Payment Card Industry (PCI)

Hardware Security Module (HSM)

Security Requirements

Version 1.0

April 2009

Document Changes

Date	Version	Author	Description
September 2003	0.5	InfoGard	Initial Draft
October 2004	0.6	InfoGard	Modifications from vendor feedback
February 2006	0.7	InfoGard	Modifications from benchmark evaluation
February 2006	0.8	InfoGard	Modifications from lab meeting
March 2008	0.85	Visa	Harmonize with PCI PED
November 2008	0.86	PCI	Modifications from lab meeting
April 2009	1.0	PCI	Initial Release

Table of Contents

Introduction

This document contains a complete set of requirements for securing Hardware Security Modules (HSM). HSMs may support a variety payment processing and cardholder authentication applications and processes. The processes which are relevant to the full set of requirements outlined in this document are:

- PIN Processing
- 3-D Secure
- Card Verification
- Card Production and Personalization
- EFTPOS
- ATM Interchange
- Cash Card Reloading
- Data Integrity
- Chip Card Transaction Processing

There are many other applications and processes that may utilize general purpose HSMs, and which may necessitate the adoption of all or a subset of the requirements listed in this document. However this document does not aim to develop a standard for general purpose HSMs for use outside of the applications listed above.

HSMs are typically housed in a secure environment and managed with additional procedural controls external to the device.

These HSM security requirements were derived from existing ISO, ANSI, Federal standards and accepted/known good practice recognized by the financial industry applicable to multi-chip products with robust security and assurance characteristics.

FIPS 140-2 Requirements

Some requirements in this manual are derived from requirements in Federal Information Processing Standard 140-2 (FIPS 140-2). These requirements are identified in this document with an asterisk (*) in the number column.

Because many FIPS 140-2 evaluations only cover a subsection of the HSM and with a number of possible security levels, existing evaluation evidence for an HSM certified against FIPS 140-2 will be assessed as follows.

The evaluator will establish:

- The HSM components that were evaluated;
- The security level of the evaluation;
- That the existing FIPS certification covers the full HSM functionality for all the related requirements.

Related Publications

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

Data Encryption Algorithm	ANXI X3.92
Banking—Retail Financial Services Symmetric Key Management	ANSI X9.24
Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	ANSI X9.42
Triple Data Encryption Algorithm: Modes of Operation	ANSI X9.52
Security Requirements for Cryptographic Modules	FIPS PUB 140-2
Personal Identification Number (PIN) Management and Security	ISO 9564
Information Technology – Security Techniques – Modes of Operation for an n-bit Block Cipher	ISO 10116
Information Technology – Security Techniques – Hash Functions	ISO 10118
Banking—Key Management (Retail)	ISO 11568
Information Technology – Security Techniques – Key Management	ISO 11770
Banking—Secure Cryptographic Devices (Retail)	ISO 13491
Information Technology – Security Techniques – Encryption Algorithms	ISO 18033
A Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications	NIST Special Publication 800-22
PCI Encrypting PIN Pad (EPP) Security Requirements	
PCI Encrypting PIN Pad (EPP) Derived Test Requirements	
PCI POS PIN Entry Device (PED) Security Requirements	
PCI POS PIN Entry Device (PED) Derived Test Requirements	
PCI PIN Security Requirements	

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

HSM Description

April 2009

HSM Identifier	
HSM 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 HSM 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 HSM Testing and Approval Program Guide *for more information.*

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

Physical Security Requirements

All HSMs must meet the following **physical** security requirements.

Number	Description of Requirement	Yes	No	N/A
A1	One of the following A1.*x* options must be met.			
A1.1*	The HSM uses mechanisms that detect tampering attempts and cause the automatic and immediate erasure of all clear-text secret information contained in the HSM, such that it becomes infeasible to recover the secret information.	☐	☐	☐
A1.2	Failure of a single security mechanism does not compromise HSM security. Protection against a threat is based on a combination of at least two independent security mechanisms. The HSM also includes characteristics such that penetration of the device results in visible tamper evidence that has a high probability of being detected.	☐	☐	☐
A2	There is no feasible way to determine any sensitive information by monitoring electro-magnetic emissions, power consumption, or any other internal or external characteristic without an attack potential of at least 25 for identification and initial exploitation as defined in Appendix A of the *PCI HSM DTRs.*	☐	☐	☐
A3	The HSM design protects against substitution of the HSM such that it is not practical to construct a duplicate from commercially available components. For example, the enclosure is not commonly available.	☐	☐	☐
A4	Sensitive functions or information are only used in the protected area(s) of the HSM. Sensitive information and functions dealing with sensitive information are protected from modification or substitution, and additionally secret and private keys are protected from disclosure without requiring an attack potential of at least 25 per HSM for identification and initial exploitation as defined in Appendix A.	☐	☐	☐
A5	If the device permits access to internal areas containing security sensitive components (e.g., for service or maintenance), immediate access to 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.	☐	☐	☐

* *Derived from Federal Information Processing Standard 140-2 (FIPS 140-2)*

Number	Description of Requirement	Yes	No	N/A
A6	An available security policy from the vendor addresses the proper use of the HSM, including information on key management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the HSM and indicate the services available for each role in a deterministic tabular form. The HSM is capable of performing only its designed functions, i.e. there is no hidden functionality. The only approved functions performed by the HSM are those allowed by the policy.	☐	☐	☐
A7	The security of the HSM is not compromised by altering environmental conditions or operational conditions (for example subjecting the HSM to temperatures or operating voltages outside the stated operating ranges).	☐	☐	☐

Logical Security Requirements

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

Number	Description of Requirement	Yes	No	N/A
B1*	The HSM provides secure interfaces that are kept logically separate by distinguishing between data and control for inputs and also between data and status for outputs.	☐	☐	☐
B2	There is no mechanism in the HSM that would allow the outputting of existing private or secret clear-text keys, 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. All cryptographic functions implemented shall not output clear-text CSPs to components that could negatively impact security.	☐	☐	☐
B3	The key-management techniques implemented in the HSM 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.	☐	☐	☐
B4*	Private and secret key entry is performed using accepted techniques according to the table below:	☐	☐	☐

Key Form	Technique		
	Manual	**Direct**	**Network**
Plain-text Keys	No	Yes	No
Plain-text Key Components	Yes	Yes	No
Enciphered Keys	Yes	Yes	Yes

* *Derived from Federal Information Processing Standard 140-2 (FIPS 140-2)*

Number	Description of Requirement	Yes	No	N/A
B5	The HSM requires the cooperation of at least two separately authenticated operators for local administration services not normally available, such as plain-text or split knowledge of manual CSP loading or CSP output, enabling or disabling HSM security functions, or the modification of authentication data. The manual entry or output of CSPs in enciphered form requires at least one authenticated operator. The HSM limits the number of function calls (services) and the time limit on these services. If the limits are exceeded, re-authentication is required.	☐	☐	☐
B6*	The HSM ensures that each cryptographic key is only used for a single cryptographic function and only for its intended purpose. * It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the HSM. The HSM does not permit any of the key usage information to be changed.	☐	☐	☐
B7	The HSM ensures that if cryptographic keys within the HSM secure boundary are rendered invalid for any reason (e.g., tamper or long term absence of applied power), the HSM will fail in a secure manner.	☐	☐	☐
B8*	The random number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.	☐	☐	☐
B9	The HSM'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 HSM outputting the clear-text PIN or other sensitive information.	☐	☐	☐
B10	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.	☐	☐	☐
B11	The HSM must automatically clear or reinitialize its internal buffers which hold sensitive information when: ▪ The transaction is completed, or ▪ The HSM has timed out or ▪ The HSM recovers from an error state.	☐	☐	☐
B12*	The HSM uses accepted cryptographic algorithms, modes, and key sizes.	☐	☐	☐

* *Derived from Federal Information Processing Standard 140-2 (FIPS 140-2)*

Number	Description of Requirement	Yes	No	N/A
B13	If the HSM is designed to be used for PIN management, the HSM meets the PIN management requirements of ISO 9564. The PIN-encryption technique implemented in the HSM is a technique included in ISO 9564.	☐	☐	☐
B14*	To ensure that the HSM is operating as designed, the device runs self-tests when powered up and at least once per day to check firmware, security mechanisms for signs of tampering, and whether the HSM is in a compromised state. When specific critical operations are performed, the HSM performs conditional tests. The techniques and actions of the HSM upon failure of a self-test are consistent with those defined in FIPS PUB 140-2.	☐	☐	☐
B15	The HSM includes cryptographic mechanisms to support secure logging of transactions, data, and events to enable auditing.	☐	☐	☐
B16	The HSM has the ability to return its unique device ID.	☐	☐	☐
B17*	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 and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive information	☐	☐	☐
B18	If the HSM 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.	☐	☐	☐

* *Derived from Federal Information Processing Standard 140-2 (FIPS 140-2)*

Device Security Requirements During Manufacturing

The HSM 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 change to the physical or functional capabilities of the HSM causes a re-certification of the device under the Physical Security Requirements 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 HSM 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 HSM 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 HSM 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 HSM, unknown and unpredictable to any person, and installed in the HSM under dual control to ensure that it is not disclosed during installation.	☐	☐	☐

Device Security Requirements Between Manufacturer and Initial Key Loading

The HSM 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 HSM 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 HSM 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.

HSM Manufacturer Information			
HSM 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	
HSM 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 HSM 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

HSM Manufacturer:	
Model Name and Number:	

INSTRUCTIONS:

*For any statement, A1-A8, B1-B18, C1-6, or D1-3, for which the answer was a "**NO**" or an "**N/A**," **explain why the answer was not "YES."***

Statement Number	Explanation

Glossary

Term	Definition
Access Controls	Ensuring that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity.
Active Erasure	Mechanism that intentionally clears data from storage through a means other than simply removing power (e.g. zeroization, inverting power).
Advanced Encryption Algorithm (AES)	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
ANSI (ANS)	American National Standards Institute. A U.S. standards accreditation organization.
Application Programming Interface (API)	A source code interface that a computer system or program library provides to support requests for services to be made of it by a computer program.
Asymmetric Cryptographic Algorithm	See *Public Key Cryptography.*
Asymmetric Key Pair	A public key and related private key created by and used with a public key cryptosystem.
Audit Journal	A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results.
Audit Trail	See *Audit Journal*.
Authentication	The verification of the identity of a person or process.
Authorization	The right granted to a user to access an object, resource or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource or function.
Availability	Ensuring that legitimate users are not unduly denied access to information and resources.
Base (Master) Derivation Key (BDK)	See *Derivation Key.*
Check Value	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible. Check values shall not allow the determination of the secret key.

Ciphertext	An encrypted message.
Clear-text	See *Plain-Text.*
Computationally Infeasible	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it with the current or predicted power of computers.
Confidentiality	Ensuring that information is not disclosed or revealed to unauthorized persons, entities, or processes.
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).
Critical Security Parameters (CSP)	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and personal identification numbers (PINs)) whose disclosure or modification can compromise the security of a cryptographic module.
Cryptographic Key (Key)	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of plain-text data into ciphertext data, ▪ The transformation of ciphertext data into plain-text data, ▪ A digital signature computed from data, ▪ The verification of a digital signature computed from data, ▪ An authentication code computed from data, or ▪ An exchange agreement of a shared secret.
Cryptographic Key Component (Key Component)	One of at least two parameters having the characteristics (for example, format, randomness) of a cryptographic key that is combined with one or more like parameters, for example, by means of modulo-2 addition, to form a cryptographic key. Throughout this document, key component may be used interchangeably with secret share or key fragment.
Cryptoperiod	Time during which a key can be used for signature verification or decryption; it should extend well beyond the lifetime of a key (where the lifetime is the time during which a key can be used to generate a signature and/or perform encryption).
Cryptosystem	A system used for the encryption and decryption of data.
Data Encryption Algorithm (DEA)	A published encryption algorithm used to protect critical information by enciphering data based upon a variable secret key. The Data Encryption Algorithm is defined in ANSI X3.92: “Data Encryption Algorithm” for encryption and decrypting data.
Decipher	See *Decrypt.*
Decrypt	A process of transforming ciphertext (unreadable) into plain-text (readable).
Decryption	See *Decrypt.*

Derivation Key	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the Derived Unique Key Per Transaction key management method. Derivation keys are normally used in a transaction-receiving (e.g., acquirer) TRSM in a one-to-many relationship to derive or decrypt the Transaction (the derived keys) Keys used by a large number of originating (e.g., terminals) TRSMs.
DES	Data Encryption Standard (see *Data Encryption Algorithm*). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm.
DTP	Detailed Test Procedure
DTR	Derived Test Requirement
Device	See *Secure Cryptographic Device.*
Dictionary Attack	Attack in which an adversary builds a dictionary of plain-text and corresponding ciphertext. When a match can be made between intercepted ciphertext and dictionary-stored ciphertext, the corresponding plain-text is immediately available from the dictionary.
Digital Signature	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.
Double-Length Key	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDES cryptographic algorithm.
Dual Control	A process of using two or more separate entities (usually persons), 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.
ECB	Electronic codebook
EFP	Environmental Failure Protection
EFTPOS	Electronic Funds Transfer at Point of Sale
Electronic Code Book (ECB) Operation	A mode of encryption using a symmetric encryption algorithm, such as DEA, in which each block of data is enciphered or deciphered without using an initial chaining vector or previously (encrypted) data blocks.
Electronic Key Entry	The entry of cryptographic keys into a security cryptographic device in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.
Encipher	See *Encrypt.*

Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data, i.e., the process of transforming plain-text into ciphertext..
Encrypted Key (Ciphertext Key)	A cryptographic key that has been encrypted with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plain-text key.
Encryption	See *Encrypt.*
EPROM	Erasable Programmable Read-Only Memory.
EEPROM	Electronically Erasable Programmable Read-Only Memory.
Exclusive-OR	Binary addition with no carry, also known as modulo 2 addition, symbolized as “XOR” and defined as: 0 + 0 = 0 0 + 1 = 1 1 + 0 = 1 1 + 1 = 0
FIPS	Federal Information Processing Standard.
Firmware	Any code within the HSM that provides security protections needed to comply with these HSM security requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under these HSM security requirements.
Hardware (Host) Security Module	See *Secure Cryptographic Device.*
Hash	A (mathematical) function, which is a non-secret algorithm, which takes any arbitrary length message as input and produces a fixed length hash result. Approved hash functions satisfy the following properties: 1) One-Way. It is computationally infeasible to find any input that maps to any pre-specified output. 2) Collision Resistant. It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output. It may be used to reduce a potentially long message into a “hash value” or “message digest” which is sufficiently compact to be input into a digital signature algorithm. A “good” hash is such that the results of applying the function to a (large) set of values in a given domain will be evenly (and randomly) distributed over a smaller range.
Hexadecimal Character	A single character in the range 0-9, A-F (upper case), representing a four-bit string
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Interface	A logical section of a cryptographic device that defines a set of entry or exit points that provide access to the device, including information flow or physical access.

Initialization Vector (IV)	A binary vector used as the input to initialize the algorithm (a stream or block cipher) for the encryption of a plain-text block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
IPSEC	IP Security Protocol
Irreversible Transformation	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.
ISO	International Organization for Standardization. An international standards accreditation organization.
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.
KEK	See *Key Encrypting Key.*
Key	See *Cryptographic Key.*
Key Agreement	A key establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
Key Archive	Process by which a key no longer in operational use at any location is stored.
Key Backup	Storage of a protected copy of a key during its operational use.
Key Bundle	The three cryptographic keys (K1, K2, K3) used with a TDEA mode.
Key Component	See *Cryptographic Key Component.*
Key Deletion	Process by which an unwanted key, and information from which the key may be reconstructed, is destroyed at its operational storage/use location.
Key Destruction	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location. Information may still exist at the location from which the key may be feasibly reconstructed.
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 Establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key Fragment	See *Cryptographic Key Component.*
Key Generation	Creation of a new key for subsequent use.
Key Instance	The occurrence of a key in one of its permissible forms, that is, plain-text key, key components and enciphered key.
Key Loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.
Key-Loading Device	A self-contained unit that is capable of storing at least one plain-text or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.
Key Pair	Two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is known only to the appropriate entities.
Key Replacement	Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.
Key (Secret) Share	One of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that less than a quorum does not provide any information about the key.
Key Storage	Holding of the key in one of the permissible forms.
Key Termination	Occurs when a key is no longer required for any purpose and all copies of the key and information required to regenerate or reconstruct the key have been deleted from all locations where they ever existed.
Key Transport	A key establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
Keying Material	The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships.
Key Usage	Employment of a key for the cryptographic purpose for which it was intended
Legitimate Use	Ensuring that resources are used only by authorized persons in authorized ways.
Manual Key Distribution	The distribution of cryptographic keys, often in a plain-text form requiring physical protection, but using a non-electronic means, such as a bonded courier.
Manual Key Entry	The entry of cryptographic keys into a secure cryptographic device, using devices such as buttons, thumb wheels, or a keyboard.
Master Derivation Key (MDK)	See *Derivation Key.*
Master Key	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a Master Key. May also be known as Master File Key or Local Master Key, depending on the vendor's nomenclature.
Non-Reversible Transformation	See *Irreversible Transformation.*
Passive Erasure	Mechanism that clears data from storage through removal of power.
Password	A string of characters used to authenticate an identity or to verify access authorization.

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.
Personal Identification Number	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.
Physically Secure Environment	An environment that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or a room built with continuous access control, physical security protection, and monitoring.
Physical Protection	The safeguarding of a secure cryptographic device or of cryptographic keys or other critical security parameters using physical means.
PIN	See *Personal Identification Number.*
PIN Encipherment Key (PEK)	A PEK is a cryptographic key that is used for the encryption or decryption of PINs.
Plain-Text	The intelligible form of an encrypted text or of its elements.
Plain-Text Key	An unencrypted cryptographic key, which is used in its current form.
Private Key	A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.
PRNG	Pseudo Random Number Generator
PROM	Programmable Read-Only Memory
Pseudo-Random	A process that is statistically random, and essentially unpredictable, although generated by an algorithmic process.
Public Key	A cryptographic key, used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Public Key (Asymmetric) Cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques, such as RSA, there are four elementary transformations: sign and verify for signature systems, and encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exists asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and where used the four elementary transformations and the corresponding keys should be kept separate. See *Asymmetric Cryptographic Algorithm.*
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware based 'noise' mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
RNG	Random Number Generator
ROM	Read-Only Memory
RSA Public Key Cryptography	Public key cryptosystem that can be used for both encryption and authentication.
Secret Key	A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. A secret key (symmetrical) cryptographic algorithm uses a single secret key for both encryption and decryption. The use of the term “secret” in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.
Secret Key (Symmetric) Cryptographic Algorithm	A cryptographic algorithm that uses a single, secret key for both encryption and decryption.
Secret Share	See *Key Share.*
Secure Cryptographic Device	A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes or both, including cryptographic algorithms.
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.
SHA-1	Secure Hash Algorithm
Shared Secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key derivation function to derive session keys.
Single-Length Key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
SK	Session Key
Split Knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
SSL	Secure Sockets Layer
Symmetric (Secret) Key	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
Tamper-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.
TDEA	See *Triple Data Encryption Algorithm.*
TDES	See *Triple Data Encryption Standard.*
TECB	TDEA electronic codebook.
TLS	Transport Layer Security
Triple Data Encryption Algorithm (TDEA)	The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.
Triple Data Encryption Standard (TDES)	See *Triple Data Encryption Algorithm.*
Triple-Length Key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.
TRSM	Tamper-Resistant Security Module: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. Also known as a secure cryptographic device.

Unprotected Memory	Components, devices, and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a secure cryptographic device.
User	Individual or (system) process authorized to access an information system or that makes use of the trust model to obtain the public key of another user. An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.
Userid	A string of characters that uniquely identifies a user to the system.
Variant of a Key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key. For example exclusive-OR'ing a non-secret constant with the original key.
Verification	The process of associating and/or checking a unique characteristic.
Working Key	A key used to cryptographically process the transaction. A Working Key is sometimes referred to as a data key, communications key, session key, or transaction key.
XOR	See *Exclusive-OR*.
Zeroization (zeroize)	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.
Zeroized	The state after zeroization has occurred.