Payment Card Industry (PCI)

Encrypting PIN Pad (EPP)

Security Requirements

Version 2.1

January 2009

Document Changes

Date	Version	Description
September 2006	2.x	Draft published for comment
November 2006	2.x	Formatting changes
April 2007	2.x	A1, A7, A8, B1, B4, B11, B13
July 2007	2.0	New version
January 2009	2.1	Clarifications and errata

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

Encrypting PIN Pads (EPPs) form a component of unattended PIN Entry Devices (PEDs). Typically, EPPs are used to enter a cardholder's PIN in a secure manner. For the purpose of this document, an EPP is considered to consist only of a secure PIN entry device. Other such PIN entry devices that contain a PIN pad and additional components such as an integrated display or card reader will need to complete the PCI POS PED security evaluation process rather than the EPP process.

EPPs are used in conjunction with ATMs, automated fuel dispensers, kiosks, and vending machines. Overall requirements for those devices can be found in other Payment Card Industry (PCI) PED security documents. Vendors may choose to have EPPs evaluated independently as the first step for PED approval, or as part of the overall PED approval for that device type. Additional criteria apply for PED approval, such as display prompt control, and where intended for offline usage, criteria applicable to the IC card reader and interaction with that reader.

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

EPPs must meet all applicable requirements. EPP vendors must have the specified device characteristics validated at independent laboratories that are recognized by the participating PCI Associations. EPP vendors must also meet the device management requirements and the Associations reserve the right to have those requirements independently validated.

Device Characteristics

Device characteristics are those attributes of the EPP 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 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 EPP 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 EPPs 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*.

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.

EPP Description

January 2009

EPP Identifier	
EPP 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 EPP 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 PIN Entry Device Testing and Approval Program Guide *for more information.*

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

Physical Security Requirements

All EPPs must meet the following **physical** requirements.

Number	Description of Requirement	Yes	No	N/A
A1	Vendors must comply with all components of A1.			
A1.1	The EPP uses tamper-detection and response mechanisms that cause the EPP to become immediately inoperable and result in the automatic and immediate erasure of any secret information that may be stored in the EPP, 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 EPP, for identification and initial exploitation as defined in Appendix A of the *PCI EPP DTRs,* **and** *Note: The replacement of both the front and rear casings shall be considered as part of any attack scenario.*	☐	☐	☐
A1.2	Failure of a single security mechanism does not compromise EPP security. Protection against a threat is based on a combination of at least two independent security mechanisms.	☐	☐	☐
A2	If the EPP permits access to internal areas (e.g., for service or maintenance), then it is not possible using this access area to insert a PIN-disclosing bug. 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 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.	☐	☐	☐
A3	The security of the EPP is not compromised by altering: ▪ Environmental conditions. ▪ Operational conditions *(An example includes subjecting the EPP to temperatures or operating voltages outside the stated operating ranges.)*	☐	☐	☐
A4	Sensitive functions or information are only used in the protected area(s) of the EPP. Sensitive information and functions dealing with sensitive information are protected from modification without requiring an attack potential of at least 25 per EPP, for identification and initial exploitation as defined in Appendix A of the *PCI EPP DTRs.*	☐	☐	☐
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.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
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 without requiring an attack potential of at least 25 per EPP to defeat or circumvent.	☐	☐	☐
A7	To determine any PIN-security-related cryptographic key resident in the EPP, by penetration of the EPP and/or by monitoring emanations from the EPP (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation as defined in Appendix A of the *PCI EPP DTRs.*	☐	☐	☐
A8	The EPP is protected against unauthorized removal. Defeating or circumventing this mechanism must require an attack potential of at least 16 per EPP for identification and initial exploitation as defined in Appendix A of the *PCI EPP DTRs*.	☐	☐	☐

Logical Security Requirements

All EPPs must meet the following **logical** requirements.

Number	Description of Requirement	Yes	No	N/A
B1	The EPP 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 EPP is in a compromised state. In the event of a failure, the EPP and its functionality fails in a secure manner.	☐	☐	☐
B2	The EPP'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 EPP outputting the clear text PIN or other sensitive information.	☐	☐	☐
B3	The firmware, and any changes thereafter, have been inspected and reviewed using a documented and auditable process, and certified as being free from hidden and unauthorized or undocumented functions.	☐	☐	☐
B4	If the EPP allows updates of firmware, the device cryptographically authenticates the firmware integrity and if the authenticity is not confirmed, the firmware update is rejected and deleted.	☐	☐	☐
B5	The EPP never outputs information to another component (e.g. a display or a device controller) allowing the differentiation of the PIN digits entered.	☐	☐	☐
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 EPP must automatically clear its internal buffers when either: ▪ The transaction is completed, or ▪ The EPP has timed out waiting for the response from the cardholder or merchant	☐	☐	☐
B7	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive information.	☐	☐	☐
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 EPP is forced to return to its normal mode.	☐	☐	☐
B9	If random numbers are generated by the EPP in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	☐	☐	☐
B10	The EPP has characteristics that prevent or significantly deter the use of a stolen device for exhaustive PIN determination.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
B11	The key-management techniques implemented in the EPP 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.	☐	☐	☐
B12	The PIN-encryption technique implemented in the EPP is a technique included in ISO 9564.	☐	☐	☐
B13	It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the EPP. The EPP must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.	☐	☐	☐
B14	There is no mechanism in the EPP that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.	☐	☐	☐
B15	If the EPP can hold multiple PIN-encryption keys and if the key to be used to encrypt the PIN can be externally selected, the EPP prohibits unauthorized key replacement and key misuse.	☐	☐	☐

Device Security Requirements During Manufacturing

The EPP 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
C1	Change-control procedures are in place so that any intended security-relevant change to the physical or functional capabilities of the EPP causes a re-certification of the device under the Physical Security Requirements and/or the Logical Security Requirements of this document.	☐	☐	☐
C2	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.	☐	☐	☐
C3	The EPP 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.	☐	☐	☐
C4	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.	☐	☐	☐
C5	Subsequent to production but prior to shipment from the manufacturer's facility, the EPP 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.	☐	☐	☐
C6	If the EPP 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 EPP, unknown and unpredictable to any person, and installed in the EPP under dual control to ensure that it is not disclosed during installation.	☐	☐	☐

Device Security Requirements Between Manufacturer and Initial Key Loading

The EPP 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
D1	The EPP 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 EPP at every point in time.	☐	☐	☐
D2	Procedures are in place to transfer accountability for the device from the manufacturer to the initial-key-loading facility.	☐	☐	☐
D3	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.

EPP Manufacturer Information			
EPP 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	
Model Name and Number:	

I, *(Name)*

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

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

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

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

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

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

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

Compliance Declaration Exception – Form C

EPP Manufacturer:	
Model Name and Number:	

INSTRUCTIONS:

*For any statement, A1-A8, B1-B15, C1-C6, D1-D3, for which the answer was a "**NO**" or an "**N/A**," **explain why the answer was not "YES."***

Statement Number	Explanation

Glossary

Term	Definition
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.
Cardholder	An individual to whom a card is issued or who is authorized to use the card.
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).
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.
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.
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.
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: ▪ ATM ▪ Automated Fuel Dispenser ▪ Card Dispensing Machine ▪ Load Device