



Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI)

Modular Security Requirements

Version 3.1

October 2011

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

Table of Contents

Document Changes	1
About This Document.....	4
Purpose.....	4
Scope of the Document	4
Main Differences from Previous Version	5
Process Flow for PTS Approval	6
Foreword	7
Evaluation Domains.....	7
Device Management.....	7
Modular approach	7
Related Publications.....	8
Device and Vendor Information	9
Required Information	9
Optional Use of Variables in the Identifier	10
Evaluation Module Information	11
POS Terminal Integration and Core Requirements Modules	11
Open Protocols Module – Protocol Declaration Form	12
Secure Reading and Exchange of Data Module	13
Evaluation Module Groupings.....	14
Evaluation Module 1: Core Requirements.....	15
A – Core Physical Security Requirements	15
B – Core Logical Security Requirements	18
C – Online PIN Security Requirement	21
D – Offline PIN Security Requirements.....	21
Evaluation Module 2: POS Terminal integration	23
E – POS Terminal Integration Security Requirements	23
Evaluation Module 3: Open Protocols	25
F – IP and Link Layer (IPLL).....	25
G – IP Protocols (IPP)	26
H – Security Protocols (IPSP).....	27
I – IP Services (IPSV).....	29
J – Security Management Compliance Requirements	31
Evaluation Module 4: Secure Reading and Exchange of Data (SRED).....	33
Account Data Protection	33
Evaluation Module 5: Device Management Security Requirements	37
L – During Manufacturing	37
M – Between Manufacturer and Initial Key Loading	39

Compliance Declaration – General Information – Form A.....	40
Compliance Declaration Statement – Form B	41
Compliance Declaration Exception – Form C	42
Appendix A: Requirements Applicability Matrix	43
Appendix B: Applicability of Requirements	44
Glossary	48

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

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

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

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

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

Scope of the Document

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

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

Upon successful compliance testing by the laboratory and approval by the PCI SSC, the PCI PTS POI device (or a secure component) will be listed on the PCI SSC website. Commercial information to be included in the Council's approval must be provided by the vendor to the test laboratory using the forms in the “Evaluation Module Information” section of this document.

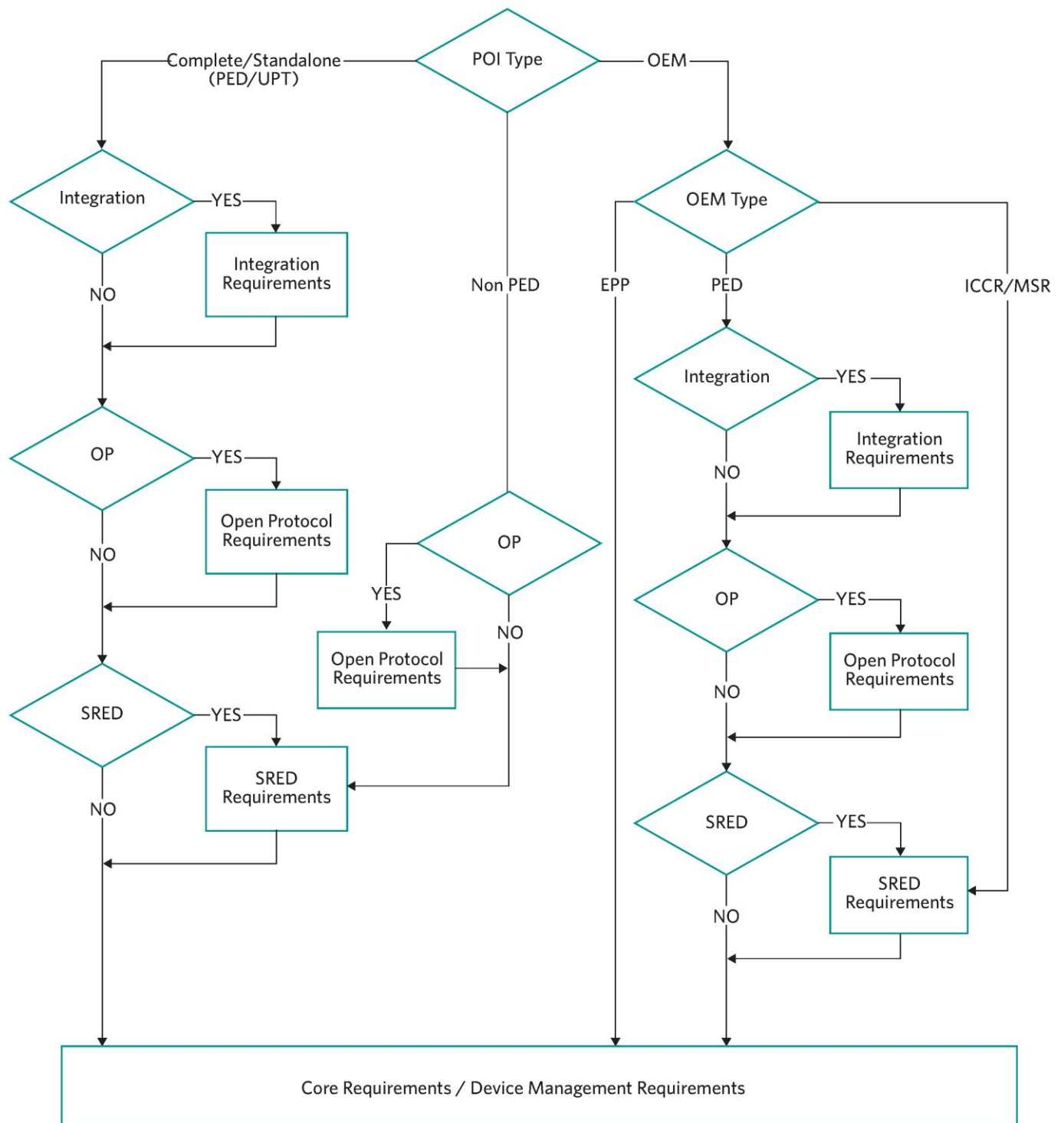
Main Differences from Previous Version

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

- A single evaluation to address the diversity of POI device architectures and integration models (dedicated PIN pads, dedicated stand-alone POS devices, vending machines, kiosks, etc.)
- The segmentation of requirements into two main evaluation modules (Device Integration Requirements and POI Device Core Requirements) to facilitate components integration and evaluation maintenance
- The addition of the following set of requirements and corresponding evaluation modules
 - Open Protocols (To address the interface of POI terminals to open networks using open protocols)
 - Secure Reading and Exchange of Data (Optional: To support secure encryption of account data in the terminal)
- The addition of non-PIN acceptance devices and secure (encrypting) card readers as approval classes.
- The collection of vendor/product information to be displayed on *PCI SSC Approved PIN Transaction Security Devices Approval List*

PTS Approval Modules Selection

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



Foreword

The requirements set forth in this document are the minimum acceptable criteria for the Payment Card Industry (PCI). The PCI has defined these requirements using a risk-reduction methodology that identifies the associated benefit when measured against acceptable costs to design and manufacture POI devices. Thus, the requirements are not intended to eliminate the possibility of fraud, but to reduce its likelihood and limit its consequences.

Evaluation Domains

Device characteristics are those attributes of the device that define its physical and its logical (functional) characteristics. The physical security characteristics of the device are those attributes that deter a physical attack on the device, for example, the penetration of the device to determine its key(s) or to plant a sensitive data-disclosing “bug” within it. Logical security characteristics include those functional capabilities that preclude, for example, allowing the device to output a clear-text PIN-encryption key.

The evaluation of physical security characteristics is very much a value judgment. Virtually any physical barrier can be defeated with sufficient time and effort. Therefore, many of the requirements have minimum attack calculation values for the identification and initial exploitation of the device based upon factors such as attack time, and expertise and equipment required. Given the evolution of attack techniques and technology, the Associations will periodically review these amounts for appropriateness.

Device Management

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

This document is only concerned with the device management for POI devices up to the point of initial key loading. Subsequent to receipt of the device at the initial key-loading facility, the responsibility for the device falls to the acquiring financial institution and its agents (e.g., merchants and processors), and is covered by the operating rules of the participating PCI payment brands and the *PCI PIN Security Requirements*.

Modular approach

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

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

Related Publications

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

<i>Banking – Retail Financial Services Symmetric Key Management</i>	ANSI X9.24
<i>Triple Data Encryption Algorithm (TDEA) Implementation</i>	ANSI X9.65
<i>Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms</i>	ANSI TR-31
<i>Identification Cards – Integrated Circuit Cards</i>	ISO 7816
<i>Personal Identification Number (PIN) Management and Security</i>	ISO 9564
<i>Banking – Key Management (Retail)</i>	ISO 11568
<i>Banking – Secure Cryptographic Devices (Retail)</i>	ISO 13491
<i>Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers</i>	ISO/IEC 18033-3
<i>Guidelines on Triple DES Modes of Operation.</i>	ISO TR 19038
<i>Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008 – Book 2: Security and Key Management</i>	EMV 4.2
<i>PCI DSS v1.2.1</i>	PCI SSC
<i>PCI DSS Wireless Guidelines</i>	PCI SSC
<i>PCI PTS POI Evaluation Vendor Questionnaire</i>	PCI SSC

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

Device and Vendor Information

Required Information

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

Device type claim	POS terminal containing a PIN entry device (select one):																								
	<input type="checkbox"/> Dedicated PIN pad												<input type="checkbox"/> Vending, AFD, Kiosk												
	<input type="checkbox"/> Stand-alone POS terminal												<input type="checkbox"/> Other												
	<input type="checkbox"/> Encrypting PIN pad (for ATM Vending, AFD or Kiosk)																								
	<input type="checkbox"/> Secure component for PIN entry device																								
<input type="checkbox"/> Non-PED POI device																									
<input type="checkbox"/> Secure (encrypting) card reader																									
Manufacturer*:												Marketing Model Name/Number*:													
Hardware Version Number*^A: Use of "x" represents a request for field to be a variable																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Firmware/Software Version Number*:													Application Version Number*: (if applicable)												
Version of PCI PTS POI Security Requirements:	V3												FAQ version:												
Device or component photo* (If applicable):	Please attach a photo of the terminal under evaluation, 320x320 pixels.																								
Validation modules required (where applicable, please see Section C – Selection of Evaluation Modules):																			Yes	No	N/A				
	POS terminal Integration																		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	Core PIN Entry Security																		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	Open Protocols																		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
	Secure Reading and Exchange of Data																		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Other																									
Previously Approved Components Used* (if applicable)																									
Summary Description/Function	Vendor Name					Marketing Name					PCI PTS Approval Number					Expiry Date					FAQ Version (if applicable)				

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

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

Optional Use of Variables in the Identifier

Hardware Version Number – Request for Use of the Variable “x”

Note: The firmware version number may also be subject to the use of variables in a manner consistent with hardware version numbers. See the PCI PTS POI Testing and Approval Program Guide for more information.

Variable “x” Position	Description of Variable “x” in the Selected Position

Evaluation Module Information

POS Terminal Integration and Core Requirements Modules

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

*	PIN Support	<input type="checkbox"/>	N/A (explain)
		<input type="checkbox"/>	Offline only
		<input type="checkbox"/>	Offline and Online
		<input type="checkbox"/>	Online only
*	Key Management	<input type="checkbox"/>	N/A (explain)
		<input type="checkbox"/>	DUKPT
		<input type="checkbox"/>	Fixed
		<input type="checkbox"/>	MK/SK
*	PIN Entry Technology	<input type="checkbox"/>	N/A (explain)
		<input type="checkbox"/>	Physical (Hard) Keys
		<input type="checkbox"/>	Touch screen
		<input type="checkbox"/>	Other
*	Prompt Control	<input type="checkbox"/>	N/A (explain)
		<input type="checkbox"/>	Acquirer-controlled
		<input type="checkbox"/>	Terminal manufacturer-controlled
		<input type="checkbox"/>	Other (explain)
*	Summary Description to be displayed on the <i>PCI SSC Approved PIN Transaction Security Devices List</i> (maximum 120 characters)		

Open Protocols Module – Protocol Declaration Form

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

	Link Layer Protocols	<input type="checkbox"/>	Yes
		<input type="checkbox"/>	No
		<input type="checkbox"/>	N/A
		Name	
	IP Protocols	<input type="checkbox"/>	Yes
		<input type="checkbox"/>	No
		<input type="checkbox"/>	N/A
		Name	
		Number	
	Security Protocols	<input type="checkbox"/>	Yes
		<input type="checkbox"/>	No
		<input type="checkbox"/>	N/A
		Name	
	IP Services	<input type="checkbox"/>	Yes
		<input type="checkbox"/>	No
		<input type="checkbox"/>	N/A
		Name	
		Port Number	
*	Summary Description to be displayed on the <i>PCI SSC Approved PIN Transaction Security Devices List</i> (maximum 120 characters)		

Secure Reading and Exchange of Data Module

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

	Does the terminal utilize secure reading and exchange of data?	<input type="checkbox"/>	Yes
		<input type="checkbox"/>	No
		<input type="checkbox"/>	N/A (explain)
*	Summary Description to be displayed on the <i>PCI SSC Approved PIN Transaction Security Devices List</i> (maximum 120 characters)		

Evaluation Module Groupings

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

Evaluation Module	Requirements Set	Remarks
1: Core Requirements	Physical and logical Security	The core logical and physical requirements of PIN-acceptance POI devices
2: POS Terminal Integration	POS Terminal Integration	<p>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).</p> <p>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.</p> <p>The POS Terminal integration Evaluation Module ensures that the integration of previously approved components does not impair the overall security as stated in security requirements. This module also supports the cost-effective maintenance of components.</p> <p>This module includes security management requirements applicable to the integrated device.</p>
3: Open Protocols	Open Protocols	A set of requirements that ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities.
4: Secure Reading and Exchange of Data	Requirements in support of cardholder account data encryption	A set of requirements that ensures cardholder data is protected.
5: Device Management	Device Management (Manufacturing and initial key loading)	Life cycle requirements for POIs and their components up until the point of initial key loading. The information is not currently validated, but is still required for vendors to complete.

Evaluation Module 1: Core Requirements

A – Core Physical Security Requirements

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

Number	Description of Requirement	Yes	No	N/A
A1	All parts of A1 must be met if A1 is applicable:			
A1.1	<p>The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanism and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader^B; and</p> <p><i>Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario.</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A1.2	Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A2	If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose sensitive data. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A3	<p>The security of the device is not compromised by altering:</p> <ul style="list-style-type: none"> ▪ Environmental conditions ▪ Operational conditions <p><i>(An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)</i></p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A4	Sensitive functions or data are only used in the protected area(s) of the device. Sensitive data and functions dealing with sensitive data are protected from modification without requiring an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation, exclusive of the IC card reader, for identification and initial exploitation ^B .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Number	Description of Requirement	Yes	No	N/A
A5	If PIN entry is accompanied by audible tones, then the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A6	There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring—even with the cooperation of the device operator or sales clerk—without requiring an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation ^C .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A7	Determination of any PIN-security-related cryptographic key resident in the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation ^C .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>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, B16.1, B16.2, or E3.4.</p> <p>(Statements A8 and B16.1 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement B16.2 is an option that allows third parties to control the means of authorization. E3.4 is for all other unattended POI devices not meeting one of the aforementioned.)</p>				
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 exploitation ^C .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A9	The device provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A10	It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 16 per device, for identification and initial exploitation, with a minimum of 8 for exploitation ^C .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A11	Secure components intended for unattended devices contain an anti-removal mechanism to protect against unauthorized removal and/or unauthorized re-installation. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation ^C .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

B – Core Logical Security Requirements

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

Number	Description of Requirement	Yes	No	N/A
B1	The device performs a self-test, which includes integrity and authenticity tests as addressed in B4, upon start-up and at least once per day to check firmware, security mechanisms for signs of tampering, and whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B2	The device’s functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the device outputting the clear-text PIN or other sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B3	The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B4	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B5	The device never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B6	Sensitive data shall not be retained any longer, or used more often, than strictly necessary. Online PINs are encrypted within the device immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button. The device must automatically clear its internal buffers when either: <ul style="list-style-type: none"> ▪ The transaction is completed, or ▪ The device has timed out waiting for the response from the cardholder or merchant. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B7	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B8	To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit imposed, after which the device is forced to return to its normal mode.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B9	If random numbers are generated by the device in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B10	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B11	The key-management techniques implemented in the device conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support the ANSI TR-31 key derivation methodology or an equivalent methodology for maintaining the TDEA key bundle.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number	Description of Requirement	Yes	No	N/A
B12	The PIN-encryption technique implemented in the device is a technique included in ISO 9564.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B13	It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the device. The device must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B14	There is no mechanism in the device that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B15	The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the device display. If other data and the PIN are entered on the same keypad, the other data entry and the PIN entry shall be clearly separate operations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>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, B16.1, B16.2, or E3.4. (Statements A8 and B16.1 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement B16.2 is an option that allows third parties to control the means of authorization. E3.4 is for all other unattended POI devices not meeting one of the aforementioned.)</p>				
B16.1	All prompts for non-PIN data entry are under the control of the cryptographic unit of the device and requiring an attack potential of at least 18 per device for identification and initial exploitation with a minimum of 9 for exploitation ^D to circumvent. If the prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts is prevented.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B16.2	Cryptographically based controls are utilized to control the device display and device usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the device. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key-management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Number	Description of Requirement	Yes	No	N/A
B17	If the device supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers with another application or the OS of the device, including modifying data objects belonging to another application.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

B18	The operating system of the device must contain only the software (components and services) necessary for the intended operation. The operating system must be configured securely and run with least privilege.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B19	The vendor must provide adequate documented security guidance for the integration of any secure component into a PIN entry POI Terminal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

C – Online PIN Security Requirement

Number	Description of Requirement	Yes	No	N/A
C1	If the device can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the device prohibits unauthorized key replacement and key misuse.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

D – Offline PIN Security Requirements

Number	Description of Requirement	Yes	No	N/A
D1	It is neither feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 20 for identification and initial exploitation, with a minimum of 10 for exploitation ^E , nor is it possible for both an ICC card and any other foreign object to reside within the card insertion slot. <i>Note: The card reader may consist of areas of different protection levels, e.g., the areas of the ICC card interface itself, and the area holding retracted cards.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D2	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D3	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D4	PIN protection during transmission between the device encrypting the PIN and the ICC Reader (at least two must apply):			
D4.1	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. ^F	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

^F When the cardholder verification method is determined to be an enciphered PIN, the encipherment must occur within the PED itself or a secure component of the terminal. The PIN must be enciphered in accordance with ISO 9564 for secure transport between the PED and the secure component.

Number	Description of Requirement	Yes	No	N/A
D4.2	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 a plain-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 plain-text to the IC card) in accordance with ISO 9564. ^G	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D4.3	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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D4.4	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 a plain-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 plain-text PIN is transmitted to the ICC reader through an unprotected environment, then the PIN block shall be enciphered in accordance with ISO 9564.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

^G A plain-text PIN from the PED to the ICC reader is never permitted except when the PED and ICC reader are integrated in a single tamper-resistant device (secure module).

Evaluation Module 2: POS Terminal integration

E – POS Terminal Integration Security Requirements

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

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

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

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

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

Number	Description of Requirement	Yes	No	N/A
Configuration Management				
E1	Any secure component integrated into a PIN entry POI terminal submitted for evaluation has a clearly identified physical and logical security perimeter (related to PIN entry and card-reading functions).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Integration of PIN Entry Functions				
E2.1	The logical and physical integration of a PCI-approved secure component (or components) into a PIN entry POI terminal must not impact the overall PIN protection level.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E2.2	The PIN pad (PIN entry area) and the surrounding area must be designed and engineered in such a way that the complete device does not facilitate the fraudulent placement of an overlay over the PIN pad. An overlay attack must require an attack potential of at least 18 for identification and initial exploitation, with a minimum of 9 for exploitation ^H .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Integration into a POS Terminal				
E3.1	The logical and physical integration of an approved secure component into a PIN entry POI terminal does not create new attack paths to the PIN.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E3.2	The PIN entry POI terminal is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E3.3	There is a clear logical and/or physical segregation between secure components and non-secure components integrated into the same device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Number	Description of Requirement	Yes	No	N/A
<p>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, B16.1, B16.2, or E3.4.</p> <p>(Statements A8 and B16.1 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement B16.2 is an option that allows third parties to control the means of authorization. E3.4 is for all unattended POS or other POI devices not meeting one of the aforementioned.)</p>				
E3.4	<p>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.</p> <p>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.</p> <p>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 exploitation¹.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E3.5	<p>The PIN-accepting POI terminal must be equipped with only one payment card PIN-acceptance interface, e.g., a keyboard. If another interface is present which can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry, e.g., it must not have numeric keys, or it is not possible to use it otherwise for numeric entry or it is controlled in a manner consistent with B16.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Removal Requirements

E4.1	The device is protected against unauthorized removal. Defeating or circumventing this mechanism must require an attack potential of at least 18 per device for identification and initial exploitation, with a minimum of 9 for exploitation ¹ .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E4.2	The vendor documents, maintains and makes available to integrators details on how to implement the protection system against unauthorized removal.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E4.3	For each embedded device, the protection system against unauthorized removal is properly implemented as documented by the embedded device manufacturer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

¹ As defined in Appendix B of the *PCI PTS POI DTRs*.

Evaluation Module 3: Open Protocols

F – IP and Link Layer (IPLL)

The vendor must complete the Security Compliance Statements concerning the IP and link layer.

This table must be completed considering the IP and link layer **in its entirety**. Answer “Yes” if **all** the options declared in the [Open Protocols Module – Protocol Declaration Form](#) are meet these security requirements.

Number	Description of Requirement	Yes	No	N/A
F1	The platform vendor has clearly identified all the link layer options that are available on the platform in the <i>Open Protocols Module –Protocol Declaration Form</i> .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F2	The platform vendor has executed a vulnerability assessment, to ensure that the IP and link layer do not contain exploitable vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The vulnerability assessment is supported by a documented analysis describing the security of the IP and link layer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The vulnerability assessment is supported by a vulnerability survey of information available in the public domain.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The vulnerability assessment is supported by testing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F3	The platform vendor maintains security guidance, describing how the IP and link layer must be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the security guidance at the disposal of application developers, system integrators, and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security guidance ensures secure use of the IP and link layer.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
F4	The default configuration of the IP and link layer is in line with the security guidance. If the device allows configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

G – IP Protocols (IPP)

The vendor must complete the Security Compliance Statements concerning the IP protocols.

This table must be completed considering the IP protocols **in their entirety**. Answer “Yes” if **all** the options declared in the [Open Protocols Module – Protocol Declaration Form](#) meet these security requirements.

Number	Description of Requirement	Yes	No	N/A
G1	The platform vendor has clearly identified all the IP protocols that are available on the platform in the <i>Open Protocols Module – Protocol Declaration Form</i> .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G2	The platform vendor has executed a vulnerability assessment, to ensure that the IP protocols do not contain exploitable vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The vulnerability assessment is supported by a documented analysis describing the security of the IP protocols.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The vulnerability assessment is supported by a vulnerability survey of information available in the public domain.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The vulnerability assessment is supported by testing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G3	The platform vendor maintains security guidance, describing how the IP protocols have to be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the security guidance at the disposal of application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security guidance ensures secure use of the IP protocols.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G4	The default configuration of the IP protocols is in line with the security guidance. If the device allows configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

H – Security Protocols (IPSP)

The vendor must complete the Security Compliance Statements concerning the security protocols (such as SSL/TLS, IPSec, PPTP, proprietary protocols, etc.).

Table H1 must be completed considering the security protocols **in their entirety**. Answer “Yes” if **all** the security protocols declared in the [Open Protocols Module – Protocol Declaration Form](#) meet these security requirements.

Table H1: Security Protocol in its Entirety

Number	Description of Requirement	Yes	No	N/A
H1	The platform vendor has clearly identified all the security protocols that are available on the platform in the <i>Open Protocols Module – Protocol Declaration Form</i> .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H2	The platform vendor has executed a vulnerability assessment, to ensure that the security protocols do not contain exploitable vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The vulnerability assessment is supported by a documented analysis describing why the vendor is convinced of the security protocols not jeopardizing platform security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The vulnerability assessment is supported by a vulnerability survey of information available in the public domain.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The vulnerability assessment is supported by testing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H3	The platform vendor maintains security guidance, describing how the IP protocols have to be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the security guidance at the disposal of application developers, system integrators, and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security guidance ensures secure use of the IP protocols.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The security guidance clearly mentions whether specific security protocols must not be used for financial applications and/or platform management.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) The security guidance clearly mentions whether specific configurations of security protocols must not be used for financial applications and/or platform management.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H4	The default configuration of the security protocols is in line with the security guidance. If the device allows configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table H2 **must be duplicated and completed for each** of the security protocols that might be used by financial applications or for device management functions.

Answer “Yes” if the security protocol **specified in the table** meets the security requirement.

Table H2: Specified Security Protocol

Security Protocol Name:				
Number	Description of Requirement	Yes	No	N/A
H5	The platform vendor maintains key management security guidance, describing how keys and certificates have to be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the key management security guidance at the disposal of internal users, and/or of application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) Key management security guidance describes the properties of all keys and certificates that can be used by the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) Key management security guidance describes the responsibilities of the platform vendor, application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) Key management security guidance ensures secure use of keys and certificates.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H6	The security protocol is able to provide the confidentiality of data sent over a network connection.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) Encryption mechanism utilizes key sizes appropriate for the algorithm(s) in question.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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, <i>Guidelines for Implementing Cryptography</i> .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H7	The security protocol is able to provide the integrity of data that is sent over a network connection.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) Integrity is provided by a MAC or by a digital signature.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) Hashing can be provided by at least one of the following algorithms: SHA-224, SHA-256, SHA-384 and SHA-512.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H8	The security protocol is able to authenticate the server.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) Server authentication utilizes key sizes appropriate for the algorithm(s) in question.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The platform is able to verify the validity of the public keys it receives.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The platform is able to verify the authenticity of the public keys it receives.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H9	The security protocol is able to detect replay of messages, and enables the secure handling of the exception.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
H10	The security protocol makes use of a random generator that has been validated against NIST SP 800-22 or equivalent.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

I – IP Services (IPSV)

The vendor must complete the Security Compliance Statements concerning the IP services (such as DNS, DHCP, HTTP, FTP, etc.).

Table I1 must be completed considering the IP services **in their entirety**. Answer “Yes” if **all** the IP services declared in the [Open Protocols Module – Protocol Declaration Form](#) meet the security requirement.

Table I1: IP Services in their Entirety

Number	Description of Requirement	Yes	No	N/A
I1	The platform vendor has clearly identified all the IP services that are available on the platform in the <i>Open Protocols Module – Protocol Declaration Form</i> .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I2	The platform vendor has executed a vulnerability assessment, to ensure that the IP services do not contain exploitable vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The assessment is supported by a documented analysis describing why the vendor is convinced of the IP services not jeopardizing platform security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The assessment is supported by a vulnerability survey of information available in the public domain.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The assessment is supported by testing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I3	The platform vendor maintains security guidance, describing how the IP services have to be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the security guidance at the disposal of application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security guidance ensures secure use of the IP services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The security guidance clearly mentions whether specific IP services must not be used for financial applications and/or platform management.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) The security guidance clearly mentions whether specific configurations of IP services must not be used for financial applications and/or platform management.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I4	The default configuration of the IP services is in line with the security guidance. If the device allows configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I5	The platform implements session management.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform keeps track of all connections and restricts the number of sessions that can remain active on the platform to the minimum necessary number.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The platform sets time limits for sessions and ensures that sessions are not left open for longer than necessary.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table I2 **must be repeated and completed** for each of the IP services that might be used by financial applications or for terminal management functions.

Answer “Yes” if the IP Service **specified in the table** meets the security requirement.

Table I2: Specified IP Service

IP Service:				
Number	Description of Requirement	Yes	No	N/A
I6	The IP Service is able to ensure confidentiality, integrity, server authentication and protection against replay by using an appropriate, and declared, security protocol.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

J – Security Management Compliance Requirements

Number	Description of Requirement	Yes	No	N/A
J1	The platform vendor maintains security guidance, describing configuration management measures for the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The platform vendor puts the security guidance at the disposal of internal users, and/or of application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security guidance covers the complete platform; including firmware, applications, certificates and keys.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The security guidance covers the complete life cycle of the platform from development, over manufacturing, up to delivery and operation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) The security guidance ensures that unauthorized modification is not possible.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	e) The security guidance ensures that any modification of a PTS-approved platform that impacts platform security, results in a change of the platform identifier.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
J2	The platform vendor has put in place security maintenance measures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The security maintenance measures are documented.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The security maintenance measures ensure timely detection of vulnerabilities that apply to the device by periodical execution of a vulnerability assessment that includes activities such as: analysis, survey of information available in the public domain, and testing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The security maintenance measures ensure timely assessment and classification of newly found vulnerabilities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) The security maintenance measures ensure timely creation of mitigation measures for newly found vulnerabilities that may impact platform security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
J3	The platform vendor has put in place vulnerability disclosure measures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The vulnerability disclosure measures are documented.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The vulnerability disclosure measures ensure a timely distribution of mitigation measures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number	Description of Requirement	Yes	No	N/A
J4	Deployed platforms can be updated, and the platform vendor maintains security guidance describing how the update mechanism has to be used.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	a) The update mechanism ensures confidentiality, integrity, server authentication and protection against replay by using an appropriate, and declared, security protocol. If the device allows software and/or configuration updates, the device cryptographically authenticates the update and if the authenticity is not confirmed, the update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b) The platform vendor puts the security guidance for updating deployed platforms at the disposal of application builders, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	c) The security guidance covers the update of firmware, applications, certificates and keys.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	d) The security guidance describes the responsibilities of application developers, system integrators and end-users of the platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	e) The security guidance ensures that deployed platforms are timely and securely updated.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

This module defines requirements for cardholder account data protection.

Account Data Protection

Number	Description of Requirement	Yes	No	N/A
Generic Security Requirements				
K1	All account data is either encrypted immediately upon entry or entered in clear-text into a secure device and processed within the secure controller of the device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K1.1	The device protects all account data upon entry (consistent with A10 for magnetic stripe data and D1 for Chip data), and there is no method of accessing the clear-text account data (using methods described in A1) without defeating the security of the device. Defeating or circumventing the security mechanism requires an attack potential of at least 16 for identification and initial exploitation, with a minimum of 8 for exploitation ^J .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K2	The logical and physical integration of an approved secure card reader into a PIN entry POI terminal does not create new attack paths to the account data. The account data is protected (consistent with A2) from the input component to the secure controller of the device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K3	Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation ^J .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K3.1	Public keys must be stored and used in a manner that protects against unauthorized modification or substitution. Unauthorized modification or substitution requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation ^J .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K4	All account data shall be encrypted using only ANSI X9 or ISO-approved encryption algorithms (e.g., AES, TDES) and should use ANSI X9 or ISO-approved modes of operation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K5	If remote key distribution is used, the device supports mutual authentication between the sending key distribution host and receiving device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K6	The device supports data origin authentication of encrypted messages.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K7	Secret and private keys which reside within the device to support account data encryption are unique per device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

^J As defined in Appendix B of the *PCI PTS POI DTRs*.

Number	Description of Requirement	Yes	No	N/A
K8	Encryption or decryption of any arbitrary data using any account data-encrypting key or key-encrypting key contained in the device is not permitted. The device must enforce that account data keys, key-encipherment keys, and PIN-encryption keys have different values.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K9	If the device may be accessed remotely for the purposes of administration, all access attempts must be cryptographically authenticated. If the authenticity of the access request cannot be confirmed, the access request is denied.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K10	The firmware, and any changes thereafter, have been inspected and reviewed consistent with B3.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K11	The device performs self-tests consistent with B1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K11.1	The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K11.2	The vendor must provide clear security guidance consistent with B2 and B6 to all application developers to ensure: <ul style="list-style-type: none"> ▪ That it is not possible for applications to be influenced by logical anomalies which could result in clear text data being outputted whilst the terminal is in encrypting mode. ▪ That account data is not retained any longer, or used more often, than strictly necessary. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K12	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K13	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 clear-text account data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K14	The security requirements specified in sections H and J of the Open Protocols module have been met.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K15	If the device is capable of communicating over an IP network, the security requirements specified in sections F, G, and I of the Open Protocols module have been met.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K16	When operating in encrypting mode, there is no mechanism in the device that would allow the outputting of clear-text account data. Changing between an encrypting and non-encrypting mode of operation requires explicit authentication.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K16.1	When operating in encrypting mode, the secure controller can only release clear-text account data to authenticated applications executing within the device.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K16.2	Account data (in either clear-text or encrypted form) shall not be retained any longer, or used more often, than strictly necessary.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number	Description of Requirement	Yes	No	N/A
K17	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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K17.1	If using a hash function to generate surrogate PAN values, input to the hash function must use a salt with minimum length of 64-bits.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K17.2	If using a hash function to generate surrogate PAN values, the salt is kept secret and appropriately protected. Disclosure of the salt cannot occur without requiring an attack potential of at least 16 per device for identification and initial exploitation with a minimum of 8 for exploitation ^K .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K18	The key-management techniques implemented in the device are consistent with B11.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K19	The device has characteristics that prevent or significantly deter the use of the device for exhaustive PAN determination.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K20	If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose any secret or private keys or account data. Immediate access to secret or private keys or account data is either prevented by the design of the internal areas (e.g., by enclosing components with such data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of secret and private keys and account data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K21	Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data. (An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K22	If the device supports multiple applications, it must enforce the separation between applications consistent with B17.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K23	The following features of the device's operating system must be in place: <ul style="list-style-type: none"> ▪ 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. ▪ The security policy enforced by the device must not allow unauthorized or unnecessary functions. ▪ API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed). 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

^K As defined in Appendix B of the *PCI PTS POI DTRs*.

Number	Description of Requirement	Yes	No	N/A
K24	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
K25	Sensitive services are protected from unauthorized use consistent with B8.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Evaluation Module 5: Device Management Security Requirements

L – During Manufacturing

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

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

Number	Description of Requirement	Yes	No	N/A
L1	Change-control procedures are in place so that any intended security-relevant change to the physical or functional capabilities of the device causes a re-certification of the device under the Core PIN Entry and/or POS Terminal Integration Security Requirements of this document.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L2	The certified firmware is protected and stored in such a manner as to preclude unauthorized modification, e.g., using dual control or standardized cryptographic authentication procedures.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L3	The device is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Core PIN Entry and/or POS Terminal Integration Security Requirements evaluation, and that unauthorized substitutions have not been made.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L4	Production software 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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L5	Subsequent to production but prior to shipment from the manufacturer’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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L6	If the device will be authenticated at the key-loading facility by means of secret information placed in the device during manufacturing, then this secret information is unique to each device, unknown and unpredictable to any person, and installed in the device under dual control to ensure that it is not disclosed during installation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Number	Description of Requirement	Yes	No	N/A
L7	Security measures during 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.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
L8	Controls exist over the repair process and the inspection/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.			

M – Between Manufacturer and Initial Key Loading

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

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

Number	Description of Requirement	Yes	No	N/A
M1	The device is shipped from the manufacturer’s facility to the initial key-loading facility, and stored en route, under auditable controls that can account for the location of every PED at every point in time.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M2	Procedures are in place to transfer accountability for the device from the manufacturer to the initial key-loading facility.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M3	While in transit from the manufacturer’s facility to the initial key-loading facility, the device is: <ul style="list-style-type: none"> Shipped and stored in tamper-evident packaging; and/or Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M4	The development security documentation must provide means to the initial key-loading facility to assure the authenticity of the TOE security relevant components.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M5	If the manufacturer is in charge of initial key loading, then the manufacturer must verify the authenticity of the POI security-related components.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M6	If the manufacturer is not in charge of initial key loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M7	Each device shall have a unique visible identifier affixed to it.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
M8	The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire life cycle of the POI security-related components and of the manner in which those components are integrated into a single POI, e.g.: <ul style="list-style-type: none"> Data on production and personalization Physical/chronological whereabouts Repair and maintenance Removal from operation Loss or theft 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Compliance Declaration – General Information – Form A

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

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

Compliance Declaration Statement – Form B

Compliance Declaration	
Manufacturer:	
Model Name and Number:	
I, (Name)	
<input type="checkbox"/> Am an officer of the above company, authorized to verify compliance of the referenced equipment.	
<input type="checkbox"/> 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:	
<input type="checkbox"/> In full compliance with the standards set forth above in the Manufacturer Self-Assessment Form.	
<input type="checkbox"/> <u>Not</u> in full compliance with the standards set forth above in the Manufacturer Self-Assessment Form as indicated in the attached Exception Form (<i>Form C</i>).	
Signature ↑	Date ↑
Printed Name ↑	Title ↑

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

Appendix A: Requirements Applicability Matrix

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

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

Appendix B: Applicability of Requirements

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

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

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

1. Identify which of the functionalities the device supports.
2. For each of the supported functionalities, report any marking "x" from the functionality column to the baseline column. "x" stands for "applicable," in which case the requirement must be considered for vendor questionnaire and possibly evaluation.

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

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

Core Logical Security Requirements

B1	x	x								
B2	x	x								
B3	x	x								
B4	x	x								
B5	x									
B6	x									
B7	x	x								
B8	x	x								
B9		x								
B10	x									
B11		x								
B12	x	x								
B13		x								
B14	x	x								
B15	x									
B16					x					If keypad that can be used to enter non-PIN data.
B17	x									
B18	x									
B19			x	x		x				

Additional Online Requirement

C1		x								
----	--	---	--	--	--	--	--	--	--	--

Additional Offline Requirements

D1			x							
D2			x							
D3			x							
D4			x							

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

POS Terminal Integration Requirements

E1	x	x	x		x	x	x	x	x	Always applicable
E2.1	x						x			
E2.2	x						x			
E3.1							x			
E3.2			x			x	x			
E3.3	x						x			
E3.4	x				x		x			If keypad that can be used to enter non-PIN data.
E3.5	x						x			
E4.1	x		x			x				
E4.2	x		x			x				
E4.3							x			

Open Protocols Security Module

All								x		All requirements applicable
-----	--	--	--	--	--	--	--	---	--	-----------------------------

Secure Reading and Exchange of Data Module

All									x	All requirements applicable
K1			x	x					x	
K1.1			x	x					x	
K3			x	x					x	
K4			x	x					x	
K7			x	x					x	
K10			x	x					x	
K11			x	x					x	
K12			x	x					x	
K13			x	x					x	

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

Device Security Requirements

During Manufacturing

L1	x	x	x	x	x	x	x	x	x	
L2	x	x	x	x	x	x	x	x	x	
L3	x	x	x	x	x	x	x	x	x	
L4	x	x	x	x	x	x	x	x	x	
L5	x	x	x	x	x	x	x	x	x	
L6	x	x	x	x	x	x	x	x	x	
L7	x	x	x	x	x	x	x	x	x	
L8	x	x	x	x	x	x	x	x	x	

Between Manufacturing and Initial Key Loading

M1	x	x	x	x	x	x	x		x	
M2	x	x	x	x	x	x	x		x	
M3	x	x	x	x	x	x	x		x	
M4	x	x	x	x	x	x	x		x	
M5	x	x	x	x	x	x	x		x	
M6	x	x	x	x	x	x	x		x	
M7	x	x	x	x	x	x	x		x	
M8	x	x	x	x	x	x	x		x	

Glossary

Term	Definition
Account Data	At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code. Other transaction-relevant information may be included at the vendor's discretion. <i>Note: Encrypted, truncated, masked and hashed PAN data (with salt) may be outputted outside of the device.</i>
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.
Encrypting PIN Pad (EPP)	Encrypting PIN Pads which require integration into UPTs or ATMs
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	Any code within the device that provides security protections needed to comply with device security requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware.
Hashing	A (mathematical) function, which is a non-secret algorithm that takes any arbitrary length message as input and produces a fixed length hash result. It must have the property that it is computationally infeasible to discover two messages that produce the same hash result. It may be used to reduce a potentially long message into a "hash value" or "message digest". 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.
Key-encrypting (encipherment or exchange) key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys.
Key variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
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.
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.
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.

Term	Definition
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.
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 an acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions are IC and/or magnetic-stripe card-based payment transactions. For these requirements, a POI device is a PIN-acceptance device.
POS POI Terminal	A general description of any terminal used to perform a card-based payment transaction when a PIN is required to confirm cardholder 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.
Secure Components (for POI Terminals)	Products which incorporate security mechanisms for PIN and account data handling and processing, and require integration into a complete terminal, such as OEM PIN entry devices and IC card readers.
Secure Controller	A secure microprocessor or security protected microprocessor within the terminal, used to manage cardholder data amongst other functions.
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 plain-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: <ul style="list-style-type: none"> ▪ 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.
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.
Terminal Vendor	Organization that submits for evaluation a POI device to the PCI PTS framework.

Term	Definition
TOE	Target of Evaluation
Truncation	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data.
Unattended Payment Terminal (UPT)	<p>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:</p> <ul style="list-style-type: none">▪ Automated fuel dispensers▪ Kiosks▪ Self-service devices – ticketing/vending or car parking terminals