined by unauthorized personnel.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
F4	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.	☐	☐	☐
F5	If the manufacturer is in charge of initial key loading, the manufacturer must verify the authenticity of the POI security-related components.	☐	☐	☐
F6	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.	☐	☐	☐
F7	Each device shall have a unique visible identifier—i.e., model name and hardware version—affixed to it. This information shall also be retrievable by a query.	☐	☐	☐
F8	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, for example: ▪ Data on production and personalization ▪ Physical/chronological whereabouts ▪ Repair and maintenance ▪ Removal from operation ▪ Loss or theft	☐	☐	☐

Compliance Declaration – General Information – Form A

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

Device Manufacturer Information			
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	
Device Manufacturer:	
Model Name and Number:	

I, *(Name)*

☐ Am an officer of the above company, authorized to verify compliance of the referenced equipment.

☐ Am an officer of the designated laboratory, authorized by the manufacturer to verify compliance of the referenced equipment.

I hereby attest that the above-referenced model of PIN entry device is:

☐ In full compliance with the standards set forth above in this document.

☐ Not in full compliance with the standards set forth above in this document as indicated in the attached Exception Form (*Form C*).

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

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. Eight 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). The tamper-detection mechanisms must protect all PIN digits.
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 contactless, magnetic-stripe, and smart card readers. This is further broken down into CTLS, 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.
Device is a module	If the device under evaluation is designed to be integrated into equipment, it applies for “terminal is a module” functionality. Modules are also referred to as OEM equipment.
Device 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.
Implements Open Protocols	A device under evaluation implements a TCP/IP stack and associated open protocols.
Protects Account Data	Secures account data in accordance with the Secure Reading and Exchange of Data (SRED).

Appendix B: Applicability of Requirements

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

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

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

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

In addition to other applicable requirements, devices implementing open protocols—e.g., Bluetooth, Wi-Fi and TLS—must be validated against the requirements noted in *Implements Open Protocols*. Devices implementing SRED must be validated against the requirements in *Protects Account Data.*

The SCRP column is used as an example of applicability for a specific POI approval class. In general, requirements applicable to SCRP are the same as SCR. However, by definition SCRPs will always handle the PIN, and those requirements will always be applicable, whereas an SCR will not necessarily handle the PIN.

SCRP includes all Physical and Logical requirements except those specific to PIN entry, display prompt control, and unattended usage.

This delineation is the expected applicability but should not be regarded as definitive. In all cases, device functionality determines applicability of requirements.

Note:

1. *In order to receive the "Open Protocols" designation devices must meet all applicable requirements in the Implements Open Protocols column.*
2. *In order to receive the "SRED" designation devices must meet all applicable requirements in the Protects Account Data column.*

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Device is a module	Device is compound	Implements Open Protocols	Protects account data	SCRP	Conditions/Comments
Physical and Logical Requirements Modules											
Physical Security Requirements											
A1	X	X	X	X					X	X	Tamper Detection
A2	X								X		Sensitive Keypad Inputs
A3	X	X							X	X	Environmental/Operational Conditions
A4	X	X							X	X	Sensitive Functions/Information Protection
A5	X										Monitoring During PIN Entry
A6		X							X	X	Invasive Attacks – Determining Keys Analysis – For SCRP applicable whenever reader handles PINs, either offline or online, and has clear-text secret or private PIN-security-related cryptographic keys resident in the device.
A7		X							X	X	Non-Invasive Attacks – Determining Keys Analysis – For SCRP applicable whenever reader handles PINs, either offline or online, and has clear-text secret or private PIN-security-related cryptographic keys resident in the device.
A8					X						Physical Security of Display Prompts – If keypad can be used to enter non-PIN data.
A9	X										Visual Observation Deterrents
A10				X					X	X	Magnetic-Stripe and/or CTLS Reader
A11									X	X	Account Data Processing
A12									X	X	Card Reader Integration
A13			X							X	ICC Reader Penetration Protection
A14			X							X	ICC Reader Construction

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Device is a module	Device is compound	Implements Open Protocols	Protects account data	SCRP	Conditions/Comments
Logical Security Requirements											
B1	X	X						X	X	X	Self-Test
B2	X	X							X	X	Firmware Updates
B2.1	X	X							X	X	Application Authentication
B2.2	X	X							X	X	Signing Mechanism
B3	X										Differentiation of Entered PIN including audible tones
B4	X								X	X	Clearing Internal Buffers
B5	X	X							X	X	Protecting Sensitive Services
B6	X	X							X	X	Sensitive Service Limits
B7		X						X	X	X	Random Numbers
B8	X										Exhaustive PIN Determination
B9		X							X	X	Key Management
B10									X	X	Account Data Encryption
B11	X									X	PIN Blocks
B12		X							X	X	Arbitrary Data
B13	X	X								X	Output Clear text
B14	X										Transaction Controls
B15					X						Logical Management of Display Prompts – If keypad can be used to enter non-PIN data.
B16	X								X	X	Application Separation
B16.1	X								X	X	Software Security Domains
B16.2	X								X	X	Application Development
B17	X								X	X	OS Configuration
B18		X									Key Substitution
B19			X	X		X					Component Integration Documentation
B20	X	X	X	X	X	X	X	X	X	X	Security Policy
B21			X							X	PIN Protection During Transmission

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Device is a module	Device is compound	Implements Open Protocols	Protects account data	SCRP	Conditions/Comments
Logical Security Requirements *(continued)*											
B22									X	X	Remote Access
B23									X	X	Output of Clear-text Account Data
B23.1									X	X	Protection of Clear-text Account Data
B24									X	X	Surrogate PANs
B25									X	X	PAN Determination
B26										X	Secure Tokens
POS Terminal Integration Requirements											
C1.1	X						X				Integration of PIN Entry Functions
C1.2	X						X				Overlay Attacks
C2.1							X				Integration Vulnerabilities
C2.2			X			X	X				Card Trapping
C2.3	X						X				Interface Segregation
C2.4	X				X		X				If keypad can be used to enter non-PIN data.
C2.5	X						X				Numeric Interface
Communications and Interfaces											
D1								X		X	Interface Identification
D2	X	X							X	X	Logical Anomalies
D3								X		X	Security Guidance
D4								X		X	Default Configuration
D5								X		X	Key-Mgt. Security Guidance
D6								X		X	Secure Protocols
D7								X		X	Data Confidentiality
D8								X		X	Date Integrity
D9								X		X	Mutual Authentication
D10								X		X	Exception Handling and Replay Protection

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Device is a module	Device is compound	Implements Open Protocols	Protects account data	SCRP	Conditions/Comments
Communications and Interfaces *(continued)*											
D11								X		X	Session Management
D12								X		X	Bluetooth
D13								X		X	Wi-Fi
D14								X			Interface Isolation
Life Cycle Security Requirements											
During Manufacturing											
E1	X	X	X	X	X	X	X	X	X	X	Change Control
E2	X	X	X	X	X	X	X	X	X	X	Firmware Certification
E3	X	X	X	X	X	X	X	X	X	X	Certified Firmware Control
E4	X	X	X	X	X	X	X	X	X	X	Component Control
E5	X	X	X	X	X	X	X	X	X	X	Production Firmware Control
E6	X	X	X	X	X	X	X	X	X	X	Post-Production Storage
E7	X	X	X	X	X	X	X	X	X	X	Secret Information
E8	X	X	X	X	X	X	X	X	X	X	Design and Development
E9	X	X	X	X	X	X	X	X	X	X	Repair and Inspection
E10	X	X	X	X	X	X	X	X	X	X	Vulnerability Assessment Procedures
E11	X	X	X	X	X	X	X	X	X	X	Vulnerability Assessment Interfaces
E12	X	X	X	X	X	X	X	X	X	X	Vulnerability Disclosure
Between Manufacturer and Initial Key Loading											
F1	X	X	X	X	X	X	X		X	X	Tamper Protection Documentation
F2	X	X	X	X	X	X	X		X	X	Transfer Procedures
F3	X	X	X	X	X	X	X		X	X	Shipping Security
F4	X	X	X	X	X	X	X		X	X	Development Security
F5	X	X	X	X	X	X	X		X	X	Component Authenticity
F6	X	X	X	X	X	X	X		X	X	Component Authenticity – Key-Loading Facility

Requirement	PIN Entry	Keys	ICCR	MSR	Feedback to cardholder	Device is a module	Device is compound	Implements Open Protocols	Protects account data	SCRP	Conditions/Comments
Between Manufacturer and Initial Key Loading *(continued)*											
F7	X	X	X	X	X	X	X		X	X	Unique Identifier
F8	X	X	X	X	X	X	X		X	X	Operational Management

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. ***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 (with the exception of prompt control and SRED applications).
Authentication	The process for establishing unambiguously the identity of an entity, process, organization, or person.
Authentication code	See *Password.*
Authorization	The right granted to a user to access an object, resource, or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource, or function.
Check Value	A computed value which is the result of passing a data value through a non-reversible algorithm. A value used to identify a key without revealing any bits of the actual key itself. TDEA must support its use, and AES shall only use a technique where the KCV is calculated by MACing an all-zero block using the CMAC algorithm as specified in *ISO 9797-1* (see also *NIST SP 800-38B*). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MAC'd using the TDEA block cipher, while a 128-bit/192-bit/256-bit AES key or component will be MAC'd using the AES-128 block cipher. Optionally, the following method may be used for TDEA where the check values are computed by encrypting an all-zero block using the key or component as the encryption key, using the leftmost n-bits of the result, where n is at most 24 bits (6 hexadecimal digits/3 bytes).

Term	Definition
Ciphertext	An encrypted message.
Clear text	The intelligible form of an encrypted text or of its elements.
Clear-text Key	An unencrypted cryptographic key used in its current form.
Commercial off-the-shelf (COTS)	A mobile device—e.g., smartphone or tablet—that is designed for mass-market distribution and is not designed specifically for payment processing.
Compromise	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including clear-text cryptographic keys and other keying material).
Cryptographic Key Component (Key Component)	One of at least two parameters having the characteristics—e.g., format, randomness—of a cryptographic key that is combined with one or more like parameters—e.g., 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.

Term	Definition
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
Encipher	See Encrypt.
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext—i.e., the process of transforming clear text 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 clear-text 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. 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 subsets of requirements. Other code that exists within the device that does not provide security and cannot impact security—with the exception of prompt control and SRED applications—is not considered firmware.

Term	Definition
Format-preserving Encryption (FPE)	Format-preserving encryption encrypts a clear text of some specified format into ciphertext of the same format.
Hash	A (mathematical) function, which is a non-secret algorithm that takes any arbitrary-length message as input and produces a fixed-length hash result. Approved hash functions satisfy the following properties: 1) One-way: It is computationally infeasible to find any input that maps to any pre-specified output. 2) Collision-resistant: It is computationally infeasible to find any two distinct inputs—e.g., messages—that map to the same output. It may be used to reduce a potentially long message into a "hash value" or "message digest" 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.
Independent Expert	An Independent Expert possesses all the following qualifications: ▪ Holds one or more professional credentials applicable to the field—e.g., doctoral-level qualifications in a relevant discipline or government certification in cryptography by an authoritative body—e.g., NSA. ▪ Has published extensively in peer-reviewed publications on the relevant subject. ▪ Has years of experience in the relevant subject. ▪ Is recognized by his/her peers in the field—e.g., awarded the Fellow or Distinguished Fellow or similar professional recognition by an appropriate body—e.g., ACM, BCS, IEEE, IET, IACR. ▪ Subscribes to an ethical code of conduct and would be subject to an ethics compliance process if warranted. Independence requires that the entity is not subject to control, restriction, modification, or limitation from a given outside source. Specifically, independence requires that a person, firm, or corporation who holds itself out for employment as a cryptologist or similar expert to more than one client company is not a regular employee of that company, does not work exclusively for one company, and where paid, is paid in each case assigned for time consumed and expenses incurred.
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.

Term	Definition
ISO	International Organization for Standardization. An international standard-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.
Key Deletion	Process by which an unwanted key, as well as information from which the key may be reconstructed, is destroyed at its operational storage/use location.
Key-distribution Host (KDH)	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to the EPP or PED and the financial-transaction processing platform communicating with those EPPs/PEDs. A KDH may be an application that operates on the same platform that is used for PIN translation and financial-transaction processing. The KDH may be used in conjunction with other processing activities. A KDH shall not be used for certificate issuance and must not be used for the storage of CA private keys.
Key-encrypting (encipherment or exchange) Key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys.
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, clear-text key, key components, and enciphered key.
Key Loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.

Term	Definition
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
Key Variant	A new TDEA key formed by a reversible process (which need not be secret) with the original TDEA key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Least Privilege	In information security, computer science, and other fields, the principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.
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.

Term	Definition
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).
Monitoring System	Monitors and provisions security controls to detect, alert, and mitigate suspected or actual threats and attacks against the SCRP, PIN CVM Application, and the COTS device.
Monitor Token	A cryptographically signed value provided by the monitoring system to the SCRP and cryptographically authenticated by the SCRP to enable its operation for a period not to exceed ten minutes. The value and its usage must have properties—e.g., time/date stamps—that ensure the prevention of replay, pre-calculation, or other attacks to allow improper continued operation or re-enablement of the SCRP.
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.
Participating Payment Brand	A payment card brand that, as of the time in question, is formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of this publication, Participating Payment Brands include PCI SSC’s Founding Members and Strategic Members.
Password	A string of characters used to authenticate an identity or to verify access authorization.
Personal Identification Number (PIN)	A numeric personal identification code that authenticates a cardholder in an authorization request that originates at a terminal with authorization only or data capture only capability. A PIN consists only of decimal digits.

Term	Definition
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.
Point of Interaction (POI)	An electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions include Integrated Circuit (IC) and magnetic-stripe contact cards, and contactless payment 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. 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. In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Term	Definition
Public Key (Asymmetric) Cryptography	A cryptographic technique that uses two related transformations—a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques, such as RSA, there are four elementary transformations: sign and verify for signature systems and encipher and decipher for encipherment systems. The signature and the decipherment 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
SCRP	Secure Card Reader PIN. An approval class as defined in the *PTS POI Device Testing and Approval Guide*
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 among 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 clear-text or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
Security Policy	A description of how the specific module meets these security requirements, including the rules derived from this standard as well as 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 clear text 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.
Service Module	A module providing for non-cardholder activities and oriented towards service or maintenance related functions and may consist of: ▪ A service keyboard (SK), ▪ A service display (SD), and ▪ 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
Session Key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys—e.g., an encryption key and a MAC key.
SHA-1	Secure Hash Algorithm. SHA-1 produces a 160-bit message digest.
SHA-2	A set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512). SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.
Shared Secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key-derivation function to derive session keys.
Single-Length Key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
SK	Session key
Split Knowledge	A condition under which two or more entities separately have information—e.g., key components—that individually convey no knowledge of the resultant combined information—e.g., a cryptographic key.
SPoC	Software-based PIN Entry on Commercial off-the-shelf (COTS) Devices. A payment solution that encompasses the set of components and processes that support the entry of PIN data into a COTS device. At a minimum, this includes a SCRP, PIN CVM Application, and the back-end systems and environments that perform attestation, monitoring, and payment and online PIN processing.
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.

Term	Definition
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.
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.
Unique Accountability	Actions are attributable to a specific person or role.
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: ▪ Automated fuel dispensers ▪ Kiosks ▪ 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	See *Key Variant.*
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.