Payment Card Industry (PCI)

Unattended Payment Terminal (UPT)

Security Requirements

Version 1.0

April 2009

Document Changes

Date	Version	Description
January 2006	0.1	First Draft
February 2006	0.2	Modifications from 7 – 9 February 2006 review
March 2006	0.3	Errata
May 2006	0.4	Added A10, changed order to comply with POS PED 1.5
July 2006	0.5	Updates to replace cost with Attack potential, and include case replacement as part of A1.1 and reorder requirements to match with POS PED
October 2006	0.6	Alignment with the draft version 2.0 of the POS PED requirements
April 2007	0.7	Vendor Comments
May 2007	0.71	Alignment with the final 2.0 versions of the PCI POS PED and PCI EPP requirements
March 2008	0.72	▪ PCI SSC Template ▪ Added changes following first pilot
November 2008	0.75	PWG/Lab meeting changes
April 2009	1.0	Initial Release

In order to provide greater consistency with International Standards and to generalize the calculations, requirements that formerly were based on a dollar threshold for attacks have been converted to a point-based attack potential scheme.

Table of Contents

Overview

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

The requirements set forth in this document are divided into the following categories:

Device Characteristics:

- Physical Security Characteristics
- Logical Security Characteristics

Device Management:

- Device Management During Manufacturing
- Device Management Between Manufacturing and Initial Key Loading

UPTs must meet all applicable requirements. UPT vendors must have the specified device characteristics validated at independent test houses that are recognized by the participating PCI Associations. UPT vendors must also meet the device management requirements. The Associations reserve the right to have those requirements independently validated.

Device Characteristics

Device characteristics are those attributes of the UPT 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 PIN-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 device characteristics within this document are further subdivided into Core, Online, and Offline.

Core requirements are those that all UPTs must meet. Additional requirements for UPTs that support online PIN verification and/or offline PIN verification follow.

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 maximum 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 UPT 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 UPTs 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 their agents (e.g., merchants and processors) and is covered by the operating rules of the Associations and the PCI PIN Security Requirements.

Definitions and Scope

The primary focus of the PCI UPT requirements is the protection of the cardholders PIN. In a wider scope, the customer card data is included in the requirements aspects, to avoid or at least complicate the collection of PINs with the card data, as defined in several requirements concerning ICC and magnetic-stripe card readers.

The UPT is a cardholder-operated payment terminal that reads, captures and transmits card information in conjunction with an unattended self-service device, including, but not limited to, the following:

- Automated Fuel Dispenser
- Ticketing Machine
- Vending Machine

The scope of these requirements does not include UPTs that are not cardholder PIN acceptance devices; nor does it include ATMs, which are separately defined.

The UPT components and design properties of interest here are:

- The UPT cabinet (CAB): The CAB is the physical boundary of the UPT. It may be the complete machine or the smallest detachable cabinet or enclosure that includes all the UPT interface units defined below. The CAB restricts access to the UPT components. For practical reasons, the physical UPT may or may not include the part of the equipment that dispenses the product or provides the service. The scope of the CAB includes the front cover presenting the interface units to the cardholder, including any signs, pictograms and instructions visible to the cardholder. All interface functions through which the cardholder performs the tasks related to the card payment are considered interface units to be included in the physical UPT (CAB).

Note: depending on the architecture, the CAB may or may not bring additional security. It is up to the vendor and the evaluator to prove that if a given implementation requires the CAB to meet any of the security requirements. If the CAB is necessary to meet one or more security requirements, then it must be identified as part of the hardware version number.

- The PIN pad, realized as an Encrypting PIN Pad (EPP): The PIN pad contains an embedded cryptographic module, which performs the task of PIN encryption and key management. For convenience, the cryptographic module (CM) of the EPP often provides other cryptographic services like message encryption and message authentication.
- The customer card reader (CR): The UPT must be equipped with at least one type of card reader, a magnetic stripe reader (MSR) or an ICC reader (ICCR). CR may be a hybrid reader and possibly motorized. If the ICC reader supports clear offline PIN, and it is not integrated with the EPP into a physically secure boundary, it must be by itself physically secure and able to establish an encrypted communication to the EPP, and may therefore contain a cryptographic module (CM).

  Note: When the card reader is a hybrid reader, it shall be considered as both an ICC reader and magnetic stripe reader for all applicable requirements.
- The UPT customer display (DSP): The display is usually directly connected to the UPT controller, and is assumed in these requirements to be a passive device, which cannot authenticate the counterpart or decrypt message content. However, that may not always be the case.
- The UPT controller (UC): The UC may be integrated in the EPP or the CR, or it may be also be a separate module, possibly a PC operated by a standard operating system. In the latter case, the UC may contain a cryptographic module. As far as it is used for PIN (re-)encryption, it is considered here.

- Cryptographic module (CM) located in the UPT controller (optional): This CM is considered only if it is used for other services related to PIN handling and firmware. References to the CM in these requirements do not include CMs present in the EPP or ICCR. Where applicable, those are directly stated.
- The communication interface (CI): The interface to the authorization host or other background systems.

These are sketched in Figures 1 through 3 below. In addition, a service module may be added to the UPT, consisting 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.

The service interface components may be (partially) remote, in which case a proper protection for the link to the UPT is required.

Logical aspects to be considered are:

- The security properties of the communication protocol between the UPT components
- The security properties of the communication protocol to the Host system for Online PIN authentication
- The key loading method and interface
- Journaling and logging

These components will be addressed as far as they may be used for sensitive services, like key management, operation mode control or software configuration.

The PIN is handled in the clear by the keypad and the smart card reader (in the case of offline verification), which are usually slave components controlled by the UPT controller. The PIN security aspects are partially addressed by the PCI EPP requirements and the PCI PED requirements.

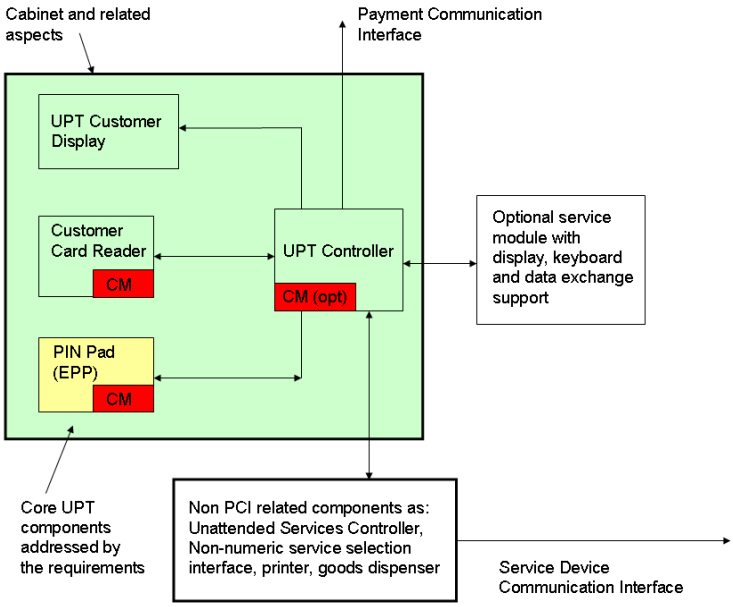
The UPT controller sets the operation modes of the EPP, the display and the card reader. The keypad entry mode of the EPP and the related display content is normally driven by the UPT controller, and any manipulation which aims at collecting PINs by modification of the relationship between display content and EPP keypad entry mode is addressed by the requirements on proper operation of the UPT controller.

Components that are not addressed by these requirements are the handling of goods and services provided by the unattended self-service device. The UPT may or may not include the interfaces used to place the order for products or services. However, if any of these interfaces exist that could be utilized for numerical input from the cardholder, it must be considered part of the UPT. Accordingly, if the UPT includes such an interface for numerical input - other than the PIN related to the card payment - all displays visible to the cardholder must be considered part of the UPT.

Figures 1 through 3 show different variants of an UPT integrated in an Unattended Self-Service Device (USSD) with the components mentioned above. These are only intended as examples of configurations and are not intended as an exhaustive list.

- Figure 1's design can be seen as an integrated POS PED type payment terminal placed into the (USSD) or even separate from the USSD.
- Figure 2 shows a single unit design, where display and controller may be shared by both the UPT and the USSD. It may be applicable to ticket vending machines.
- Figure 3 gives an example of splitting the UPT into several appropriately secure units that communicate in a secure way.

Figure 1: Self-Contained UPT within an Unattended Self-Service Device



The colors in the block diagrams above and below indicate different levels of attack potential required. Red stands for an attack potential of 35, yellow for an attack potential of 25, and green indicates an attack potential of 16 (14 for the MSR).

Figure 2: Combined UPT and Self-Service Device

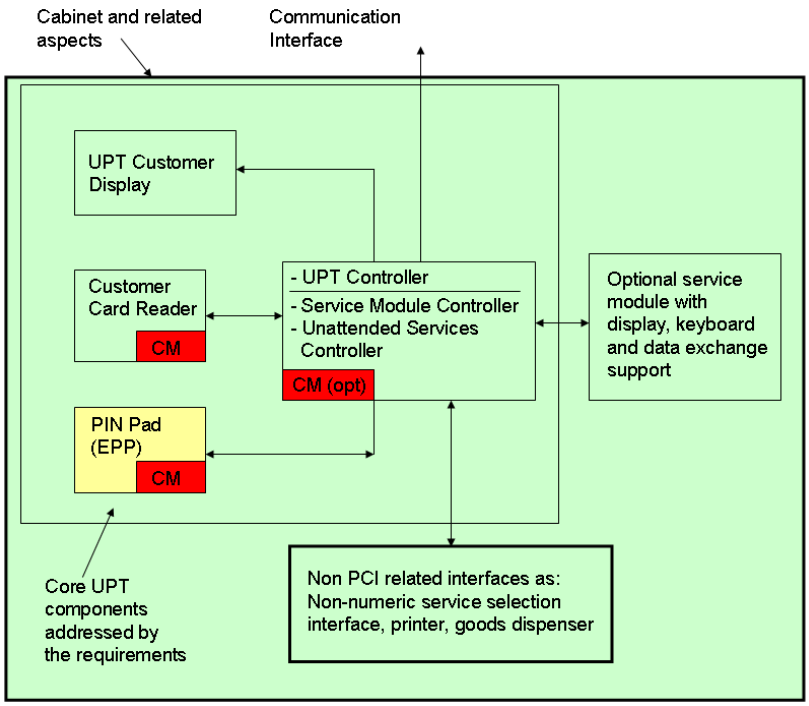
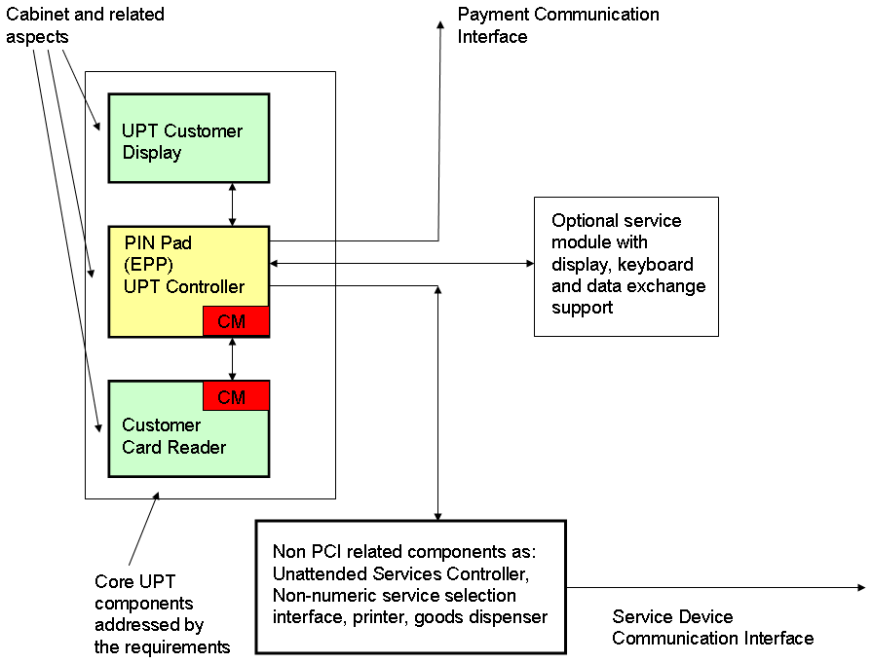


Figure 3: Single Component UPT within an Unattended Self-Service Device



Related Publications

The following ANSI and ISO standards are applicable and related to the information in this document.

Banking—Retail Financial Services Symmetric Key Management	ANSI X9.24
Triple Data Encryption Algorithm: Modes of Operation	ANSI X9.52
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms	ANSI TR-31
Personal Identification Number (PIN) Management and Security	ISO 9564
Banking—Key Management (Retail)	ISO 11568
Banking—Secure Cryptographic Devices (Retail)	ISO 13491

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

UPT Description

April 2009

UPT Identifier	
UPT 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 Version Number:	
Application Version Number: (if applicable)	

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.

Optional Use of Variables in the UPT Identifier

[A]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 UPT Testing and Approval Program Guide *for more information.*

Variable "x" Position	Description of Variable "x" in the Selected Position

Physical Security Requirements

All UPT devices must meet the following **physical** requirements.

Number	Description of Requirement	Part	Yes	No	N/A
A1	Vendors must comply with all components of A1.				
A1.1	The UPT uses tamper detection and response mechanisms, which cause the UPT to become immediately inoperable, and results in the automatic and immediate erasure of any secret information that may be stored in the UPT, such that it becomes infeasible to recover the secret information. 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 25 per UPT, exclusive of the ICC reader, for identification and initial exploitation as defined in Appendix B of the PCI UPT DTRs, **and** *Note: The replacement of casing parts shall be considered as part of any attack scenario*	**EPP** **CM**	☐ ☐	☐ ☐	☐ ☐
A1.2	Failure of a single security mechanism does not compromise UPT security. Protection against a threat is based on a combination of at least two independent security mechanisms.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
A2	If the UPT or its components permit access to internal areas (e.g. for service or maintenance) that process or store sensitive data, then it is not possible using this access area to insert a PIN disclosing bug. Immediate access to such sensitive data such as PINs or cryptographic data is either prevented by the design of the internal areas (e.g. by enclosing the components with tamper resistant/responsive enclosures), or it has a mechanism so that access to internal areas causes the immediate erasure of sensitive data.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
A3	The security of the UPT is not compromised by altering: ▪ Environmental conditions ▪ Operational conditions *(An example includes subjecting components containing or processing sensitive data to temperatures or operating voltages outside the stated operating ranges.)*	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
A4	Sensitive functions or information are only used in the protected area(s) of the UPT. Sensitive information and functions dealing with sensitive information are protected from modification without requiring an attack potential of at least 25 per UPT, exclusive of the IC card reader, for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs.*	**EPP** **CM**	☐ ☐	☐ ☐	☐ ☐

Number	Description of Requirement	Part	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. *Note: See also Requirement B5.*	**EPP**	☐	☐	☐
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 terminal operator without requiring an attack potential of at least 25 per UPT to defeat or circumvent, for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs*.	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
A7	To determine any PIN-security-related cryptographic key resident in the UPT, by penetration of the UPT and/or by monitoring emanations from the EPP or ICC reader (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs.*	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
A8	The EPP and the IC card reader of the UPT are protected against removal; defeating or circumventing this mechanism must require an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs*. *Note: This protection may be provided by a suitable strong cabinet.*	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
A9	The UPT provides a means to deter the visual observation of PIN values as the cardholder is entering them. *Note: Case design must be part of the hardware version number.* *Note: Some markets may require Option A.1 of Appendix A of the DTR or a stricter criterion.*	**UPT**	☐	☐	☐
A10	The UPT is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attack).	**UPT**	☐	☐	☐
A11	It is not feasible to penetrate the UPT to make any additions, substitutions, or modifications to the Magnetic Stripe Reader or the UPT's hardware or software, in order to determine (e.g. skimming attacks must be prevented) or modify magnetic stripe track data, without requiring an attack potential of at least 14 per UPT, for identification and initial exploitation, as defined in Appendix B of the *PCI UPT DTRs*.	**UPT**	☐	☐	☐

Logical Security Requirements

All UPT devices must meet the following **logical** requirements.

Number	Description of Requirement	Part	Yes	No	N/A
B1	The UPT 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 the firmware of the EPP and the ICC reader, the software of the UPT controller, security mechanisms for signs of tampering, and whether the UPT is in a compromised state. In the event of a failure, the relevant component's functionality fails in a secure manner.	**EPP** **ICCR** **UC** **CM**	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐
B2	The UPT's relevant component'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 relevant component outputting the clear-text PIN or other sensitive information.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
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.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
B4	If the UPT allows updates of firmware or other software that impacts security, the software integrity is cryptographically authenticated by the device. If the authenticity of the update is not confirmed, the software update is rejected and deleted. ▪ The authentication must not be performed by a component of lesser protection strength than the one for which the firmware/software is intended, **OR** ▪ The authentication must be performed by the target component of the firmware/software.	**EPP** **ICCR** **UC** **CM**	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐
B5	A PIN-handling component of the UPT (e.g. the EPP) never outputs information to another component (e.g. a display or a device controller) allowing the differentiation of the PIN digits entered.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐

Number	Description of Requirement	Part	Yes	No	N/A
B6	Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the EPP immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button. The UPT must automatically clear its internal buffers when either: ▪ The transaction is completed, **OR** ▪ The UPT has timed-out waiting for the response from the cardholder or merchant.	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
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 information.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
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 UPT is forced to return to its normal mode.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
B9	If the UPT generates random numbers in connection with security over sensitive data, then the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
B10	The EPP has characteristics that prevent or significantly deter the use of a stolen device for exhaustive PIN determination.	**EPP**	☐	☐	☐
B11	The key-management techniques implemented in the UPT conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support ANSI TR-31 or an equivalent methodology for maintaining the TDEA key bundle. ***Note:*** *Clear keys or clear-key parts must not be loaded using the service module.*	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
B12	The PIN-encryption technique implemented in the UPT is a technique included in ISO 9564.	**EPP**	☐	☐	☐
B13	It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the UPT. The UPT must enforce that data keys, key-encipherment keys and PIN-encryption keys have different values.	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐

Number	Description of Requirement	Part	Yes	No	N/A
B14	There is no mechanism in the UPT 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.	**EPP** **ICCR** **CM**	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
B15	If the UPT has a keypad that can be used to enter non-PIN data, then at least one of the following **B15.x** statements must be true.				
B15.1	All prompts for non-PIN data entry are under the control of the cryptographic unit of the UPT and circumventing the control requires an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs*. 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, ***OR***	**EPP** **UC**	☐ ☐	☐ ☐	☐ ☐
B15.2	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 16 per UPT for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs*, ***OR***	**EPP** **UC**	☐ ☐	☐ ☐	☐ ☐
B15.3	The UPT (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 EPP, e.g., by using cryptographic authentication. If commands impacting the correspondence between the display messages and the operating state of the EPP 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 EPP cannot occur without requiring an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B of the *PCI UPT DTRs*.	**EPP** **UC**	☐ ☐	☐ ☐	☐ ☐
B16	If the UPT supports multiple applications, it must enforce the separation between applications. It must not be possible that one application interferes with or tampers another application or the OS of the UPT, including modifying data objects belonging to another application.	**UC**	☐	☐	☐

Number	Description of Requirement	Part	Yes	No	N/A
B17	The operating system of the UPT must contain only the components and the services necessary for the intended operation. It must be configured and run with least privilege.	**UC**	☐	☐	☐
B18	The UPT 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.	**UPT**	☐	☐	☐

Online Security Requirements

All **online** UPT devices must meet the following requirement.

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

Offline Security Requirements

All **offline** UPT devices must meet the following requirements.

Number	Description of Requirement	Part	Yes	No	N/A
D1	It is not 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 16, for identification and initial exploitation, as defined in Appendix B of the *PCI UPT DTRs*. *Note: The ICC reader may consist of areas of different protection levels e.g., the areas of the IC card interface itself, and the area holding retracted cards.*	**ICCR**	☐	☐	☐
D2	Vendors must comply with all components of D2.				
D2.1	The slot of the ICC reader into which the IC card is inserted does not have sufficient space to hold a PIN-disclosing "bug" when a card is inserted, nor can it feasibly be enlarged to provide space for a PIN-disclosing "bug." It is not possible for both an IC card and any other foreign object to reside within the card insertion slot.	**ICCR** **CAB**	☐ ☐	☐ ☐	☐ ☐
D2.2	The opening for the insertion of the IC card is in full view of the cardholder prior to card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	**ICCR** **CAB**	☐ ☐	☐ ☐	☐ ☐
D3	The ICC reader of the UPT is constructed and integrated into the UPT so that wires running out of the slot of the ICC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	**ICCR** **CAB**	☐ ☐	☐ ☐	☐ ☐

Number	Description of Requirement	Part	Yes	No	N/A
D4	PIN protection during transmission within the UPT (at least **one** must apply):				
D4.1	If the UPT's EPP and the ICC reader are not integrated into the same secure module and the cardholder verification method (i.e., the IC card requires) is determined to be an enciphered PIN, then the PIN block shall be enciphered between the EPP and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.[A]	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
D4.2	If the UPT's EPP and the ICC reader are not integrated into the same secure module and the cardholder verification method is determined to be a plaintext PIN, then the PIN block shall be enciphered from the EPP to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.[B]	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
D4.3	If the UPT's EPP and the ICC reader are integrated into the same secure module and the cardholder verification method is determined to be an enciphered PIN, then the PIN block shall be enciphered using an authenticated encipherment key of the IC card.[B]	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐
D4.4	If the UPT's EPP and the ICC reader are integrated into the same secure module and the cardholder verification method is determined to be a plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the 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.[A]	**EPP** **ICCR**	☐ ☐	☐ ☐	☐ ☐

[A] A plain-text PIN from the EPP to the ICC reader is never permitted except when the EPP and ICC reader are integrated in a single tamper-resistant device.

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

Device Security Requirements During Manufacturing

The UPT manufacturer, subject to Association 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
E1	Change-control procedures are in place so that any intended security relevant change to the physical or functional capabilities of the UPT causes a re-certification of the device under the Physical Security Requirements and/or the Logical Security Requirements of this document.	☐	☐	☐
E2	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.	☐	☐	☐
E3	The UPT is assembled in a manner that the components used in the manufacturing process are those components that were certified by the Physical Security Requirements evaluation, and that unauthorized substitutions have not been made.	☐	☐	☐
E4	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.	☐	☐	☐
E5	Subsequent to production but prior to shipment from the manufacturer's facility, the UPT 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.	☐	☐	☐
E6	If the UPT 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 UPT, unknown and unpredictable to any person, and installed in the UPT under dual control to ensure that it is not disclosed during installation.	☐	☐	☐

Device Security Requirements between Manufacturer and Initial Key Loading

The UPT manufacturer, subject to Association 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
F1	The UPT 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 UPT at every point in time.	☐	☐	☐
F2	Procedures are in place to transfer accountability for the device from the manufacturer to the initial-key-loading facility.	☐	☐	☐
F3	While in transit from the manufacturer's facility to the initial-key-loading facility, the device is: ▪ Shipped and stored in tamper-evident packaging; and/or ▪ Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial-key-loading facility, but that cannot feasibly be determined by unauthorized personnel.	☐	☐	☐

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 Manufacturer Self-Assessment Form.

UPT Manufacturer Information			
UPT Manufacturer:			
Address 1:			
Address 2:			
City:		**State/Prov:**	
Country:		**Mail Code:**	
Primary Contact:			
Position/Title:			
Telephone No:		**Fax:**	
E-mail Address:			

Compliance Declaration Statement – Form B

Compliance Declaration	
UPT 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 UPT is:

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

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

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

Attach to this form a device-specification sheet that highlights the device characteristics including photos of the device. These photos are to include both external and internal pictures of the device. The internal pictures are to be sufficient to show the various components of the device.

Compliance Declaration Exception – Form C

UPT Manufacturer:	
Model Name and Number:	

INSTRUCTIONS:

*For any statement, A1-A11, B1-B20, C1-C6, D1-D4, for which the answer was a "**NO**" or an "**N/A**," **explain why the answer was not "YES."***

Statement Number	Explanation

Glossary

Active Display	Active display is the term given to terminals, which allow display prompts to be changed once the device has been deployed. An example would be where a device uses security controls to determine how application programs are written, loaded and executed. Cryptographic mechanisms must be in place to protect the control of the terminal display. The device must use cryptographically based controls to drive the terminal display such that it is infeasible for an entity not possessing a specified unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the terminal.
ATM	An unattended terminal that has electronic capability, accepts PINs, disburses currency or cheques and may provide balance information, funds transfers between accounts, and prepaid card loading and other services.
Cabinet (CAB)	The CAB is the physical boundary of the UPT. It may be the complete machine or the smallest detachable cabinet or enclosure that includes all the UPT interface units defined below. The CAB restricts access to the UPT components. For practical reasons, the physical UPT may or may not include the part of the equipment that dispenses the product or provides the service. The scope of the CAB includes the front cover presenting the interface units to the cardholder, including any signs, pictograms and instructions visible to the cardholder. All interface functions through which the cardholder performs the tasks related to the card payment are considered interface units to be included in the physical UPT (CAB).
Cardholder	An individual to whom a card is issued or who is authorized to use the card.
Communication Interface (CI)	The interface to the authorization host or other background systems.
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 plain-text cryptographic keys and other keying material).
Cryptographic Module (CM)	The CM, located in the UPT controller (optional), is considered only if it is used for other services related to PIN handling and firmware. References to the CM in these requirements do not include CMs present in the EPP or ICCR. Where applicable, those are directly stated.
Customer Card Reader (CR)	The UPT must be equipped with at least one type of card reader, a magnetic-stripe reader (MSR) or an ICC reader (ICCR). CR may be a hybrid reader and possibly motorized. If the ICC reader supports clear offline PIN, and it is not integrated with the EPP into a physically secure boundary, it must be by itself physically secure and able to establish an encrypted communication to the EPP, and may therefore contain a cryptographic module (CM).
Customer Display (DSP)	The display is usually directly connected to the UPT controller, and is assumed in these requirements to be a passive device, which cannot authenticate the counterpart or decrypt message content. However, that may not always be the case.

Dual Control	A process of using two or more separate entities (usually persons), who are operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key-generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see "split knowledge."
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.
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 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.
Firmware	Any code within the EPP that provides security protections needed to comply with these EPP security requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under these EPP security requirements.
ICC Reader	A device that interfaces to IC cards. It may be integrated into a PED or designed as a separate device with its own shell and its own computing capability.
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
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 Common Criteria for composite evaluations, attack paths, attack quotations, and methodology.
Key Bundle	The three cryptographic keys (K1, K2, K3) used with a TDEA mode.
KEK	See Key-encrypting key
Key-encrypting (encipherment or exchange) Key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys. Also known as a key-encryption or key-exchange key.

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.
Magnetic Stripe Reader	A device that reads Magnetic Strip Cards. It may be integrated into another module of the UPT or the ICC reader as a hybrid reader.
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.
Merchant	An entity that contracts with an acquirer to originate transactions and that displays card acceptance marks for PIN-based transactions.
Offline PIN Verification	A process used to verify the Cardholder's identity by comparing the PIN entered at the Chip-Reading Device to the PIN value contained in the Chip.
Online PIN Verification	A process used to verify the Cardholder's identity by sending an encrypted PIN value to the Issuer for validation in an Authorization Request.
Personal Identification Number (PIN)	A numeric personal identification code that authenticates a cardholder in an authorization request that originates at a terminal with authorization only or data capture only capability. A PIN consists only of decimal digits.
PIN Entry Device (PED)	A device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor and storage for PIN processing sufficiently secure for the key management scheme used, and firmware. A PED has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell.
Sensitive (secret) Data (information)	Data that must be protected against unauthorized disclosure, alteration or destruction, especially plain-text PINs, and secret and private cryptographic keys, and includes design characteristics, status information, and so forth.
Sensitive Functions	Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs and passwords.
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.
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.
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 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, thereby preventing a success.
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.
Terminal	A device/system that initiates a transaction. It includes a PED and/or an ICC reader as well as additional hardware and/or software to provide a payment management interface and a communication interface to an acquirer's host.
Unattended Acceptance Terminal (UAT)	See Unattended Payment Terminal.
Unattended Payment Terminal	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment including, but not limited to, the following: ▪ Automated Fuel Dispenser ▪ Ticketing Machine ▪ Vending Machine
UPT Controller (UC)	The UC may be integrated in the EPP or the CR, or it may be also be a separate module, possibly a PC-operated by a standard operating system. In the latter case, the UC may contain a cryptographic module. As far as it is used for PIN (re-)encryption, it is considered here.