Payment Card Industry (PCI)
POS PIN Entry Device

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, A11, B1, B4, B11, B13, D1, D4
July 2007	2.0	PCI Security Standards Council adoption of PED requirements
January 2009	2.1	Clarifications and errata

Requirements A7, B10, B11, B12, B13, and B14 were formerly online PIN only requirements and are now core requirements applicable to all devices evaluated using these requirements.

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 PIN entry devices (PEDs). Thus, the requirements are not intended to eliminate the possibility of fraud, but to reduce its likelihood and limit its consequences.

These requirements 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

Device Characteristics

Device characteristics are those attributes of the PED 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 PEDs must meet. Additional requirements for PEDs 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 PED 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 point-of-sale PEDs 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 Associations and the *PCI PIN Security Requirements*.

Related Publications

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

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.

PED Description

January 2009

PED Identifier	
PED 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 PED 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 PIN Entry Devices 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 PED uses tamper-detection and response mechanisms that cause the PED to become immediately inoperable and result in the automatic and immediate erasure of any secret information that may be stored in the PED, 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 PED, exclusive of the IC card reader, for identification and initial exploitation as defined in Appendix B of the *PCI POS PED 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 PED security. Protection against a threat is based on a combination of at least two independent security mechanisms.	☐	☐	☐
A2	If the PED or ICC reader[A] permits access to internal areas (e.g., for service or maintenance), 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 components with sensitive data into 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 PED is not compromised by altering:
	
	  ▪ Environmental conditions.
	
	  ▪ Operational conditions
	
	(An example includes subjecting the PED to temperatures or operating voltages outside the stated operating ranges.)
		☐	☐	☐

[A] The **"or"** in the term "PED or ICC reader" in this requirement and the following ones is a logical "or." If the security property mentioned depends on design properties of the PED and the ICC reader, either independently or together, the requirement must be met by each of the two devices.

Number	Description of Requirement	Yes	No	N/A
A4	Sensitive functions or information are only used in the protected area(s) of the PED. Sensitive information and functions dealing with sensitive information are protected from modification without requiring an attack potential of at least 25 per PED, exclusive of the IC card reader, for identification and initial exploitation as defined in Appendix B of the *PCI POS PED 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.	☐	☐	☐
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 or sales clerk without requiring an attack potential of at least 25 per PED as defined in Appendix B of the *PCI POS PED DTRs* to defeat or circumvent.	☐	☐	☐
A7	To determine any PIN-security-related cryptographic key resident in the PED or ICC reader, by penetration of the PED or ICC reader and/or by monitoring emanations from the PED 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 POS PED DTRs.*	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
A8	If the PED has a keypad that can be used to enter non-PIN data, then at least **one** of the following **A8.x** statements must be true. *(Statements A8.1 and A8.2 are intended to be met by the vendor controlling the means of authorizing prompt changes. Statement A8.3 is the option that is intended to allow third parties to control the means of authorization.)*			
A8.1	All prompts for non-PIN data entry are under the control of the cryptographic unit of the PED and requiring an attack potential of at least 16 per PED for identification and initial exploitation as defined in Appendix B of the *PCI POS PED DTRs* 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, **or**	☐	☐	☐
A8.2	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 PED for identification and initial exploitation as defined in Appendix B of the *PCI POS PED DTRs,* **or**	☐	☐	☐
A8.3	For active display devices, cryptographically based controls are utilized to control the PED display and PED 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 PED. 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.	☐	☐	☐
A9	The PED provides a means to deter the visual observation of PIN values as they are being entered by the cardholder. *Note: Some markets may require option A.1 of Appendix A or a stricter criterion.*	☐	☐	☐
A10	The design of the PED or ICC reader is such that it is not practical to construct a duplicate PED or ICC reader from commercially available components. For example, the casing used to house the device's electronic components is not commonly available.	☐	☐	☐
A11	It is not feasible to penetrate the PED to make any additions, substitutions, or modifications to the magnetic-stripe read head and associated hardware or software, in order to determine or modify magnetic-stripe track data, without requiring an attack potential of at least 14 per PED, for identification and initial exploitation, as defined in Appendix B of the *PCI POS PED DTRs*.	☐	☐	☐

Logical Security Requirements

All PIN Entry Devices must meet the following **logical** requirements.

Number	Description of Requirement	Yes	No	N/A
B1	The PED 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 PED is in a compromised state. In the event of a failure, the PED and its functionality fail in a secure manner.	☐	☐	☐
B2	The PED'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 PED 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 PED allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	☐	☐	☐
B5	The PED never displays the entered PIN digits. Any array related to PIN entry displays only non-significant symbols, e.g., asterisks.	☐	☐	☐
B6	Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the PED immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button. The PED must automatically clear its internal buffers when either: - The transaction is completed, or - The PED 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 PED is forced to return to its normal mode.	☐	☐	☐
B9	If random numbers are generated by the PED in connection with security over sensitive data, the random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	☐	☐	☐
B10	The PED has characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.	☐	☐	☐

Number	Description of Requirement	Yes	No	N/A
B11	The key-management techniques implemented in the PED 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 PED 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 PED. The PED must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.	☐	☐	☐
B14	There is no mechanism in the PED that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.	☐	☐	☐
B15	The entry of any other transaction data must be separate from the PIN-entry process, avoiding the accidental display of a cardholder PIN on the PED 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.	☐	☐	☐

Additional Online Requirements

All Online PIN Entry Devices must meet the following requirement.

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

Additional Offline Requirements

All Offline PIN Entry Devices must meet the following requirements.

Number	Description of Requirement	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. *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.*	☐	☐	☐
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 ICC card and any other foreign object to reside within the card insertion slot.	☐	☐	☐
D2.2	The opening for the insertion of the IC card is in full view of the cardholder during card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.	☐	☐	☐
D3	The ICC reader is constructed so that wires running out of the slot of the IC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.	☐	☐	☐
D4	PIN Protection During Transmission Between PED and ICC Reader (at least **one** must apply):			
D4.1	If the PED 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, the PIN block shall be enciphered between the PED and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.[B]	☐	☐	☐
D4.2	If the PED 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 PED 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.[C]	☐	☐	☐

[B] 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.

[C] 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.

Number	Description of Requirement	Yes	No	N/A
D4.3	If the PED 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.[B]	☐	☐	☐
D4.4	If the PED 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.[C]	☐	☐	☐

[B] 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.

[C] 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.

Device Security Requirements During Manufacturing

The PED manufacturer, subject to PCI participant site inspections, confirms the following:

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 PED 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 PED 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 PED 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 PED 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 PED, unknown and unpredictable to any person, and installed in the PED under dual control to ensure that it is not disclosed during installation.	☐	☐	☐

Device Management Requirements
(Between Manufacturer and Initial Key Loading)

The PED 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 PED 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.	☐	☐	☐
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.

PED Manufacturer Information			
PED 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	
PED Manufacturer:	
Model Name and Number:	

I, *(Name)*

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

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

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

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

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

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

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

PED Manufacturer:	
Model Name and Number:	

INSTRUCTIONS:

*For any statement, A1-A11, B1-B15, C1, D1-D4, E1-E6, and F1-F3, for which the answer was a "**NO**" or an "**N/A**," explain why the answer was not "YES."*

Statement Number	Explanation

Glossary

Term	Definition
Active Display	"Active display" is the term given to PEDs that 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 PED display. The device must use cryptographically-based controls to drive the PED 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 PED.
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.
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.
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.
Split Knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic 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