
# Payment Card Industry (PCI)
# PIN Security Requirements

**Version 1.0**

September 2011

# Document Changes

| Date | Version | Description |
|---|---|---|
| September 2011 | 1.0 | Initial Release |
| | | |

# Table of Contents

# Overview

This document contains a complete set of requirements for the secure management, processing and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals. These PIN Security Requirements are based on the industry standards referenced in the "PIN Security Requirements – Technical Reference" section.

The 32 requirements presented in this document are organized into seven logically related groups, referred to as "Control Objectives." These requirements are intended for use by all acquiring institutions and agents responsible for PIN transaction processing on the payment card industry participants' denominated accounts and should be used in conjunction with applicable industry standards.

This document:

- Identifies minimum security requirements for PIN-based interchange transactions.
- Outlines the minimum acceptable requirements for securing PINs and encryption keys.
- Assists all retail electronic payment system participants in establishing assurances that cardholder PINs will not be compromised.

***Note:***

*Security considerations not directly related to PIN processing of interchange transactions are beyond the scope of this document.*

For specific requirements pertaining to acquiring entities involved in the implementation of symmetric key distribution using asymmetric keys (remote key distribution) or those entities involved in the operation of Certification Authorities for such purposes, see Normative Annex A. Acquiring entities involved in remote key distribution are subject both to the requirements stipulated in the Technical Reference section of this document and the additional criteria stipulated in Annex A.

For specific requirements pertaining to entities that operate key-injection facilities for the injection of keys (KEKs, PEKs, etc.) used for the acquisition of PIN data, see Normative Annex B.

The key sizes specified in this document are the minimums for the specified algorithms. PCI shall specify larger key sizes as appropriate at a future date. Individual payment brands may specify the use of larger key size minimums in connection with the processing of their transactions.

### *Usage Conventions*

This manual has been prepared with certain conventions. The words "must" and "shall" indicate a mandatory requirement. The word "should" indicates a best practice.

### *Effective Date*

The effective date for this document is September 2011.

# Control Objectives

## OBJECTIVE 1

***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***

1. All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD. SCDs are considered tamper-responsive or physically secure devices i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys and all useful residues of PINs and keys contained within it.

   All newly deployed ATMs and POS PIN-acceptance devices must be compliant with the applicable PCI Point of Interaction Security Requirements. Newly deployed hardware security modules (HSMs) should be PCI approved. For specific considerations, contact the payment brand(s) of interest.

2. Cardholder PINs shall be processed in accordance with approved standards.

   a. All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.

   b. All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the *EMV IC Card Specifications for Payment Systems* and ISO 9564.

3. For online interchange transactions, PINs must be only encrypted using ISO 9564–1 PIN-block formats 0, 1, or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.

4. PINs must not be stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.

## OBJECTIVE 2

***Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.***

5. All keys and key components must be generated using an approved random or pseudo-random process.

6. Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.

7. Documented procedures must exist and be demonstrably in use for all key-generation processing.

## OBJECTIVE 3

***Keys are conveyed or transmitted in a secure manner.***

8. Secret or private keys shall be transferred by:
   a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or
   b. Transmitting the key in cipher-text form.

   Public keys must be conveyed in a manner that protects their integrity and authenticity.

9. During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be:
   a. Under the continuous supervision of a person with authorized access to this component, or
   b. Locked in a security container (including tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, or
   c. Contained within a physically secure SCD.

10. All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.

11. Documented procedures must exist and be demonstrably in use for all key transmission and conveyance processing.

## OBJECTIVE 4

***Key-loading to hosts and PIN entry devices is handled in a secure manner.***

12. Secret and private keys must be input into host hardware security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.
   a. Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge.
   b. Key-establishment techniques using public-key cryptography must be implemented securely.

13. The mechanisms used to load secret and private keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.

14. All hardware and passwords used for key-loading must be managed under dual control.

15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.

16. Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.

## OBJECTIVE 5

***Keys are used in a manner that prevents or detects their unauthorized usage.***

17. Unique secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations.
18. Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.
19. Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.
20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device.

## OBJECTIVE 6

***Keys are administered in a secure manner.***

21. Secret keys used for enciphering PIN-encryption keys, or for PIN encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.

22. Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.

23. Key variants must only be used in devices that possess the original key. Key variants must not be used at different levels of the key hierarchy e.g., a variant of a key-encipherment key used for key exchange must not be used as a working key or as a master file key for local storage.

24. Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.

25. Access to secret and private cryptographic keys and key material must be:
    a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use, and
    b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.

26. Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.

27. Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.

28. Documented procedures must exist and be demonstrably in use for all key-administration operations.

## OBJECTIVE 7

***Equipment used to process PINs and keys is managed in a secure manner.***

29. PIN-processing equipment (e.g., PEDs and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the loading of cryptographic keys and that precautions are taken to minimize the threat of compromise once deployed.

30. Procedures must exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.

31. Any SCD capable of encrypting a key and producing cryptograms of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:

    a. Dual access controls required to enable the key-encryption function

    b. Physical protection of the equipment (e.g., locked access to it) under dual control

    c. Restriction of logical access to the equipment.

32. Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.

# PIN Security Requirements—Technical Reference

## Introduction

This Technical Reference contains the specific standards that apply to individual PIN Security Requirements. Furthermore, it provides implementation criteria on how the requirements can be realized. Other implementation methods may be considered, assuming that they provide at least the same level of security.

This Technical Reference refers to Triple-DES (TDEA) with at least double-length key as the cryptographic standard for PIN encryption.

As of this date, the following standards are reflected in the composite PIN Security Requirements:

***Note:***

*From time to time, the standards change in order to more completely reflect the state of both technology and the threat environment at a particular point in time. It is necessary to ensure that the correct Technical Reference is used when evaluating whether a process, technique, piece of equipment, or policy is compliant with a specific requirement.*

## ANSI, EMV, ISO, FIPS, NIST, and PCI Standards

| Source | Publication |
|---|---|
| **ANSI** | *ANSI X3.92: Data Encryption Algorithm* |
| | *ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques* |
| | *ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography* |
| | *ANSI X9.44: Key Establishment Using Integer Factorization Cryptography* |
| | *ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA* |
| | *ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography* |
| | *ANSI X9.65: Triple Data Encryption Algorithm (TDEA) Implementation* |
| | *ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms* |
| **EMV** | *EMV: Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management* |
| **FIPS** | *FIPS PUB 140–2: Security Requirements for Cryptographic Modules* |

| Source | Publication |
|---|---|
| **ISO** | *ISO 9564: Personal Identification Number Management and Security* |
| | *ISO 11568: Banking – Key Management (Retail)* |
| | *ISO 11770–2: Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques* |
| | *ISO 11770–3: Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)* |
| | *ISO 13491: Banking – Secure Cryptographic Devices (Retail)* |
| | *ISO 16609: Banking – Requirements for message authentication using symmetric techniques* |
| | *ISO/IEC 18033-3: Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers* |
| | *ISO TR19038: Guidelines on Triple DES Modes of Operation* |
| **NIST** | *NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* |
| **PCI SSC** | *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements* |
| | *Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements* |
| | *Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements* |
| | *Payment Card Industry (PCI) Hardware Security Module (HSM) Derived Test Requirements* |

## Requirement/Standards Cross-Reference

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 1. All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD. SCDs are considered tamper responsive or physically secure devices—i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys, and all useful residues of PINs and keys contained within it.<br><br>All newly deployed ATMs and POS PIN-acceptance devices must be compliant with the applicable *PCI Point of Interaction Security Requirements*. Newly deployed hardware security modules (HSMs) should be PCI approved. For specific considerations, contact the payment brand(s) of interest. | A secure cryptographic device (SCD) must meet the requirements of a "Physically Secure Device" as defined in **ISO 9564**. Such a device must have a negligible probability of being successfully penetrated to disclose all or part of any secret or private cryptographic key or PIN. A SCD shall be used only after it has been determined that the device's internal operation has not been modified to allow penetration (e.g., the insertion within the device of an active or passive "tapping" mechanism). An SCD (e.g., a PIN entry device (PED)) that complies with this definition may use a fixed key or a master key/session key key-management technique—that is, a unique (at least) double-length TDES PIN-encryption key for each PED—or may use double-length key DUKPT as specified in **ANSI X9.24: PART 1.**<br><br>An SCD relying upon compromise-prevention controls requires that penetration of the device when operated in its intended manner and environment shall cause the automatic and immediate erasure of all PINs, secret or private cryptographic keys and other secret values, and any useful residuals of those contained within the device. These devices must employ physical barriers so that there is a negligible probability of tampering that could successfully disclose such a key.<br><br>In the cases where a PIN is required to travel outside the tamper-resistant enclosure of the PED, the PED must encrypt the PIN directly at the point of entry within the secure cryptographic boundary of the PED to meet the requirements for compromise prevention. PEDs in which the clear-text (unenciphered) PIN travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.<br><br>Purchase orders for point-of-interaction PIN-acceptance devices must specify compliance to the applicable *PCI Point of Interaction Security Requirements*. |
| 2. Cardholder PINs shall be processed in accordance with approved standards.<br><br>a. All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.<br><br>*(Continued on next page)* | Online PIN translation must only occur using one of the allowed key-management methods: DUKPT, fixed key, master key/session key.<br><br>Online PINs must be encrypted using an algorithm and key size that is specified in ISO 9564. Currently, the only approved algorithm for online PIN is the TDEA using the electronic code book (TECB) mode of operation as described in **ANSI X9.65**. For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in **ANSI X9.65**. |

<table>
<tr><th>PIN Security Requirement</th><th>International/Industry Standard(s)</th></tr>
<tr><td>b. All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the EMV IC Card Specifications for Payment Systems.</td><td>See Book 2, Section 7, of the EMV IC Card Specifications for Payment Systems, and ISO 9564.
<table>
<tr><th>PIN submission method</th><th>PED and IC reader integrated as a device meeting the requirements of ISO 9564</th><th>PED and IC reader not integrated as a device meeting the requirements of ISO 9564</th></tr>
<tr><td>1. Enciphered PIN block submitted to the IC</td><td>The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</td><td>The PIN block shall be enciphered between the PED and the IC reader in accordance with ISO 9564 or enciphered using an authenticated encipherment key of the IC.<br>The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</td></tr>
<tr><td>2. Plain-text PIN block submitted to the IC</td><td>No encipherment of the PIN block is required.</td><td>The PIN block shall be enciphered from the PED to the IC reader in accordance with ISO 9564.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>PIN Security Requirement</th><th>International/Industry Standard(s)</th></tr>
<tr><td>3. For online interchange transactions, PINs must only be encrypted using ISO 9564–1 PIN-block formats 0, 1, or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.</td><td>
For secure transmission of the PIN from the point of PIN entry to the card issuer, the encrypted PIN-block format must comply with ISO 9564 format 0, ISO 9564 format 1, or ISO 9564 format 3. ISO format 3 is the recommended format.<br><br>
For ISO format 0 and 3, the clear-text PIN block and the Primary Account Number block must be XOR'ed together and then Triple-DES encrypted in electronic code book (ECB) mode to form the 64-bit output cipher block (the reversibly encrypted PIN block). ISO format 1 and format 2 are formed by the concatenation of two fields: the plain-text PIN field and the filler field.<br><br>
PINs enciphered using one of the PIN-block formats (ISO format 0, 1, 2, and 3) shall not be translated into non-standard PIN-block formats.<br><br>
PINs enciphered only for transmission between the PIN entry device and the IC reader must use one of the PIN-block formats specified in ISO 9564. Where ISO format 2 is used, a unique key per transaction method in accordance with ISO 11568 shall be used. Format 2 shall only be used in connection with either offline PIN verification or PIN change operations in connection with ICC environments.<br><br>
PINs enciphered using ISO format 0 or ISO format 3 must not be translated into any other PIN-block format other than ISO format 0 or ISO format 3. PINs enciphered using ISO format 1 may be translated into ISO format 0 or ISO format 3, but must not be translated back into ISO format 1.<br><br>
Translations between PIN-block formats that both include the PAN shall not support a change in the PAN. The PIN-translation capability between ISO formats 0 and 3 (including translations from ISO 0 format to ISO 0 format, or from ISO 3 format to ISO 3 format) must not allow a change of PAN.<br><br>
The following illustrates translations from formats 0, 1, and 3:
<table>
<tr><th colspan="4">Translation</th></tr>
<tr><th>To → / From ↓</th><th>ISO Format 0</th><th>ISO Format 1</th><th>ISO Format 3</th></tr>
<tr><td>ISO Format 0</td><td>Change of PAN not permitted</td><td>Not permitted</td><td>Change of PAN not permitted</td></tr>
<tr><td>ISO Format 1</td><td>PAN input</td><td>Permitted</td><td>PAN input</td></tr>
<tr><td>ISO Format 3</td><td>Change of PAN not permitted</td><td>Not permitted</td><td>Change of PAN not permitted</td></tr>
</table>
</td></tr>
</table>

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 4. PINs must not be stored except as part of a store-and-forward transaction, and only for the minimum time necessary. | Transactions may be stored and forwarded under certain conditions as noted in **ISO 9564**. PIN blocks, even encrypted, must not be retained in transaction journals or logs. PIN blocks are required in messages sent for authorization, but must not be retained for any subsequent verification of the transaction. PIN blocks may be temporarily stored as a system-recovery mechanism in order to recover authorization processing. For the storage of other data elements, see the *PCI Data Security Standards.* |
| 5. All keys and key components must be generated using an approved random or pseudo-random process. | Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys.<br><br>Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic-key generation relies upon good-quality, randomly generated values. An independent laboratory must certify self-developed implementations of a cryptographic pseudo-random number generator, which includes testing in accordance to the statistical tests defined in **NIST SP 800-22,** consistent with testing performed on PCI approved HSMs and POIs. |
| 6. Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals. | The output of the key-generation process must be monitored by at least two authorized individuals who can ensure there is no unauthorized tap or other mechanism that might disclose a clear-text secret or private key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.<br><br>Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.<br><br>Printed key components must be printed within blind mailers or sealed immediately after printing so that only the party entrusted with it can observe each component and so that tampering can be detected.<br><br>Any residue from the printing, export, display or recording process that might disclose a component must be destroyed before an unauthorized person can obtain it. |
| 7. Documented procedures must exist and be demonstrably in use for all key-generation processing. | Written key-creation procedures must exist and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of those procedures. All key-creation events must be documented. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 8. Secret or private keys shall be transferred by:<br>a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or<br>b. Transmitting the key in cipher-text form.<br>Public keys must be conveyed in a manner that protects their integrity and authenticity. | Specific techniques exist regarding transferring keys in order to maintain their integrity. An encryption key, typically a key-encryption key (KEK), must be transferred by physically forwarding the separate components of the key using different communication channels or transmitted in cipher-text form. Key components must be transferred in either tamper-evident, authenticable packaging or within an SCD. No person shall have access to any clear-text key during the transport process.<br>A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key. E.g., in an m-of-n scheme, such that any three key components or shares can be used to derive the key, no single individual can have access to more than two components/shares.<br>Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.<br>E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) has already been encrypted in accordance with these requirements—i.e., in an SCD. This is due to the existence of these key values in unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear text of any encrypted text or files conveyed through those systems.<br>Public keys must use a mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received. |
| 9. During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be:<br>a. Under the continuous supervision of a person with authorized access to this component, or<br>b. Locked in a security container (including tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, or<br>c. Contained within a physically secure SCD. | Key components are the separate parts of a clear-text key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, key components exist for KEKs, such as keys used to encrypt working keys for transport across some communication channel. Until such keys can be protected by encryption, or by inclusion in an SCD, the separate parts must be managed under the strict principles of dual control and split knowledge. Dual control involves 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 the materials involved. No single person shall be able to access or use all components or a quorum of shares of a single secret or private cryptographic key. Split knowledge is a condition under which two or more entities separately have key components that individually do not convey any knowledge of the resultant cryptographic key.<br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 9. *(Continued)* | Procedures must require that plain-text key components stored in tamper-evident, authenticable envelopes that show signs of tampering must result in the destruction and replacement of the set of components, as well as any keys encrypted under this key.<br><br>No one but the authorized key custodian (and designated backup) shall have physical access to a key component prior to transmittal or upon receipt of a component. Mechanisms must exist to ensure that only authorized custodians place key components into tamper-evident, authenticable packaging for transmittal and that only authorized custodians open tamper-evident, authenticable packaging containing key components upon receipt.<br><br>Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must exist to verify receipt of the appropriate bag numbers. |
| 10. All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed. | All DES keys used for encrypting keys for transmittal must be at least double-length keys and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.<br><br>RSA keys used to transmit or convey other keys must use a key modulus of at least 1024 bits. RSA keys encrypting keys greater in strength than double-length TDEA keys shall use a modulus of at least 2048 bits. An RSA key with a modulus of at least 1536 bits should be used to encipher double-length TDEA keys. RSA keys with a modulus of 2048 or higher should be used wherever both endpoints support those sizes.<br><br>In all cases, keys existing outside of an SCD must be protected by keys of equal or greater strength as delineated in Annex C. |
| 11. Documented procedures must exist and be demonstrably in use for all key transmission and conveyance processing. | Written procedures must exist and all affected parties must be aware of those procedures. Conveyance or receipt of keys managed as components or otherwise outside an SCD must be documented. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 12. Secret and private keys must be input into host hardware security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.<br>a. Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge.<br>b. Key-establishment techniques using public-key cryptography must be implemented securely. | The master file key and any key-encryption key, when loaded from the individual key components, must be loaded using the principles of dual control and split knowledge. Procedures must be established that will prohibit any one person from having access to all components of a single encryption key.<br><br>Key components shall be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components—for example, via XOR'ing. Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two eight-hexadecimal character halves to form a sixteen-hexadecimal secret key. The resulting key must exist only within the SCD.<br><br>Host security module (HSM) master file keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.<br><br>For manual key-loading, dual control requires split knowledge of the key among the entities. Manual key-loading may involve the use of media such as paper or specially designed key-loading hardware devices.<br><br>Any other SCD loaded with the same key components must combine all entered key components using the identical process.<br><br>The initial terminal master key (TMK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key may use asymmetric techniques, manual techniques, or the existing TMK to encrypt the replacement TMK for download. Keys shall not be reloaded by any methodology in the event of a compromised device, which must be withdrawn from use.<br><br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 12. *(Continued)* | TR-31 or an equivalent methodology should be used for key-loading whenever a symmetric key is loaded, encrypted by another symmetric key. This applies whether symmetric keys are loaded manually (i.e., through the keypad), using a key-injection device, or from a remote host. It does not apply when clear-text symmetric keys or their components are loaded using standard dual control techniques.<br><br>Any equivalent method must include the cryptographic binding of the key usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key must take place within the secure cryptographic boundary of the device.<br><br>Key-establishment protocols using public-key cryptography may also be used to distribute PED-symmetric keys. These key-establishment protocols may use either key transport or key agreement. In a key-transport protocol, the key is created by one entity and securely transmitted to the receiving entity. For a key-agreement protocol, both entities contribute information, which is then used by the parties to derive a shared secret key.<br><br>A public-key technique for the distribution of symmetric secret keys must:<br>▪ Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA).<br>▪ Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question.<br>▪ Provide for mutual device authentication for both the host and the PED or host to host if applicable, including assurance to the host that the PED actually has (or actually can) compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key.<br>▪ Meet all applicable requirements described in *Annex A* of this document. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 13. The mechanisms used to load secret and private keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component. | SCD equipment must be inspected to detect evidence of monitoring and to ensure dual control procedures are not circumvented during key-loading.<br><br>An SCD must transfer a plain-text secret or private key only when at least two authorized individuals are identified by the device—e.g., by means of passwords or other unique means of identification.<br><br>Plain-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that there is no tap at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys, and that the device has not been subject to any tampering that could lead to the disclosure of keys or sensitive data.<br><br>Non-SCDs shall not be used in the loading of clear-text secret or private keys or their components, outside of a secure key-loading facility, as delineated in Annex B. For example, ATM controller (computer) keyboards shall never be used for the loading of clear-text secret or private keys or their components.<br><br>The injection of key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) must result in either of the following:<br>▪ The medium is placed into secure storage, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device, *or*<br>▪ All traces of the component are erased or otherwise destroyed from the electronic medium.<br><br>For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:<br>▪ The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; *and*<br>▪ The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it; *and*<br>▪ The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs; *and*<br>▪ The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.<br><br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 13. *(Continued)* | The media upon which a component resides must be physically safeguarded at all times.<br><br>Any tokens, EPROMs, or other key component holders used in loading encryption keys must be maintained using the same controls used in maintaining the security of hard copy key components. These devices must be in the physical possession of only the designated component holder and only for the minimum practical time.<br><br>If the component is not in human comprehensible form (e.g., in a PROM module, in a smart card, on a magnetic-stripe card, and so forth), it must be in the physical possession of only one entity for the minimum practical time until the component in entered into an SCD.<br><br>If the component is in human-readable form (e.g., printed within a PIN-mailer type document), it must be visible only at one point in time to only one person (the designated component custodian) and only for the duration of time required for this person to privately enter the key component into an SCD.<br><br>Printed key-component documents must not be opened until just prior to entry.<br><br>The component must never be in the physical possession of an entity when any one such entity is or ever has been similarly entrusted with any other component of this same key. |
| 14. All hardware and passwords used for key-loading must be managed under dual control. | Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. Use of the equipment must be monitored and a log of all key-loading activities maintained for audit purposes. All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.<br><br>Passwords must be managed such that no single individual has the capability to enable key loading.<br><br>Any physical (e.g., brass) key(s) used to enable key-loading must not be in the control or possession of any one individual who could use those keys to load secret or private cryptographic keys under single control. |
| 15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised. | A cryptographic-based validation mechanism helps to ensure the authenticity and integrity of keys and components (e.g., testing key-check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See **ISO 11568**. Recorded or displayed key-component check values and key check values shall not exceed six hexadecimal characters in length.<br><br>The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plain-text form, must:<br><br>▪ Be within a certificate; or<br>▪ Be within a PKCS#10; or<br>▪ Be within a SCD; or<br>▪ Have a MAC (message authentication code) created using the algorithm defined in **ISO 9807.** |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 16. Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities. | Written procedures must exist and all parties involved in cryptographic key-loading must be aware of those procedures. All key-loading events must be documented. |
| 17. Unique secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations. | Where two organizations share a key to encrypt PINs (including key-encipherment keys used to encrypt the PIN-encryption key) communicated between them, that key must be unique to those two organizations and must not be given to any other organization.<br><br>This technique of using unique keys for communication between two organizations is referred to as "zone encryption" and is required. Keys may exist at more than one pair of locations for disaster recovery or load-balancing (e.g., dual processing sites). |
| 18. Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys. | Multiple synchronization errors in PIN translation may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted. Procedures for investigating repeated synchronization errors must exist to help reduce the risk of an adversary substituting a key known only to them.<br><br>To prevent substitution of a compromised key for a legitimate key, key-component documents that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.<br><br>TDEA keys should be managed as key bundles at all times, e.g., using TR-31. The bundle and the individual keys should:<br>▪ Have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source;<br>▪ Be used in the appropriate order as specified by the particular mode;<br>▪ Be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged; and<br>▪ Cannot be unbundled for any purpose. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 19. Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems. | Encryption keys must be used only for the purpose they were intended (e.g., key-encryption keys must not to be used as PIN-encryption keys). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.<br><br>MFKs and their variants used by host processing systems for encipherment of keys for local storage shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration.<br><br>Private keys shall be used only to create digital signatures and to perform decryption operations. Private keys shall never be used to encrypt other keys.<br><br>Keys must never be shared or substituted in a processor's production and test systems. Except by chance, keys used in production must never be used in testing and keys used in testing must never be used in production. |
| 20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device. | Any key used to encrypt a PIN in a PED must be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.<br><br>In a master/session key approach, the master key(s) and all session keys must be unique to each cryptographic device.<br><br>If a transaction-originating terminal interfaces with more than one acquirer, the transaction-originating terminal SCD must have a completely different and unique key or set of keys for each acquirer. These different keys, or set of keys, must be totally independent and not variants of one another.<br><br>Keys that are generated by a derivation process and derived from the same Base Derivation Key must use unique data for the derivation process so that all such cryptographic devices receive unique initial secret keys.<br><br>Entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring financial institutions must use different Base Derivation Keys for each financial institution. The processing entity may share one or more Base Derivation Keys for merchants that are sponsored by the same acquirer. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 21. Secret keys used for enciphering PIN-encryption keys, or for PIN encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge. | Effective implementation of these principles requires the existence of barriers beyond procedural controls to prevent any custodian (or non-custodian for any individual component) from gaining access to all key components. An effective implementation would have physically secure and separate locking containers that only the appropriate key custodian (and their designated backup) could physically access.<br><br>Components for a specific key that are stored in separate envelopes, but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers. Furniture-based locks or containers with a limited set of unique keys are not sufficient to meet the requirement for physical barriers.<br><br>Key components may be stored on tokens (e.g., PC cards, smart cards, and so forth). These tokens must be stored in a special manner to prevent unauthorized individuals from accessing the key components. For example, if key components are stored on tokens that are secured in safes, more than one person might have access to these tokens. Therefore, additional protection is needed for each token (possibly by using tamper-evident, authenticable envelopes) to enable the token's owner to determine whether a token was used by another person. In particular, key components for each specific custodian must be stored in separate secure containers.<br><br>If a key is stored on a token and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup) must have possession of both the token and its corresponding PIN.<br><br>Printed or magnetically recorded key components must reside only within tamper-evident, authenticable sealed envelopes so that the component cannot be ascertained without opening the envelope.<br><br>DES keys that are used to encipher other keys or to encipher PINs, and which exist outside of an SCD, must be enciphered using keys of equal or greater strength as delineated in Annex C. For example:<br><br>▪ The TDEA using at least double-length keys, or<br>▪ RSA using a key modulus of at least 1024 bits.<br><br>A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.<br><br>Symmetric secret keys may be enciphered using public-key cryptography for distribution to PEDs as part of a key-establishment protocol as defined in Requirement 12. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 22. Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key. | Key components must never be never reloaded when there is any suspicion that either the originally loaded key or the device has been compromised. If suspicious alteration is detected, new keys must not be installed until the SCD has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.<br><br>A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key.<br><br>Procedures must include a documented escalation process and notification to organizations that currently share or have previously shared the key(s). The procedures shall include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, and so forth.<br><br>The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.<br><br>Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.<br><br>Specific events must be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:<br>▪ Missing cryptographic devices<br>▪ Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries<br>▪ Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate<br>▪ Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities<br>▪ Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation.<br><br>*(Continued on next page)* |

<table>
<tr><th>PIN Security Requirement</th><th>International/Industry Standard(s)</th></tr>
<tr><td>22. (Continued)</td><td>If attempts to load a secret or private key or key component into a cryptographic device fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased or otherwise destroyed in the original device. Prolonged use of a key increases the risk of its cryptanalytic compromise, depending upon, for example, implementation, key length and availability of corresponding cipher texts/plain texts. Cryptoperiods for keys should be assigned to minimize this risk taking into account any additional risk associated with key changes. For example, recommended maximum cryptoperiods for the following TDES double-length keys, based on guidance in NIST SP800-57, ISO TR 14742 and NIST SP800-131 are:
<table>
<tr><th>Type of Key Exchange</th><th>Key Type</th><th>Cryptoperiod</th></tr>
<tr><td>Static</td><td>PEK</td><td>12 months</td></tr>
<tr><td>Dynamic</td><td>KEK</td><td>3 years</td></tr>
<tr><td>Dynamic</td><td>PEK</td><td>12 hours (or UKPT)</td></tr>
</table>
UKPT is the preferred option.</td></tr>
<tr><td>23. Key variants must be used only in devices that possess the original key. Key variants must not be used at different levels of the key hierarchy, e.g., a variant of a key-encipherment key used for key exchange must not be used as a working key or as a master-file key for local storage.</td><td>A secret key used to encrypt a PIN for interchange must never be used for any other cryptographic purpose. A key used to protect the PIN-encrypting key must never be used for any other cryptographic purpose other than key encipherment.<br><br>Variants of the same key may be used for different purposes. Any variant of the PEK or a key used to protect the PEK must be protected in the same manner i.e., under the principles of dual control and split knowledge.<br><br>An MFK used by host processing systems for encipherment of keys for local storage, and variants of the MFK must not be used external to the (logical) configuration that houses the MFK itself.</td></tr>
</table>

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 24. Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed. | Instances of keys that are no longer used or that have been replaced by a new key must be destroyed. Clear-text key components or shares maintained on paper must be burned, pulped, or shredded in a cross-cut shredder. Keys on other storage media types and in other permissible forms of a key instance (physically secured, enciphered, or components) must be destroyed following the procedures outlined in **ISO–9564** or **ISO–11568**. In all cases, a third party—other than the custodian—must observe the destruction and sign an affidavit of destruction.<br><br>The procedures for destroying keys that are no longer used or have been replaced by a new key must be documented.<br><br>Key-encipherment-key components used for the conveyance of working keys must be destroyed after successful loading and validation as operational. |
| 25. Access to secret and private cryptographic keys and key material must be:<br>a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.<br>b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. | Limiting the number of key custodians to a minimum helps reduce the opportunity for key compromise. In general, the designation of a primary and a backup key custodian for each component is sufficient. This designation must be documented by having each custodian sign a Key Custodian Form. The forms must specifically authorize the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them. Each custodian must sign a Key Custodian Form acknowledging these responsibilities before receiving custody of key components or enablers (for example, PINs) for keys or their components. Key custodians must be free from undue influence in discharging their custodial duties.<br><br>Key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual. For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme, such as 3 of 5 key shares, no more than two key custodians can report to the same individual. In all cases, neither the direct reports nor the direct reports in combination with their immediate supervisor shall possess a quorum of key components sufficient to form any given key. |
| 26. Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD. | At a minimum, the logs must include the date and time in/out, purpose of access, name and signature of custodian accessing the component, envelope number (if applicable). |
| 27. Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key. | The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as the primary keys. (See Requirement 21—i.e., within an SCD, unless encrypted or securely stored and managed using the principles of dual control and split).<br><br>Backups (including cloning) must require a minimum of two authorized individuals to enable the process.<br><br>***Note:***<br>*It is not a requirement to have backup copies of key components or keys.* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 28. Documented procedures must exist and be demonstrably in use for all key-administration operations. | Written procedures must exist and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as:<br>▪ Security awareness training<br>▪ Role definition—nominated individual with overall responsibility<br>▪ Background checks for personnel<br>▪ Management of personnel changes, including revocation of access control and other privileges when personnel move. |
| 29. PIN-processing equipment (e.g., PEDs and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the loading of cryptographic keys and that precautions are taken to minimize the threat of compromise once deployed. | HSMs and PEDs must be placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering or is not otherwise subject to misuse. To achieve this, controls must exist to protect secure cryptographic devices from unauthorized access before, during, and after installation. Access to all cryptographic hardware must be documented, defined, and controlled. Cryptographic devices **must not** use default keys or data. A documented security policy must exist that specifies personnel with authorized access to all secure cryptographic devices.<br><br>Unauthorized individuals must not be able to access, modify, or substitute any secure cryptographic device. A documented chain of custody must exist to ensure that all cryptographic hardware is controlled from its receipt through its installation and use. Controls must ensure that all installed hardware components are from a legitimate source.<br><br>Dual-control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or back-up devices. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted cryptographic devices but must not supplant the implementation of dual-control mechanisms.<br><br>This requires physical protection of the device up to the point of key-insertion or inspection, and possibly testing of the device immediately prior to key-insertion. Techniques include, but are not limited to, the following:<br><br>a. Cryptographic devices are transported from the manufacturer's facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.<br>b. Cryptographic devices are shipped from the manufacturer's facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident, authenticable packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs.<br><br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 29. *(Continued)* | c. The manufacturer's facility loads into each cryptographic device a secret, device-unique "transport-protection token." The SCD used for key-insertion has the capability to verify the presence of the correct "transport-protection token" before overwriting this value with the initial key that will be used.<br>d. Each cryptographic device is carefully inspected and perhaps tested immediately prior to key-insertion using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized modifications.<br>• Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised.<br>• Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.<br>Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:<br>▪ Protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it, and<br>▪ Detect lost or stolen equipment.<br>Procedures must include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.<br>Notwithstanding how the device is inspected and tested, it is mandatory to verify the device serial number against the purchase order, invoice, waybill, or similar document to ensure that device substitution has not occurred.<br>Documents used for this process must be received via a different communication channel—i.e., the control document used must not have arrived with the equipment.<br>PIN-processing equipment shall be used only for its specified purpose. It must not be possible for the equipment to be operated in an unauthorized manner or beyond the scope of the operating procedures specified for the equipment.<br>The security policy enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required in PIN-processing equipment to support specified functionality must be disabled before the equipment is commissioned. For example, PIN-change functionality or PIN-block format translation functionality may not need to be supported or can be limited.<br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 29. *(Continued)* | Physical and logical protections must exist for deployed POS devices. For example, as delineated in the PCI SSC *Skimming Prevention – Best Practices for Merchants* document:<br>▪ Deployed devices are physically mounted or tethered to prevent removal<br>▪ Implementation of a terminal authentication system whereby the host system continuously verifies that terminals are online and operating correctly. If a terminal is ever replaced with an unauthorized device (or is unplugged, as would be necessary to execute this attack), the host system would immediately be aware of tampering. |
| 30. Procedures must exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service. | If an SCD has been removed from service, all keys stored within the device that have been used (or potentially could be) for any cryptographic purpose must be destroyed.<br>▪ All critical initialization, deployment, usage, and decommissioning processes must impose the principles of dual control and split knowledge (e.g., key- or component-loading, firmware- or software-loading, and verification and activation of anti-tamper mechanisms).<br>▪ Key and data storage must be zeroized when a device is decommissioned.<br>If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys. |
| 31. Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:<br>a. Dual access controls are required to enable the key-encryption function.<br>b. Physical protection of the equipment (e.g., locked access to it) under dual control.<br>c. Restriction of logical access to the equipment. | Cryptographic equipment must be managed in a secure manner in order to minimize the opportunity for key compromise or key substitution. Physical keys, authorization codes, passwords, or other enablers must be managed so that no one person can use both the enabler(s) and the device which can create cryptograms of known keys or key components under a key-encipherment key used in production.<br>Unauthorized use of secure cryptographic devices (including key-loading devices) shall be prevented or detected by all of the following:<br>▪ The device is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected;<br>▪ The device has functional or physical characteristics (e.g., passwords or physical high-security keys) that prevent use of the device except under the dual control of at least two authorized people; and when in a state in which it is useable, the device is under the continuous supervision of at least two such people who ensure that any unauthorized use of the device would be detected.<br>*(Continued on next page)* |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 31. *(Continued)* | Network access to the device is based on the following controls:<br>▪ **PCI DSS:** The network shall meet any PCI DSS compliance requirements.<br>▪ **Network separation:** The HSM production network shall be logically and physically separate from any other business networks.<br>▪ **Firewalls (Hardware or Software)**: The HSM production network should use a nested firewall configuration with an external and inner network boundary, protected by a firewall and coupled with an IDS.<br>▪ **Access controls**: Authorized access to logical and physical components of the HSM production network shall be based on timed access and dual control. It is strongly recommended that devices and applications be set with the most stringent logical access control settings where applicable. Access-control settings shall be specified for production domains, servers, proxy servers, firewalls, routers, organizational units (OUs) and other protected resources.<br>▪ **IDS (Intrusion-detection system):** The HSM network environment shall be monitored using IDS on a 24/7 basis. Monitoring, as a minimum, should include normal and exception reporting on personal access, violation of established protocols and processes that affect the HSMs, for example: unusual/out of pattern access events, software/firmware loads, HSM velocity checking.<br>▪ **VPN (Virtual Private Networks)**: Separate internal IP addresses and/or separate VPNs should be applied to HSM production networks where direct cabling or device isolation into a single physical location is not practical. Encrypted VPN solutions should be used to separate the production network platform from any other internal network.<br>▪ **Logging and auditing**: 24/7 logging and reviews of audit trails shall be implemented for devices and any platforms that support the production network, for example ACL's (access-control lists), organizational units (OUs) and other protected resources.<br>▪ **Staff**: It is strongly recommended that patch management, database administration or system administration services are conducted for the HSM production environment under dual control and authorized/monitored by the appropriate network security management personnel. |

| PIN Security Requirement | International/Industry Standard(s) |
|---|---|
| 32. Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned. | Written procedures must exist and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections given to PIN-processing devices before they are placed into service, as well as devices being decommissioned.<br><br>Procedures that govern access to HSMs must be in place and known to data center staff and any others involved with the physical security of such devices.<br><br>HSM security policies/configurations must be validated to secure settings at least annually. For example, PIN-block formats without a defined business need must be disabled in accordance with Requirement 3.<br><br>HSMs used for acquiring functions should not also be used for issuing functions. Acquiring and issuing functionality should be logically segmented within a given network. HSMs used for acquiring functions shall not be configured to output clear-text PINs. |

# Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques

This normative annex contains detailed requirements that apply to remote key-establishment and distribution applications and is in addition to key- and equipment-management criteria stated in the main body of the *PCI PIN Security Requirements*. Remote key-distribution schemes should be used for initial key-loading only, i.e., establishment of the TDES key hierarchy, such as a terminal master key. Standard symmetric key-exchange mechanisms should be used for subsequent TMK, PEK, or other symmetric key exchanges, except where a device requires a new key-initialization due to unforeseen loss of the existing TMK. Using asymmetric techniques for routine key exchange can result in unnecessary exposure to man-in-the-middle attacks and should not be used.

These requirements pertain to two distinct areas.

1. Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.
2. Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key-distribution using asymmetric techniques.

Certification Authority requirements apply to all entities (acquirers, manufacturers, key-distribution hosts (KDH), and other third parties) signing public keys to be used for remote distribution of cryptographic keys, whether in X.509 certificate-based schemes or other designs, to allow for the required authentication of these signed public keys. For purposes of these requirements, a certificate is any digitally signed value containing a public key, where the term "digitally signed" refers to any cryptographic method used to enforce the integrity and authenticity of a block of data through the encryption of a whole or digest of that block of data with a private key. The CA requirements apply only to methods that allow for the distribution and use of such signed keys to multiple systems, and as such do not apply to systems that apply symmetric cryptography to keys for authentication (such as through the use of MACs or CMACs).

The Certificate Authority requirements are not intended to be applied to devices that sign their own keys, nor to key-loading systems where the key loading is not performed remotely and authentication is provided by another method (such as properly implemented dual control and key-loading device(s))— even if these systems involve the use of certificates.

Requirements below that pertain only to Certification and Registration Authority operations are designated CA/RA.

The control objectives and security requirements are delineated as found in the preceding "Technical Reference" section of this document, and are in addition to those requirements.

| Objective | Additional Security Requirements |
|---|---|
| **Objective 1** | ***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.*** |
| | No additional security requirements added for "Symmetric Key Distribution using Asymmetric Techniques". |
| **Objective 2** | ***Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.*** |
| 5. All keys and key components must be generated using an approved random or pseudo-random process. | Key pairs must be generated using a random or pseudo-random process in accordance with PCI requirements as defined in the *Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements.* Key-generation methods must meet the current ANSI and ISO standards for the algorithm(s) in question.<br>Secret and private cryptographic keys must be unique and are equally likely to be generated. The probability that any two cryptographic keys must be identical is negligible. |
| 6. Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals. | For use by a device, key pairs must be:<br>a. Generated by the device itself, or<br>b. Generated externally, in which case the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after transfer to the device. |

<table>
<tr><th>Objective</th><th>Additional Security Requirements</th></tr>
<tr><td>Objective 3</td><td>Keys are conveyed or transmitted in a secure manner.</td></tr>
<tr><td>10. All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.</td><td>Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used.<br><br>The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used for key transport, exchange or establishment:<br><br>
<table>
<tr><th>Algorithm</th><th>DES</th><th>RSA</th><th>Elliptic Curve</th><th>DSA</th><th>AES</th></tr>
<tr><td>Minimum key size in number of bits:</td><td>112</td><td>1024</td><td>160</td><td>1024/160</td><td>128</td></tr>
</table>
<br>DES refers to TDES keys with non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.<br><br>For Diffie-Hellman implementations:<br>
▪ Entities must securely generate and distribute the system-wide parameters: generator g, prime number p and parameter q, the large prime factor of (p - 1). As described in ANSI X9.42, parameter p must be at least 1024 bits long, and parameter q must be at least 160 bits long. Each entity shall generate a private key x and a public key y using the domain parameters (p, q, g,). Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in the Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements .<br>
▪ Entities must authenticate the Diffie-Hellman public keys using DSA, a certificate, or a symmetric MAC. (Based on TDES. See ISO 16609 – Banking – Requirements for message authentication using symmetric techniques; Method 3 should be used).<br>
▪ RSA keys encrypting keys greater in strength than double-length TDEA keys shall use a modulus of at least 2048 bits. An RSA key with a modulus of at least 1536 bits should be used to encipher double-length TDEA keys.</td></tr>
</table>

| Objective | Additional Security Requirements |
|---|---|
| **Objective 4** | ***Key-loading to hosts and PIN entry devices is handled in a secure manner.*** |
| 15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised. | The devices (EPPs/PEDs and key-distribution hosts (KDHs)) involved in using public-key schemes must check the validity of other such devices involved in the communication prior to any key transport, exchange or establishment. Validation of authentication credentials must occur immediately prior to any key-establishment, including both initial and any subsequent key exchanges. Examples of this kind of validation include checking current certificate revocation lists or embedding valid authorized key-distribution host certificates in EPPs/PEDs and disallowing communication with unauthorized key-distribution hosts, as delineated by techniques defined in the Technical FAQs for *PCI PTS POI Security Requirements.*<br><br>Mechanisms must exist to prevent a non-authorized host from performing key transport, key exchange or key establishment with EPPs/PEDs. An example of this kind of mechanism is through limiting communication between the EPP/PED and hosts to only those hosts contained in a list of valid hosts managed by the EPP/PED.<br><br>Within an implementation design, there shall be no means available for "man in the middle" attacks on the ongoing key exchanges between an EPP/PED and the KDH. System implementations must be designed and implemented to prevent replay attacks.<br><br>Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device and must provide for key protection in accordance with this document. That is, the secrecy of the private key and the integrity of the public key must be ensured. |
| **Objective 5** | ***Keys are used in a manner that prevents or detects their unauthorized usage.*** |
| 18. Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys. | EPPs/PEDs shall only communicate with CAs for the purpose of certificate signing, or for key-injection where the certificate-issuing authority generates the key pair on behalf of the EPP/PED; and with KDHs for key management, normal transaction processing and certificate (entity) status checking.<br><br>KDHs shall only communicate with EPPs/PEDs for the purpose of key management and normal transaction processing; and with CAs for the purpose of certificate signing and certificate (entity) status checking. |

| Objective | Additional Security Requirements |
|---|---|
| 19. Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems. | Key pairs shall not be reused for certificate renewal or replacement. Only one certificate shall be issued per key pair. Certificates for a key pair shall not be renewed using the same keys.<br><br>Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose I.e., keys are used in accordance with their certificate policy—see RFC 3647- *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.<br><br>▪ CA/RA: Certification authority (CA) certificate/certificate (entity) status checking (for example CRL) signature keys, or signature keys for updating valid/authorized host lists in EPPs/PEDs shall not be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates. The keys used for certificate signing and certificate (entity) status checking (and if applicable, self-signed roots) may be for combined usage, or may exist as separate keys dedicated to either certificate signing or certificate (entity) status checking.<br>▪ CA/RA: CAs that issue certificates to other CAs must not be used to issue certificates to EPPs or PEDs.<br>▪ Public keys are used only for either encryption or for verifying digital signatures, but not both (except for EPPs/PEDs).<br>▪ Private keys can only be used for decryption or for creating digital signatures, but not both (except for EPPs/PEDs).<br><br>Public-key-based implementations must provide mechanisms for restricting and controlling the use of public and private keys. For example, this can be accomplished through the use of X.509 compliant certificate extensions.<br><br>CA and KDH private keys must not be shared between devices except for load-balancing and disaster recovery. EPP and POS PED private keys must not be shared.<br><br>***Note:*** *If a business rationale exists, a production platform (HSMs and servers/stand-alone computers) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the CA and RA server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.*<br><br>*At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.* |

| Objective | Additional Security Requirements |
|---|---|
| 20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device. | Keys must be uniquely identifiable in all hosts and EPPs/PEDs. Keys must be identifiable via cryptographically verifiable means (e.g., through the use of digital signatures or key check values).<br><br>Key pairs must be unique per device including key-distribution hosts (except as otherwise provided for), EPPs and POS PEDs. |
| **Objective 6** | ***Keys are administered in a secure manner.*** |
| 21. Secret keys used for enciphering PIN-encryption keys, or for PIN encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge. | Private keys used to sign certificates, certificate status lists, messages or for secret-key protection must exist only in one of the following forms:<br>▪ Within a secure cryptographic device, e.g., an HSM or EPP/PED that meets applicable PCI requirements for such a device,<br>▪ Encrypted using an algorithm and key size of equivalent or greater strength, or<br>▪ As components using a recognized (e.g., Shamir) secret sharing scheme. |

| Objective | Additional Security Requirements |
|---|---|
| 22. Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key. | **CA/RA – All apply**<br><br>In order to provide for continuity of service in the event of the loss of a root key (e.g., through compromise or expiration), a key-distribution management system and the associated end entities (EPPs, KDHs, POS PEDs) should provide support for more than one root.<br><br>Root CAs must provide for segmentation of risk to address-key compromise. An example of this would be the deployment of subordinate CAs.<br><br>Mechanisms must be in place to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke subordinate certificates and notify affected entities.<br><br>The CA must cease issuance of certificates if a compromise is known or suspected and perform a damage assessment, including a documented analysis of how and why the event occurred. In the event of the issuance of phony certificates with the compromised key, the CA shall determine whether to recall and reissue all signed certificates with a newly generated signing key. Mechanisms (e.g., digital time-stamping) must exist to ensure that phony certificates cannot be successfully used.<br><br>The compromised CA must notify any superior or subordinate CAs of the compromise. Subordinate CAs and KDHs should have their certificates reissued and distributed to them or be notified to apply for new certificates.<br><br>Minimum cryptographic strength for the CA system shall be:<br><br>▪ Root – minimum RSA 2048 bits or equivalent;<br>▪ Subordinate CAs, EPP/PED devices and KDHs – minimum RSA 1024 bits or equivalent.<br><br>The following key-pair lifecycle shall exist:<br><br>▪ Expiration of EPP/PED keys within twelve (12) months after the device's expected end-of-life;<br>▪ Expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key. |

| Objective | Additional Security Requirements |
|---|---|
| 25. Access to secret or private cryptographic keys and key material must be:<br>a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.<br>b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. | **CA/RA – All apply**<br><br>Logical security controls for systems protect from unauthorized access, modification, substitution, insertion or deletion. All user access shall be directly attributable to an individual user—e.g., through the use of unique IDs—and be restricted to actions authorized for that role through the use of a combination of CA software, operating system and procedural controls.<br><br>The system enforces an explicit and well-defined and documented certificate security policy and certification practice statement. This must include that:<br><br>▪ CA systems that issue certificates to other CAs or to KDHs, must be operated offline using a dedicated closed network (not a network segment). The network is used only for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access shall exist only for the purposes of "pushing" certificate status information to relying parties (e.g., EPPs, KDHs, POS PEDs).<br>▪ No CA or Registration Authority (RA) software updates are done over the network (local console access must be used for CA or RA software updates).<br>▪ Non-console access requires two-factor authentication. This also pertains to the use of remote console access.<br>▪ Remote user access to the CA or RA system environments shall be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.<br>▪ CA certificate (for EPP/PED/KDH authentication and validity status checking) signing keys must be enabled using a minimum of at least dual control.<br>▪ Certificate requests may be vetted (approved) using single user logical access to the RA application.<br><br>The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection; the practice referred to as dual control. At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).<br><br>For systems accessible via non-local console access, the operating system(s) utilized must be hardened. Services that are not necessary or that allow nonsecure access (e.g., rlogin, rshell, etc. commands in UNIX) must be removed or disabled. Unnecessary ports must also be disabled. Documentation must exist to support the enablement of all active services and ports.<br><br>*(Continued on next page)* |

| Objective | Additional Security Requirements |
|---|---|
| Objective 6, Item 25<br>*(Continued)* | Vendor default IDs which are required only as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason. Vendor default IDs such as "Guest" must be removed or disabled. Default passwords must be changed during initial installation.<br><br>Audit trails must include, but not be limited to all key-management operations, such as key generation, backup, recovery, compromise, and destruction and certificate generation or revocation, together with the identity of the person authorizing the operation and persons handling any key material (such as key components or keys stored in portable devices or media). The logs must be protected from alteration and destruction, and archived in accordance with all regulatory and legal requirements.<br><br>Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.<br><br>Logical events are divided into operating system and CA application events. For both events the following must be recorded in the form of an audit record:<br>▪ Date and time of the event,<br>▪ Identity of the entity and/or user that caused the event,<br>▪ Type of event, and<br>▪ Success or failure of the event.<br><br>CA application logs must use a digital signature or a symmetric MAC (based on TDES – see *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for protection from alteration. The signing/MACing key(s) used for this must be protected using a secure cryptographic device.<br><br>Components of the system operated online, for example the RA, must include for operational support the use of pass phrase management techniques encompassing at a minimum the following:<br>▪ Minimum length of eight characters using a mix of alphabetic, numeric, and special characters.<br>▪ System enforced expiration life not to exceed thirty days.<br>▪ System enforced minimum life of at least one day.<br>▪ Maximum invalid attempts not to exceed five before suspending the user ID.<br>▪ System-enforced pass-phrase history preventing the reuse of any pass phrase used in the last twelve months.<br>▪ Initial, assigned pass phrases are pre-expired (user must replace at first logon).<br><br>*(Continued on next page)* |

| Objective | Additional Security Requirements |
|---|---|
| Objective 6, Item 25<br>*(Continued)* | ▪ Vendor-default pass phrases are changed at installation and, where applicable, for updates.<br>▪ Pass phrases are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.<br>▪ The embedding of pass phrases in shell scripts, command files, communication scripts, etc., is strictly prohibited.<br><br>Log-on security tokens (e.g., smart cards) and cryptographic devices are not subject to the pass phrase management requirements for maximum and minimum lives as stated above. Security tokens must have an associated usage-authentication mechanism, such as biometrics or associated PINs/pass phrases, to enable their usage. Where PINs/pass phrases are used, they must be at least eight characters. |
| 28. Documented procedures must exist and be demonstrably in use for all key-administration operations. | **CA/RA – All apply**<br><br>CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.<br><br>The certificate issuing and management authority may consist of one or more devices that are responsible for the issuance, revocation, and overall management of certificates and certificate status information.<br><br>Each CA operator **must** develop a certification practice statement (CPS)—see RFC 3647- *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content—that can be reviewed by the payment brands. This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific single document or a collection of specific documents. The CPS must be consistent with the requirements described within this document. The CA shall operate in accordance with its CPS.<br><br>Documented procedures must exist and be demonstrably in use by CAs to validate the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.<br><br>For CA and KDH certificate signing requests, including certificate or key validity status changes (e.g., revocation. suspension, replacement), verification must include validation that:<br>▪ The entity submitting the request is who it claims to be.<br>▪ The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity.<br>▪ The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested.<br>▪ The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.<br>▪ The RA will retain documentation and audit trails relating to the identification of entities for all certificates issued and certificates whose status had changed for the life of the associated certificates. |

| Objective | Additional Security Requirements |
|---|---|
| **Objective 7** | ***Equipment used to process PINs and keys is managed in a secure manner.*** |
| 31. Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:<br>a. Dual access controls are required to enable the key-encryption function.<br>b. Physical protection of the equipment (e.g., locked access to it) under dual control.<br>c. Restriction of logical access to the equipment. | **CA/RA** – **All apply**<br>CA and RA database and application servers, and cryptographic devices must reside in a physically secure and monitored environment.<br>The physically secure environment must restrict access to only authorized personnel. The physically secure environment must have an intrusion-detection system and restricted access via, for example, locks or tokens.<br>Documented procedures must exist for the granting and revocation of access privileges, which include reviewing manual or electronic logs of accesses. Specifically, Certificate Processing operations must:<br>▪ Operate in a physically secure dedicated room not used for any other business activities but certificate operations (stand-alone).<br>▪ Provide for the documentation of all access granting, revocation, and review procedures and of specific access authorizations, whether logical or physical.<br>▪ Require dual-control access. The room must never be occupied by a single individual for more than thirty (30) seconds. The enforcement mechanism must be automated. The system must enforce anti-pass-back.<br>▪ Use electronically (e.g., badge and/or biometric) managed dual occupancy.<br>▪ Allow access only to pre-designated staff with defined business needs and duties. Visitors must be authorized and escorted at all times.<br>▪ Use CCTV monitoring (motion-activated systems that are separate from the intrusion-detection system may be used) of the CA operating platform that must record to time-lapse VCRs or similar mechanisms. Surveillance cameras must not be configured to allow the monitoring of computer screens, keyboards, PIN pads, etc.<br>*(Continued on next page)* |

| Objective | Additional Security Requirements |
|---|---|
| Objective 7, Item 31 *(Continued)* | ▪ Require that personnel with access to the physically secure environment must not have access to the media (e.g., VCR tapes, digital recording systems, etc.) with the recorded surveillance data. Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. Systems using digital recording mechanisms must have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.<br>▪ Provide for continuous (motion activated systems may be used) lighting for cameras.<br>▪ Have a 24/7 intrusion-detection system for the physically secure environment. Protect the secure area by motion detectors when unoccupied. This must be connected to the alarm system and automatically activated every time all authorized personnel have exited the secure area. Any windows in the secure area must be locked, protected by alarmed sensors, or otherwise similarly secured.<br>▪ Use access logs to record personnel entering the secure room, including documented reasons for the access. The logs may consist of either electronic, manual, or both. Visitors must sign an access log detailing name, organization, date, time in and out, and purpose of visit. The person escorting the visitor must also initial the log.<br>▪ Tie all access-control and monitoring systems to an uninterruptible power source (UPS).<br>▪ Document all alarm events. Under no circumstances shall an individual sign off on an alarm event in which they were involved.<br>▪ Establish that the use of any emergency entry or exit mechanism must cause an alarm event.<br>▪ Require that all alarms for physical intrusion necessitate an active response by personnel assigned security duties within 30 minutes.<br>▪ Implement a process for synchronizing the time and date stamps of the access, intrusion-detection and monitoring (camera) systems to ensure accuracy of logs. This may be done by either automated or manual mechanisms. If a manual process is utilized, the process must occur at least quarterly. Documentation of the synchronization must be retained for at least a one-year period.<br>*(Continued on next page)* |

| Objective | Additional Security Requirements |
|---|---|
| Objective 7, Item 31 *(Continued)* | Root CAs and their equivalent operations must exist only in a high security environment.<br><br>CAs and their associated RA servers that issue certificates to Key-distribution Hosts or subordinate CAs must additionally meet the following:<br>▪ The physically secure environment must have true floor-to-ceiling (slab-to-slab) walls. Alternatively, solid materials, steel mesh, or bars may be utilized below floors and above ceilings to protect against intrusions—e.g., a caged environment.<br>▪ This physically secure environment must have a 24/7 intrusion-detection system:<br>• The intrusion-detection system must have 24-hour monitoring (including UPS).<br>• The intrusion-detection system must include the use of motion sensors.<br>• The system must be capable of and perform recording and archiving of alarm activity.<br>• Alarm activity must include unauthorized entry attempts or any deliberate or inadvertent actions that disable the intrusion-detection system.<br>• All logged alarm activity information must be reviewed and resolved.<br>▪ One or more cameras must provide continuous (motion-activated systems that are separate from the intrusion-detection system may be used) monitoring of entry and exit to the physically secure environment. Lighting must exist for the camera images. Recording must be at a minimum of five frames equally every three seconds.<br>▪ Use three layers of physical security in the CA facility with increasing levels of access control for each of the following levels:<br>**Level One Barrier:**<br>This level consists of the entrance to the facility. The building or secure facility entrance will allow the entrance of only authorized personnel to the facility. A guarded entrance or foyer with a receptionist requires the use of a logbook to register authorized visitors (guests) to the facility.<br>**Level Two Barrier:**<br>This level secures the entrance beyond the foyer/reception area to the CA facility. This entrance must be monitored by a video recording system and require secure entry of authorized personnel only. All entry through this barrier must be logged. Single entry into this barrier is allowed. Authorized visitors must be escorted at all times when within this barrier and beyond.<br><br>*(Continued on next page)* |

| Objective | Additional Security Requirements |
|---|---|
| Objective 7, Item 31 *(Continued)* | **Level Three Barrier:**<br>This level provides access to the dedicated room housing the CA and signing engines. This entrance requires dual access. Personnel with access must be divided into an "A" group and a "B" group, such that access requires at least one member from each group. The A and B groups must correlate to separate organizational units.<br>Doors must have locks and all authorized personnel having access through this barrier must have successfully completed a background security check and are assigned resources (staff, dedicated personnel) of the CA operator. Other personnel that require entry to this level must be accompanied by two (2) authorized and assigned resources at all times.<br>CA Personnel (authorized individuals with a formal PKI role) entering the physically secure CA environment must sign an access logbook. This log must be maintained within the CA room. This logbook must include:<br>▪ Name and signature of the individual,<br>▪ Participant's organization,<br>▪ Date and time in and out, and<br>▪ Reason for visit.<br>Visitors (contractors, maintenance personnel, etc.) must also sign an access logbook. In addition to the aforementioned, the logbook for visitor access must include name and signature of the individuals escorting the visitor.<br>Access to the room creates an audit event, which must be logged. Motion sensors must be in place to activate cameras (if cameras are not recording all activity continually). Invalid access attempts also create audit records, which must be followed up on by security personnel.<br>Automated login and logout enforcement of personnel is required at Level Three. This area must never be occupied by less than two persons except during the time of login and logout. This period for entrance and egress will not exceed 30 seconds. For time of single occupancy exceeding 30 seconds, the system must automatically generate an audit event that must be followed up on by security personnel. |

# Normative Annex B – Key-injection Facilities

## *Key-Injection Facility Security Requirements Technical Reference*

## Introduction

This technical reference contains the specific requirements that apply to key-injection facilities, and includes applicable criteria from the main body of the *PCI PIN Security Requirements.* Furthermore, it provides implementation criteria on how the requirements can be realized. Other implementation methods may be considered, assuming that they provide at least the same level of security.

This Technical Reference refers to Triple-DES (TDEA) with at least double-length keys as the cryptographic standard for PIN encryption. However, defining the schedule for the migration from single-DES to triple-DES is reserved to the payment brands. The Advanced Encryption Standard may be used in place of TDES for key-management purposes.

***Note:***

*From time to time, the standards change in order to more completely reflect the state of both technology and the threat environment at a particular point in time. It is necessary to ensure that the correct Technical Reference is used when evaluating whether a process, technique, piece of equipment, or policy is compliant with a specific requirement.*

Key-injection systems that allow clear-text secret and/or private keys and/or their components to appear in unprotected memory (e.g., within a computer and outside of the secure boundary of a secure cryptographic device) are inherently less secure. Any such systems are subject to additional controls as delineated in the criteria in this annex. The payment brands may establish dates by which all key-injection facilities providing key-injection services to multiple entities shall have to use secure cryptographic hardware for key-injection.

Key-injection facilities that are engaged in either or both of the following must also meet the criteria delineated in Annex A:

1. Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.
2. Remote distribution of symmetric keys using asymmetric techniques to transaction originating devices. These criteria pertain to the characteristics of the actual key-distribution methodology implemented.

## Requirement/Standards Cross-Reference

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 1. All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD. SCDs are considered tamper-responsive or physically secure devices: penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys and all useful residues of PINs and keys contained within it.<br><br>All newly deployed ATMs and POS PIN-acceptance devices must be compliant with the applicable *PCI Point of Interaction Security Requirements*. Newly deployed hardware security modules (HSMs) should be PCI approved. For specific considerations, contact the payment brand(s) of interest. | Key-injection facilities must only inject keys into equipment that conforms to the requirements for SCDs.<br><br>Key-injection platforms and systems that include hardware devices for managing (e.g., generating and storing) the keys must ensure those hardware devices conform to the requirements for SCDs.<br><br>A secure cryptographic device (SCD) must meet the requirements of a Physically Secure Device as defined in **ISO 9564**. Such a device must have a negligible probability of being successfully penetrated to disclose all or part of any secret or private cryptographic key or PIN. A SCD shall only be used after it has been determined that the device's internal operation has not been modified to allow penetration (e.g., the insertion within the device of an active or passive "tapping" mechanism). An SCD (e.g., a PIN entry device (PED)) that complies with this definition may use a Fixed Key or a Master Key/Session Key key-management technique, that is, a unique (at least) double-length PIN-encryption key for each PED, or may use double-length key DUKPT as specified in **ANSI X9.24-Part 1**.<br><br>An SCD relying upon compromise-prevention controls requires that penetration of the device when operated in its intended manner and environment shall cause the automatic and immediate erasure of all PINs, secret or private cryptographic keys, and other secret values, and any useful residuals of those contained within the device. These devices must employ physical barriers so that there is a negligible probability of tampering that could successfully disclose such a key.<br><br>Purchase orders for point-of-interaction PIN-acceptance devices must specify compliance to the applicable *PCI Point of Interaction Security Requirements*. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 5. All keys and key components must be generated using an approved random or pseudo-random process. | Where the key-injection platform includes features that generate keys, those keys must be generated in compliance with these requirements.<br><br>Some key-injection platforms may only "import" key components (instead of generating them), and those imported key components must be generated in accordance with the *PCI PIN Security Requirements*.<br><br>Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys.<br><br>Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values. An independent laboratory must certify self-developed implementations of a cryptographic pseudo-random number generator, which includes testing in accordance to the statistical tests defined in **NIST SP 800-22** consistent with testing performed on PCI approved HSMs and POIs. |
| 6. Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals. | Key-injection facilities must implement procedures to protect the key-generation process such that compromise of a key during its creation is not possible without collusion between at least two trusted individuals. Procedures must be in place to ensure that no one person can singly inject keys into devices. Procedures and physical and logical barriers must exist to prevent and detect compromise of the key-generation process.<br><br>Some key-injection platforms use personal-computer (PC)-based software applications whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of a SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key-injection facilities that use PC-based key-loading software platforms that allow clear-text secret and/or private keys and/or their components to exist in unprotected memory must at a minimum implement the compensating controls outlined in Requirement 13.<br><br>The output of the key-generation process must be monitored by at least two authorized individuals who can ensure there is no unauthorized tap or other mechanism that might disclose a clear-text secret or private key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.<br><br>Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.<br><br>Printed key components must be printed within blind mailers or sealed immediately after printing so that only the party entrusted with it can observe each component and so that tampering can be detected.<br><br>Any residue from the printing, export, display or recording process that might disclose a component must be destroyed before an unauthorized person can obtain it. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 7. Documented procedures must exist and be demonstrably in use for all key-generation processing. | Written key-creation procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of those procedures. All key-creation events performed by a key-injection facility must be documented. |
| 8. Secret or private keys must be transferred by:<br>a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, **or**<br>b. Transmitting the key in cipher-text form.<br>Public keys must be conveyed in a manner that protects their integrity and authenticity. | Keys conveyed *to* a key-injection facility must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:<br>▪ Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method,<br>▪ Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf or from a merchant to a third party that is performing key-injection on their behalf),<br>▪ Terminal master keys (TMKs) used in the master key/session key key-management method,<br>▪ PIN-encryption keys used in the fixed-transaction key method,<br>▪ Public keys used in remote key-establishment and distribution applications.<br>Keys conveyed *from* a key-injection facility (including facilities that are device manufacturers) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:<br>▪ Digitally signed HSM-authentication public key(s) that are signed by a device manufacturer's private key and subsequently loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable),<br>▪ Device manufacturer's authentication key loaded into the HSM for supporting certain key-establishment and distribution applications protocols (if applicable).<br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 8. *(Continued)* | Specific techniques exist in how keys must be transferred in order to maintain their integrity. An encryption key, typically a key-encryption key (KEK), must be transferred by physically forwarding the separate components of the key using different communication channels or transmitted in cipher-text form. Key components must be transferred in either tamper-evident, authenticable packaging or within an SCD. No person shall have access to any clear-text key during the transport process.<br><br>A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares sufficient to form the necessary threshold to derive the key. E.g., in an m-of-n scheme, such that any three key components or shares can be used to derive the key, no single individual can have access to more than two components/shares.<br><br>E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) has already been encrypted in accordance with these requirements, i.e., in an SCD. This is due to the existence of these key values in unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear text of any encrypted text or files conveyed through those systems. Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.<br><br>Public keys must use a mechanism independent of the actual conveyance method to validate that the correct key was received. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 9. During its transmission, conveyance, or movement between any two organizational entities any single, unencrypted secret or private key component must at all times be:<br>a. Under the continuous supervision of a person with authorized access to this component, **or**<br>b. Locked in a security container (including tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, **or**<br>c. Contained within a physically secure SCD. | Key components conveyed to and from a key-injection facility must be conveyed in compliance with these requirements. Such key components include but are not limited to those for Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf), or key components for the BDKs themselves, and terminal master keys used in the master key/session key key-management method.<br>Key components are the separate parts of a clear-text key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, key components exist for KEKs, such as keys used to encrypt working keys for transport across some communication channel. Until such keys can be protected by encryption, or by inclusion in an SCD, the separate parts must be managed under the strict principles of dual control and split knowledge. Dual control involves a process of using two or more separate entities (usually persons), which are operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of the materials involved. No single person shall be able to access or use all components or a quorum of shares of a single secret or private cryptographic key. Split knowledge is a condition under which two or more entities separately have key components that individually do not convey any knowledge of the resultant cryptographic key.<br>Procedures must require that plain-text key components stored in tamper-evident, authenticable envelopes that show signs of tampering must result in the destruction and replacement of the set of components, as well as any keys encrypted under this key.<br>No one but the authorized key custodian (and designated backup) shall have physical access to a key component prior to transmittal or upon receipt of a component. Mechanisms must exist to ensure that only authorized custodians place key components into tamper-evident, authenticable packaging for transmittal and that only authorized custodians open tamper-evident, authenticable packaging containing key components upon receipt.<br>Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must exist to verify receipt of the appropriate bag numbers. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 10. All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed. | Key-encryption keys used to convey keys to a key-injection facility must be (at least) as strong as any key transmitted or conveyed. Such keys include key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf).<br>All DES keys used for encrypting keys for transmittal must be at least double-length keys and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment. A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.<br>RSA keys used to transmit or convey other keys must use a key modulus of at least 1024 bits. RSA keys encrypting keys greater in strength than double-length TDEA keys shall use a modulus of at least 2048 bits. An RSA key with a modulus of at least 1536 bits should be used to encipher double-length TDEA keys. RSA keys with a modulus of 2048 or higher should be used wherever both endpoints support those sizes.<br>In all cases, keys existing outside of an SCD must be protected by keys of equal or greater strength as delineated in Annex C. |
| 11. Documented procedures must exist and be demonstrably in use for all key transmission and conveyance processing. | Written procedures must exist and all affected parties must be aware of those procedures. Conveyance or receipt of keys managed as components or otherwise outside an SCD must be documented. All key conveyance events performed by a key-injection facility must be documented. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 12. Secret and private keys must be input into host hardware security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.<br>a. Unencrypted secret or private keys must be entered into host hardware security modules (HSMs) and PIN entry devices (PEDs) using the principles of dual control and split knowledge.<br>b. Key-establishment techniques using public-key cryptography must be implemented securely. | Key-injection facilities must load keys (unencrypted symmetric keys must be loaded as key components) using dual control and for secret and private keys, split knowledge. Such keys include, but are not limited to:<br>▪ Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key-management method,<br>▪ Key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is injecting keys on their behalf),<br>▪ Terminal master keys (TMKs) used in the master key/session key key-management method,<br>▪ PIN-encryption keys used in the fixed-transaction key method,<br>▪ Master keys for key-injection platforms and systems that include hardware devices (SCDs) for managing (e.g., generating and storing) the keys used to encrypt other keys for storage in the key-injection platform system,<br>▪ Public and private key pairs loaded into the POIs for supporting remote key-establishment and distribution applications,<br>▪ Digitally signed POI public key(s) that are signed by a device manufacture's private key and subsequently loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable. Dual control is not necessary where other mechanisms exist to validate the authenticity of the key, such as the presence in the device of an authentication key,<br>▪ Device manufacturer's authentication key (e.g., vendor root CA public key) loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable).<br><br>Key-injection facilities must implement dual control and split knowledge controls for the loading of keys into equipment. Such controls can include (but are not limited to):<br>▪ Physical dual access controls that electronically provide for restricted entry and egress from a room dedicated to key-injection such that the badge access system enforces the presence of at least two authorized individuals at all times in the room so that no one person can singly access the key-loading equipment. Access is restricted to only appropriate personnel involved in the key-loading process.<br>▪ Logical dual control via multiple logins with unique user IDs to the key-injection platform application such that no one person can operate the application to singly inject cryptographic keys into devices.<br>▪ Key-injection platform applications that force the entry of multiple key components and the implementation of procedures involving multiple key custodians that store and access key components under dual-control and split-knowledge mechanisms.<br>▪ Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry.<br><br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 12. *(Continued)* | The master file key and any key-encryption key, when loaded from the individual key components, must be loaded using the principles of dual control and split knowledge. Procedures must be established that will prohibit any one person from having access to all components of a single encryption key.<br><br>Key components shall be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components—for example, via XOR'ing. Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two eight-hexadecimal character halves to form a sixteen-hexadecimal secret key. The resulting key must exist only within the SCD.<br><br>Host security module (HSM) master file keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.<br><br>For manual key-loading, dual control requires split knowledge of the key among the entities. Manual key-loading may involve the use of media such as paper or specially designed key-loading hardware devices.<br><br>Any other SCD loaded with the same key components must combine all entered key components using the identical process.<br><br>The initial terminal master key (TMK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key may use asymmetric techniques, manual techniques or the existing TMK to encrypt the replacement TMK for download. Keys shall not be reloaded by any methodology in the event of a compromised device, which must be withdrawn from use.<br><br>TR-31 or an equivalent methodology should be used for key-loading whenever a symmetric key is loaded encrypted by another symmetric key. This applies whether symmetric keys are loaded manually (i.e., through the keypad), using a key-injection device, or from a remote host. It does not apply when clear-text symmetric keys or their components are loaded using standard dual-control techniques.<br><br>Any equivalent method must include the cryptographic binding of the key-usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key must take place within the secure cryptographic boundary of the device.<br><br>Key-establishment protocols using public-key cryptography may also be used to distribute PED symmetric keys. These key-establishment protocols may use either key transport or key agreement. In a key transport protocol, the key is created by one entity and securely transmitted to the receiving entity. For a key agreement protocol, both entities contribute information, which is then used by the parties to derive a shared secret key. Meet all applicable requirements described in Annex A of this document.<br><br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 12. *(Continued)* | A public-key technique for the distribution of symmetric secret keys must:<br>▪ Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA).<br>▪ Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question.<br>▪ Provide for mutual device authentication for both the host and the PED, or host-to-host if applicable, including assurance to the host that the PED actually has (or actually can) compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key. |
| 13. The mechanisms used to load secret and private keys, such as terminals, external PIN pads, key guns, or similar devices and methods must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component. | Key-injection facilities must ensure key-loading mechanisms are not subject to disclosure of key components or keys.<br>Some key-injection platforms use personal-computer (PC)-based software applications whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. These weaknesses include:<br>▪ XOR'ing of key components is performed in software.<br>▪ Clear-text keys and components can reside in software during the key-loading process.<br>▪ Some systems require only a single password.<br>▪ Some systems store the keys (e.g., BDKs, TMKs) on removable media or smart cards. These keys are in the clear with some systems.<br>▪ PCs, by default, are not managed under dual control. Extra steps (e.g., logical user IDs, physical access controls, etc.) must be implemented to prevent single control of a PC.<br>▪ Data can be recorded in the PC's non-volatile storage.<br>▪ Software Trojan horses or keyboard sniffers can be installed on PCs.<br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 13. *(Continued)* | Key-injection facilities that use PC-based key-loading software platforms which allow clear-text secret and/or private keys and/or their components to exist in unprotected memory outside the secure boundary of an SCD must minimally implement the following additional controls:<br>▪ PCs must be:<br>• Stand-alone (i.e., without modems, not connected to a LAN or WAN, not capable of wireless connections, etc.),<br>• Dedicated to only the key-loading function (e.g., there must not be any other application software installed), and<br>• Located in a physically secure room that is dedicated to key-loading activities.<br>▪ All hardware used in key-loading (including the PC) must be managed under dual control. Key-injection must not occur unless there are minimally two individuals in the key-injection room at all times during the process. If a situation arises that would cause only one person to be in the room, all individuals must exit until at least two can be inside.<br>▪ PC access and use must be monitored and logs of all key-loading must be maintained. These logs must be retained for a minimum of three years. The logs must be regularly reviewed by an authorized person who does not have access to the room or to the PC. The reviews must be documented. The logs must include but not be limited to:<br>• Logs of access to the room from a badge access system,<br>• Logs of access to the room from a manual sign-in sheet,<br>• User sign-on logs on the PC at the operating system level,<br>• User sign-on logs on the PC at the application level,<br>• Logs of the device IDs and serial numbers that are loaded along with the date and time and the individuals performing the key-injection,<br>• Video surveillance logs.<br>▪ Cable attachments and the PC must be examined before each use to ensure the equipment is free from tampering.<br>▪ The PC must be started from a powered-off position every time key-loading activities occur.<br>▪ The software application must load keys without recording any clear-text values on portable media or other unsecured devices.<br>▪ Keys must not be stored except within an SCD.<br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 13. *(Continued)* | ▪ The personnel responsible for the systems administration of the PC (e.g., a Windows administrator who configures the PC's user IDs and file settings, etc.) must not have authorized access into the room—they must be escorted by authorized key-injection personnel, and they must not have user IDs or passwords to operate the key-injection application.<br>▪ The key-injection personnel must not have system's administration capability at either the O/S or the application level on the PC.<br>▪ The PC must not be able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.<br>▪ Key-injection facilities must cover all openings on the PC that are not used for key-injection with security seals that are tamper-evident and serialized. Examples include but are not limited to PCMCIA, network, infrared and modem connections on the PC, and access to the hard drive and memory. The seals must be recorded in a log and the log must be maintained along with the other key-loading logs in a dual control safe. Verification of the seals must be performed prior to key-loading activities.<br>▪ If the PC application stores keys (e.g., BDKs or TMKs) on portable electronic media (e.g., smart cards), the media must be secured under dual control when not in use (e.g., in a dual control safe). If possible, instead of storing the key on those media, the key should be manually entered at the start of each key-injection session from components that are maintained under dual control and split knowledge.<br>***Note:*** *For DUKPT implementations, the BDK should be loaded from components each time and this requires manual tracking of the device ID counter and serial numbers from the previous key-loading session.* Key-injection facilities with PC applications that require passwords to be used to initiate decryption of keys on portable electronic media (e.g., smart cards) must ensure the passwords are maintained under dual control and split knowledge.<br>▪ Manufacturer's default passwords for PC-based applications must be changed.<br>SCD equipment must be inspected to detect evidence of monitoring and to ensure that dual-control procedures are not circumvented during key-loading .<br>An SCD must transfer a plain-text secret or private key only when at least two authorized individuals are identified by the device (e.g., by means of passwords or other unique means of identification).<br>Plain-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that there is no tap at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys, and that the device has not been subject to any tampering which could lead to the disclosure of keys or sensitive data.<br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 13. *(Continued)* | Non-SCDs shall not be used in the loading of clear-text secret or private keys or their components, outside of a secure key-loading facility, as delineated in Annex B. For example, ATM controller (computer) keyboards shall never be used for the loading of clear-text secret or private keys or their components.<br><br>The injection of key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) must result in either of the following:<br>▪ The medium is placed into secure storage, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device, or<br>▪ All traces of the component are erased or otherwise destroyed from the electronic medium.<br><br>For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:<br>▪ The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; and<br>▪ The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it; and<br>▪ The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs; and<br>▪ The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.<br><br>The media upon which a component resides must be physically safeguarded at all times.<br><br>Any tokens, EPROMs, or other key component holders used in loading encryption keys must be maintained using the same controls used in maintaining the security of hard copy key components. These devices must be in the physical possession of only the designated component holder and only for the minimum practical time.<br><br>If the component is not in human-comprehensible form (e.g., in a PROM module, in a smart card, on a magnetic-stripe card, and so forth), it must be in the physical possession of only one entity for the minimum practical time until the component is entered into an SCD.<br><br>If the component is in human-readable form (e.g., printed within a PIN-mailer-type document), it must be visible only at one point in time to only one person (the designated component custodian) and only for the duration of time required for this person to privately enter the key component into an SCD.<br><br>Printed key-component documents must not be opened until just prior to entry.<br><br>The component must never be in the physical possession of an entity when any one such entity is or ever has been similarly entrusted with any other component of this same key. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 14. All hardware and passwords used for key-loading must be managed under dual control. | Key-injection facilities must ensure that the key-injection application passwords and user IDs are managed under dual control. Also, the hardware used for key-injection must be managed under dual control. Vendor default passwords must be changed.<br><br>Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. Use of the equipment must be monitored and a log of all key-loading activities maintained for audit purposes. All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.<br><br>Passwords must be managed such that no single individual has the capability to enable key loading.<br><br>Any physical (e.g., brass) key(s) used to enable key-loading must not be in the control or possession of any one individual who could use those keys to load secret or private cryptographic keys under single control. |
| 15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised. | A cryptographic-based validation mechanism helps to ensure the authenticity and integrity of keys and components (e.g., testing-key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See **ISO 11568**. Recorded or displayed key-component check values and key check values shall not exceed six hexadecimal characters in length.<br><br>The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plain-text form, must:<br><br>▪ Be within a certificate; or<br>▪ Be within a PKCS#10; or<br>▪ Be within a SCD; or<br>▪ Have a MAC (message authentication code) created using the algorithm defined in **ISO 9807.** |
| 16. Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities. | Written procedures must exist and all parties involved in cryptographic key-loading must be aware of those procedures. All key-loading events performed by a key-injection facility must be documented. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 18. Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys. | Key-injection facilities must implement controls to protect against unauthorized substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to:<br>▪ All key-loading must be performed using dual control and split knowledge. Controls must be in place to prevent and detect the loading of keys by any one single person. Controls include physical access to the room, logical access to the key-loading application, video surveillance of activities in the key-injection room, physical access to secret or private cryptographic key components or shares, etc.<br>▪ All devices loaded with keys must be tracked at each key-loading session by serial number.<br>▪ Unloaded devices must be managed in accordance with Requirement 29.<br>▪ Key-injection facilities must use something unique about the EPP or POS device (e.g., serial number) when deriving the key (e.g., DUKPT, TMK) injected into it.<br>Multiple synchronization errors in PIN translation may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted. Procedures for investigating repeated synchronization errors must exist to help reduce the risk of an adversary substituting a key known only to them.<br>To prevent substitution of a compromised key for a legitimate key, key-component documents that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.<br>TDEA keys should be managed as key bundles at all times, e.g., using TR-31. The bundle and the individual keys should:<br>▪ Have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source;<br>▪ Be used in the appropriate order as specified by the particular mode;<br>▪ Be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged; and<br>▪ Cannot be unbundled for any purpose. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 19. Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems. | Key-injection facilities must have a separate test system for the injection of test keys.<br>▪ Test keys must not be injected using the production platform, and test keys must not be injected into production equipment.<br>▪ Production keys must not be injected using a test platform, and production keys must not be injected into equipment that is to be used for testing purposes.<br>▪ Keys used for signing of test certificates must be test keys.<br>▪ Keys used for signing of production certificates must be production keys.<br><br>Encryption keys must only be used for the purpose they were intended (e.g., key-encryption keys must not be used as PIN-encryption keys). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.<br><br>MFKs and their variants used by host processing systems for encipherment of keys for local storage shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration.<br><br>Private keys shall only be used to create digital signatures and to perform decryption operations. Private keys shall never be used to encrypt other keys. Keys must never be shared or substituted in a processor's production and test systems. Except by chance, keys used in production must never be used in testing, and keys used in testing must never be used in production.<br><br>***Note:*** *If a business rationale exists, a production platform (HSMs and servers/stand-alone computers) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the key injection server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.*<br><br>*At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device. | Key-injection facilities must ensure that unique keys are loaded into each device. The same key(s) must not be loaded into multiple devices.<br><br>Key-injection facilities that load DUKPT keys must use separate BDKs for different entities.<br><br>Key-injection facilities that load DUKPT keys for various terminal types for the same entity must use separate BDKs per terminal type if the terminal IDs can be duplicated among the multiple types of terminals. In other words, the key-injection facilities must ensure that any one given key cannot be derived for multiple devices except by chance.<br><br>Any key used to encrypt a PIN in a PED must be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.<br><br>In a master/session key approach, the master key(s) and all session keys must be unique to each cryptographic device.<br><br>If a transaction-originating terminal interfaces with more than one acquirer, the transaction-originating terminal SCD must have a completely different and unique key or set of keys for each acquirer. These different keys, or set of keys, must be totally independent and not variants of one another.<br><br>Keys that are generated by a derivation process and derived from the same Base Derivation Key must use unique data for the derivation process so that all such cryptographic devices receive unique initial secret keys.<br><br>Entities processing or injecting DUKPT or other key derivation methodologies on behalf of multiple acquiring financial institutions must use different Base Derivation Keys for each financial institution. The processing entity may share one or more Base Derivation Keys for merchants that are sponsored by the same acquirer.<br><br>***Remote Key-Establishment and Distribution Applications***<br><br>The following requirements apply to key-injection facilities participating in remote key-establishment and distribution applications:<br>▪ Keys must be uniquely identifiable in all hosts and EPPs/PEDs. Keys must be identifiable via cryptographically verifiable means (e.g., through the use of digital signatures or key check values).<br>▪ Key pairs must be unique per device including key-distribution hosts (except as otherwise provided for), EPPs and POS PEDs. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 21. Secret keys used for enciphering PIN-encryption keys, or for PIN encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge. | Key-injection facilities must ensure that KEKs and PIN encryption keys do not exist outside of SCDs except when encrypted or stored under dual control and split knowledge.<br><br>Some key-injection platforms use Personal Computer (PC) based software applications whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems do not therefore meet this requirement. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key-injection facilities that use PC-based key-loading software platforms whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD must minimally implement the compensating controls outlined in Requirement 13.<br><br>Effective implementation of these principles requires the existence of barriers beyond procedural controls to prevent any custodian (or non-custodian for any individual component) from gaining access to all key components. An effective implementation would have physically secure and separate locking containers that only the appropriate key custodian (and their designated backup) could physically access.<br><br>Components for a specific key that are stored in separate envelopes, but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers. Furniture-based locks or containers with a limited set of unique keys are not sufficient to meet the requirement for physical barriers.<br><br>Key components may be stored on tokens (e.g., PC cards, smart cards, and so forth). These tokens must be stored in a special manner to prevent unauthorized individuals from accessing the key components. For example, if key components are stored on tokens that are secured in safes, more than one person might have access to these tokens. Therefore, additional protection is needed for each token (possibly by using tamper-evident, authenticable envelopes) to enable the token's owner to determine whether a token was used by another person. In particular, key components for each specific custodian must be stored in separate secure containers.<br><br>If a key is stored on a token and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup) must have possession of both the token and its corresponding PIN.<br><br>Printed or magnetically recorded key components must reside only within tamper-evident, authenticable, sealed envelopes so that the component cannot be ascertained without opening the envelope.<br><br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 21. *(Continued)* | DES keys that are used to encipher other keys or to encipher PINs, and which exist outside of an SCD, must be enciphered using keys of equal or greater strength as delineated in Annex C. For example:<br>▪ The TDEA using at least double-length keys or<br>▪ RSA using a key modulus of at least 1024 bits.<br>A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.<br>Symmetric secret keys may be enciphered using public-key cryptography for distribution to PEDs as part of a key-establishment protocol as defined in Requirement 12. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 22. Procedures must exist and be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key. | Key-injection facilities must have written procedures to follow in the event of compromise of any key associated with the key-injection platform and process. Written procedures must exist and all parties involved in cryptographic key-loading must be aware of those procedures. All key-compromise procedures must be documented.<br><br>Key components must never be reloaded when there is any suspicion that either the originally loaded key or the device has been compromised. If suspicious alteration is detected, new keys must not be installed until the SCD has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.<br><br>A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.<br><br>Procedures must include a documented escalation process and notification to organizations that currently share or have previously shared the key(s). The procedures must include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, and so forth.<br><br>The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.<br><br>Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.<br><br>Specific events must be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:<br>▪ Missing cryptographic devices<br>▪ Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries<br>▪ Tamper-evident seals or authenticable envelopes that have been opened without authorization or show signs of attempts to open or penetrate<br>▪ Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities<br>▪ Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation.<br><br>If attempts to load a secret or private key or key component into a cryptographic device fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased or otherwise destroyed in the original device.<br><br>*(Continued on next page)* |

<table>
<tr><th>Key-Injection Facility Security Requirement</th><th>International/Industry Standard(s)</th></tr>
<tr><td>22. (Continued)</td><td>Prolonged use of a key increases the risk of its cryptanalytic compromise, depending upon, for example, implementation, key length, and availability of corresponding cipher texts/plain texts. Cryptoperiods for keys should be assigned to minimize this risk taking into account any additional risk associated with key changes. For example, recommended maximum cryptoperiods for the following TDES double-length keys, based on guidance in NIST SP800-57, ISO TR 14742 and NIST SP800-131 are:
<table>
<tr><th>Type of Key Exchange</th><th>Key Type</th><th>Cryptoperiod</th></tr>
<tr><td>Static</td><td>PEK</td><td>12 months</td></tr>
<tr><td>Dynamic</td><td>KEK</td><td>3 years</td></tr>
<tr><td>Dynamic</td><td>PEK</td><td>12 hours (or UKPT)</td></tr>
</table>
UKPT is the preferred option.</td></tr>
<tr><td>23. Key variants must be used only in devices that possess the original key. Key variants must not be used at different levels of the key hierarchy e.g., a variant of a key-encipherment key used for key exchange must not be used as a working key or as a master file key for local storage.</td><td>A secret key used to encrypt a PIN for interchange must never be used for any other cryptographic purpose. A key used to protect the PIN-encrypting key must never be used for any other cryptographic purpose other than key encipherment.<br>Variants of the same key may be used for different purposes. Any variant of the PEK or a key used to protect the PEK must be protected in the same manner—i.e., under the principles of dual control and split knowledge.<br>An MFK used by host processing systems for encipherment of keys for local storage, and variants of the MFK must not be used external to the (logical) configuration that houses the MFK itself.</td></tr>
<tr><td>24. Secret and private keys and key components that are no longer used or have been replaced must be securely destroyed.</td><td>Instances of keys (including components or shares) that are no longer used or that have been replaced by a new key must be destroyed. Clear-text key components or shares maintained on paper must be burned, pulped or shredded in a crosscut shredder. Keys on other storage-media types and in other permissible forms of a key instance (physically secured, enciphered, or components) must be destroyed following the procedures outlined in ISO-9564-1 or ISO-11568-2. In all cases, a third party—other than the custodian—must observe the destruction and sign an affidavit of destruction.<br>The procedures for destroying keys that are no longer used or that have been replaced by new keys must be documented.<br>Key-encipherment key components used for the conveyance of working keys must be destroyed after successful loading and validation as operational.</td></tr>
</table>

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 25. Access to secret and private cryptographic keys and key material must be:<br>a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.<br>b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. | Limiting the number of key custodians to a minimum helps reduce the opportunity for key compromise. In general, the designation of a primary and a backup key custodian for each component is sufficient. This designation must be documented by having each custodian sign a Key Custodian Form. The form must specifically authorize the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them. Each custodian must sign a Key Custodian Form acknowledging these responsibilities before receiving custody of key components or enablers (for example, PINs) for keys or their components. Key custodians must be free from undue influence in discharging their custodial duties.<br>Key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual. For example, for a key managed as three components, at least two individuals must report to different individuals. In an m-of-n scheme, such as 3 of 5 key shares, no more than two key custodians can report to the same individual. In all cases, neither the direct reports, nor the direct reports in combination with their immediate supervisor shall possess a quorum of key components sufficient to form any given key. |
| 26. Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD. | Key-injection facilities must maintain logs for the key management of all keys and keying material used in all key-loading sessions. These include keys and materials removed from safes and used in the loading process.<br>At a minimum, the logs must include the date and time in/out, purpose of access, name and signature of custodian accessing the component, envelope number (if applicable). |
| 27. Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key. | The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as the primary keys (see Requirement 21—i.e., within an SCD, unless encrypted or securely stored and managed using the principles of dual control and split knowledge).<br>Backups (including cloning) must require a minimum of two authorized individuals to enable the process.<br>***Note:***<br>*It is not a requirement to have backup copies of key components or keys.* |
| 28. Documented procedures must exist and be demonstrably in use for all key-administration operations. | Written procedures must exist and all affected parties must be aware of those procedures. All activities related to key administration performed by a key-injection facilities must be documented. This includes all aspects of key administration, as well as:<br>▪ Security awareness training.<br>▪ Role definition - nominated individual with overall responsibility.<br>▪ Background checks for personnel.<br>▪ Management of personnel changes, including revocation of access control and other privileges when personnel move. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 29. PIN-processing equipment (e.g., PEDs and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the loading of cryptographic keys and that precautions are taken to minimize the threat of compromise once deployed. | Key-injection facilities must ensure that only legitimate, unaltered devices are loaded with cryptographic keys.<br><br>Secure areas must be established for the inventory of PEDs that have not had keys injected. The area must have extended walls from the real floor to the real ceiling using sheetrock, wire mesh, or equivalent. Equivalence can be steel cages extending floor to real ceiling. The cages can have a steel cage top in lieu of the sides extending to the real ceiling. The cages must have locks (with logs) or badge control with logging for entry.<br><br>HSMs and PEDs must be placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering or is otherwise subject to misuse. To achieve this, controls must exist to protect secure cryptographic devices from unauthorized access before, during, and after installation. Access to all cryptographic hardware must be documented, defined, and controlled. Cryptographic devices **must not** use default keys or data. A documented security policy must exist that specifies personnel with authorized access to all secure cryptographic devices. Unauthorized individuals must not be able to access, modify, or substitute any secure cryptographic device. A documented chain of custody must exist to ensure that all cryptographic hardware is controlled from its receipt through its installation and use. Controls must ensure that all installed hardware components are from a legitimate source.<br><br>Dual-control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or backup devices. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted cryptographic devices but must not supplant the implementation of dual-control mechanisms.<br><br>This requires physical protection of the device up to the point of key-insertion or inspection, and possibly testing of the device immediately prior to key-insertion. Techniques include, but are not limited to, the following:<br>▪ Cryptographic devices are transported from the manufacturer's facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.<br>▪ Cryptographic devices are shipped from the manufacturer's facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident, authenticable packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs.<br>▪ The manufacturer's facility loads into each cryptographic device a secret, device-unique "transport-protection token." The SCD used for key-insertion has the capability to verify the presence of the correct "transport-protection token" before overwriting this value with the initial key that will be used.<br><br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 29. *(Continued)* | ▪ Each cryptographic device is carefully inspected and perhaps tested immediately prior to key-insertion using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized modifications.<br>• Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised.<br>• Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.<br>Documented inventory-control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:<br>▪ Protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it, and<br>▪ Detect lost or stolen equipment.<br>Procedures must include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.<br>Notwithstanding how the device is inspected and tested, it is mandatory to verify the device serial number against the purchase order, invoice, waybill or similar document to ensure that device substitution has not occurred.<br>Documents used for this process must be received via a different communication channel (i.e., the control document used must not have arrived with the shipment of the equipment).<br>PIN-processing equipment shall only be used for its specified purpose. It must not be possible for the equipment to be operated in an unauthorized manner or beyond the scope of the operating procedures specified for the equipment.<br>The security policy enforced by the HSM must not allow unauthorized or unnecessary functions. HSM API functionality and commands that are not required in PIN processing equipment to support specified functionality must be disabled before the equipment is commissioned. For example, PIN change functionality or PIN-block format translation functionality may not need to be supported or can be limited. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 30. Procedures must exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service. | Key-injection facilities must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any SCDs (e.g., HSM) used in the key-injection platform, as well as to any devices that have been loaded with keys and securely stored or warehoused on site that are subsequently deemed to be unnecessary and never to be placed into service.<br><br>If a key-injection facility receives a used device to reload with keys, procedures shall ensure that old keys that may be in the device are destroyed prior to loading of new keys. (The used device should have had its keys destroyed when it was removed from service, but this is a prudent secondary check that the keys were destroyed).<br><br>If an SCD has been removed from service, all keys stored within the device that have been used (or potentially could be) for any cryptographic purpose must be destroyed.<br>▪ All critical initialization, deployment, usage, and decommissioning processes—e.g., key- or component-loading, firmware- or software-loading, and verification and activation of anti-tamper mechanisms—must impose the principles of dual control and split knowledge.<br>▪ Key and data storage must be zeroized when a device is decommissioned.<br><br>If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 31. Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:<br>**a.** Dual access controls are required to enable the key-encryption function.<br>**b.** Physical protection of the equipment (e.g., locked access to it) under dual control.<br>c. Restriction of logical access to the equipment. | Key-injection facilities must ensure protection against unauthorized use for SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.<br>The facility must implement a secure area (i.e., room) for key injection. This key injection room shall:<br>1. Exist in a secure area with extended walls from the real floor to the real ceiling using sheetrock or wire mesh.<br>2. Alarm or block any windows into the room to detect and/or prevent access.<br>3. Install a solid-core door or a steel door, ensuring that door hinges cannot be removed from outside the room.<br>4. Implement a badge control system that supports dual-access requirements for entry to the secure area and supports anti-pass-back.<br>5. Ensure that the badge system supports an alarm (e.g., through use of motion detection) when one person remains in the secure area alone beyond 30 seconds.<br>6. Install either two safes with dual control (key and combination or two combinations) or one safe with two locked non-removable steel containers where the two key custodians possess the key.<br>7. Utilize a CCTV system that supports remote monitoring on a 7/24 basis so that alarms can be remotely resolved by authorized personnel<br>8. Secure the CCTV server and digital storage in a separate secure area that is not accessible to the personnel that have access to the key injection area<br>9. Focus the cameras on the entrance door, inventories of devices both pre and post key injection, any safe that is present and the equipment used for key injection (without focusing on any combination locks or keyboards used to enter passwords or other authentication credentials).<br>Cryptographic equipment must be managed in a secure manner in order to minimize the opportunity for key compromise or key substitution. Physical keys, authorization codes, passwords, or other enablers must be managed so that no one person can use both the enabler(s) and the device which can create cryptograms of known keys or key components under a key-encipherment key used in production.<br>Unauthorized use of secure cryptographic devices (including key-loading devices) shall be prevented or detected by all of the following:<br>▪ The device is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected;<br>*(Continued on next page)* |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 31. *(Continued)* | ▪ The device has functional or physical characteristics (e.g., passwords or physical high-security keys) that prevent use of the device except under the dual control of at least two authorized people; and when in a state in which it is useable, the device is under the continuous supervision of at least two such people who ensure that any unauthorized use of the device would be detected.<br><br>Network access to the device is based on the following controls:<br>▪ **PCI DSS:** The network shall meet any PCI DSS compliance requirements.<br>▪ **Network separation:** The HSM production network shall be logically and physically separate from any other business networks.<br>▪ **Firewalls (Hardware or Software)**: The HSM production network should use a nested firewall configuration with an external and inner network boundary, protected by a firewall and coupled with an IDS.<br>▪ **Access controls:** Authorized access to logical and physical components of the HSM production network shall be based on timed access and dual control. It is strongly recommended that devices and applications be set with the most stringent, logical access-control settings where applicable. Access-control settings shall be specified for production domains, servers, proxy servers, firewalls, routers, and organizational units (OUs) and other protected resources.<br>▪ **IDS (Intrusion-detection system):** The HSM network environment shall be monitored using IDS on a 24/7 basis. Monitoring, as a minimum, should include normal and exception reporting on personal access, violation of established protocols, and processes that affect the HSMs—for example, unusual/out-of-pattern access events, software/firmware loads, HSM velocity checking.<br>▪ **VPN (Virtual Private Networks)**: Separate internal IP addresses and/or separate VPNs should be applied to HSM production networks where direct cabling or device isolation into a single physical location is not practical. Encrypted VPN solutions should be used to separate the production network platform from any other internal network.<br>▪ **Logging and auditing**: 24/7 logging and reviews of audit trails shall be implemented for devices and any platforms that support the production network, for example ACLs (access control lists), organizational units (OUs) and other protected resources.<br>▪ **Staff**: It is strongly recommended that patch management, database administration, or system administration services be conducted for the HSM production environment under dual control and authorized/monitored by the appropriate network security management personnel. |

| Key-Injection Facility Security Requirement | International/Industry Standard(s) |
|---|---|
| 32. Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned. | Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed by key-injection facilities on to PIN-processing devices before they are placed into service, as well as devices being decommissioned.<br><br>Procedures that govern access to HSMs must be in place and known to data-center staff and any others involved with the physical security of such devices.<br><br>HSM security policies/configurations must be validated to secure settings at least annually. |

# Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange, or establishment and for data protection:

| Algorithm | DES | RSA | Elliptic Curve | DSA | AES |
|---|---|---|---|---|---|
| Minimum key size in number of bits: | 112 | 1024 | 160 | 1024/160 | 128 |

*Key-encipherment keys shall be at least of equal or greater strength than any key that they are protecting.* ***This applies to any key-encipherment keys used for the protection of secret or private keys that are stored or for keys used to encrypt any secret or private keys for loading or transport. For purposes of this requirement, the following algorithms and keys sizes by row are considered equivalent.***

| Algorithm | DES | RSA | Elliptic Curve | DSA/D-H | AES |
|---|---|---|---|---|---|
| Minimum key size in number of bits: | 112 | 1024 | 160 | 1024/160 | - |
| Minimum key size in number of bits: | 168 | 2048 | 224 | 2048/224 | - |
| Minimum key size in number of bits: | - | 3072 | 256 | 3072/256 | 128 |
| Minimum key size in number of bits: | - | 7680 | 384 | 7680/384 | 192 |
| Minimum key size in number of bits: | - | 15360 | 512 | 15360/512 | 256 |

DES refers to TDES keys with non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

For Diffie-Hellman implementations:

- Entities must securely generate and distribute the system-wide parameters: generator *g,* prime number *p* and parameter *q,* the large prime factor of (*p* - 1). Parameter *p* must be at least 2048 bits long, and parameter *q* must be at least 224 bits long. Each entity shall generate a private key *x* and a public key *y* using the domain parameters (*p, q, g*,). Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
- Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES—see *ISO 16609 – Banking –Requirements for message authentication using symmetric techniques;* Method 3 should be used).

# Glossary

| Term | Definition |
|---|---|
| **Access controls** | Controls to ensure that specific objects, functions, or resources can only be accessed by authorized users in authorized ways. |
| **Acquirer** | The institution (or its agent) that receives from a card acceptor the data relating to financial transactions with PINs. The acquirer is the entity that forwards the financial transaction into an interchange system. |
| **Algorithm** | A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result. |
| **ANSI** | American National Standards Institute, a U.S. standards accreditation organization. |
| **Asymmetric cryptography (techniques)** | See *Public-key cryptography.* |
| **ATM** | Automated teller machine. An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks. |
| **Authentication** | The process for establishing unambiguously the identity of an entity, organization, or person. |
| **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. |
| **Base (master) Derivation Key (BDK)** | See *Derivation key.* |
| **Cardholder** | An individual to whom a card is issued or who is authorized to use the card. |
| **Card issuer** | The institution or its agent that issues the payment card to the cardholder. |
| **Certificate** | For purposes of these requirements, a certificate is any digitally signed value containing a public key. |
| **Certificate revocation** | The process of revoking an otherwise valid certificate by the entity that issued that certificate. Revoked certificates are placed on a certificate revocation list (CRL) or the information is conveyed using OCSP as specified in the product/service specification. |
| **Certificate Revocation List (CRL)** | A list of revoked certificates. Entities that generate, maintain, and distribute CRLs can include, for example, the root or subordinate CAs. |
| **Certification authority (CA)** | For purposes of these requirements, a certification authority is any entity signing public keys, whether in X.509 certificate based schemes or other designs for use in connection with the remote distribution of symmetric keys using asymmetric techniques. |
| **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 gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key must not be feasible. |

| Term | Definition |
|---|---|
| **Cipher text** | Data in its enciphered form. |
| **Clear text** | *See* Plain text. |
| **Communicating nodes** | Two entities (usually institutions) sending and receiving transactions. This is to include alternate processing sites either owned or contracted by either communicating entity. |
| **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). |
| **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. |
| **Credentials** | Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key. |
| **Critical security parameters (CSP)** | Security-related information (e.g., cryptographic keys or authentication data such as passwords and PINs) appearing in plain-text or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic device or the security of the information protected by the device. |
| **Cryptographic boundary** | An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. In the context of this document, key component may be used to equate a secret share that is part of a recognized cryptographic secret-sharing scheme. |
| **Cryptographic key** | A parameter used in conjunction with a cryptographic algorithm that determines:<br>▪ The transformation of plain-text data into cipher-text data,<br>▪ The transformation of cipher-text data into plain-text data,<br>▪ A digital signature computed from data,<br>▪ The verification of a digital signature computed from data,<br>▪ An authentication code computed from data, or<br>▪ An exchange agreement of a shared secret. |
| **Cryptographic key component** | A parameter used in conjunction with other key components in an approved security function to form a plain-text cryptographic key or perform a cryptographic function. |
| **Customers** | Customers are financial institutions that:<br>a. Offer payment cards for one or more of the participating payment brands (issuers);<br>b. Accept such payment cards for cash disbursement and directly or indirectly enter the resulting transaction receipt into interchange (acquirers); or<br>c. Offer financial services to merchants or authorized third parties who accept such payment cards for merchandise, services, or cash disbursement, and directly or indirectly enter the resulting transaction receipt into interchange (acquirers). |

| Term | Definition |
|---|---|
| **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 encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity-checking to ensure that the key is transmitted properly. |
| **Decipher** | See *Decrypt.* |
| **Decrypt** | A process of transforming cipher text (unreadable) into plain text (readable). |
| **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.<br>Derivation keys are normally used in a transaction-receiving (e.g., acquirer) SCD in a one-to-many relationship to derive or decrypt the transaction keys (the derived keys) used by a large number of originating (e.g., terminals) SCDs. |
| **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. |
| **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. |
| **Electronic code book (ECB) operation** | A mode of encryption using the data encryption algorithm, in which each block of data is enciphered or deciphered without using an initial chaining vector or previously (encrypted) data blocks. |
| **EEPROM** | Electronically erasable programmable read-only memory. |
| **Electronic key entry** | The entry of cryptographic keys into a secure 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.* |

| Term | Definition |
|---|---|
| **Encrypt** | The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data. |
| **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 other unattended device (e.g., an unattended kiosk or automated 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.<br>Encrypting PIN pads require integration into UPTs or ATMs. |
| **EPROM** | Erasable programmable read-only memory. |
| **Exclusive-OR** | Binary addition without carry, also known as "modulo 2 addition," symbolized as "XOR" and defined as:<br>▪ 0 + 0 = 0<br>▪ 0 + 1 = 1<br>▪ 1 + 0 = 1<br>▪ 1 + 1 = 0 |
| **FIPS** | Federal Information Processing Standard. |
| **Firmware** | The programs and data (i.e., software) permanently stored in hardware (e.g., in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software. |
| **Hardware (host) security module** | A physically and logically protected hardware device that provides a secure set of cryptographic services. |
| **Hash function** | A (mathematical) function that is a non-secret algorithm, which takes any arbitrary-length message as input and produces a fixed-length hash result. It must have the property that it is computationally infeasible to discover two different messages that produce the same hash result. It may be used to reduce a potentially long message into a "hash value" or "message digest" 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. |
| **Initialization vector** | A binary vector used as the input to initialize the algorithm 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. |
| **Integrity** | Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data. |
| **Interchange** | The exchange of clearing records between financial institution customers. |
| **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. |

| Term | Definition |
|---|---|
| **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. |
| **Issuer** | The institution holding the account identified by the primary account number (PAN). |
| **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 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. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle must never be used separately for any other purpose. |
| **Key component** | *See* Cryptographic Key Component. |
| **Key derivation process** | A process, which derives one or more session keys from a shared secret and (possibly) other public information. |
| **Key destruction** | Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location. |
| **Key-distribution host (KDH)** | A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to the EPP or PED and the financial processing platform communicating with those EPPs/PEDs. A KDH may be an application that operates on the same platform that is used for PIN translation and financial transaction processing. The KDH may be used in conjunction with other processing activities. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys. |
| **Key-encrypting (encipherment or exchange) key** | A cryptographic key that is used for the encryption or decryption of other keys. |
| **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 generation** | Creation of a new key for subsequent use. |
| **Key instance** | The occurrence of a key in one of its permissible forms, i.e., plain-text key, key components, 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. |

| Term | Definition |
|---|---|
| **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** | A key pair comprises the 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 transport** | A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected. |
| **Key usage** | Employment of a key for the cryptographic purpose for which it was intended. |
| **Key variant** | A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key. |
| **Keying material** | The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships. |
| **Manual key-loading** | The entry of cryptographic keys into a secure cryptographic device from a printed form, 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. |
| **Message** | A communication containing one or more transactions or related information. |
| **Node** | Any point in a network that does some form of data processing, such as a terminal, acquirer, or switch. |
| **Non-reversible transformation** | See *Irreversible transformation.* |
| **Online Certificate Status Protocol (OCSP)** | The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response. |
| **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. |

| Term | Definition |
|---|---|
| **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. |
| **Out-of-band notification** | Notification using a communication means independent of the primary communications means. |
| **PAN** | Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. |
| **Password** | A string of characters used to authenticate an identity or to verify access authorization. |
| **Personal identification number (PIN)** | A numeric personal identification code that authenticates a cardholder in an authorization request originating at a terminal with authorization-only or data-capture-only capability. A PIN consists only of decimal digits. |
| **Physical protection** | The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means. |
| **Physically secure environment** | An environment 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 purpose-built room with continuous access control, physical security protection, and monitoring. |
| **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. |
| **PIN entry device (PED)** | A PED is 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 and is a complete terminal that can be provided to a merchant "as is" to undertake PIN-related transactions. This may include either attended or unattended POS POI terminals. |
| **PIN pad** | See *PIN entry device.* |
| **Plain text** | Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as clear text. |
| **Plain-text key** | An unencrypted cryptographic key, which is used in its current form. |
| **Point of interaction** | See *Point of transaction.* |
| **Point of transaction** | The physical location where a merchant or acquirer (in a face-to-face environment) or an unattended acceptance terminal (in an unattended environment) completes a transaction receipt. |
| **Private key** | A cryptographic key, used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public.<br>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. |
| **PROM** | Programmable read-only memory. |

| Term | Definition |
|---|---|
| **Pseudo-random** | A value that is statistically random and essentially random and unpredictable although generated by an algorithm. |
| **Public key** | A cryptographic key, used with a public-key cryptographic algorithm, uniquely associated with an entity, and that may be made public.<br>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.<br>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.<br>With asymmetric cryptographic techniques, 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. |
| **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. |
| **Registration authority (RA)** | An entity that performs registration services on behalf of a certification authority (CA). Registration authorities (RAs) work with a particular certification authority (CA) to vet requests for certificates that will then be issued by the certification authority. |
| **ROM** | Read-only memory. |
| **Root certification authority (RCA)** | The RCA is the top level certification authority in a public key infrastructure. A RCA is a CA which signs its own public key with the associated private key. RCAs only issue certificates to subordinate CAs. Root CAs do not issue certificates directly to KDHs, EPPs, or PEDs. RCAs may also issue certificate status lists for certificates within its hierarchy. |

| Term | Definition |
|---|---|
| **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. |
| **Secure cryptographic device (SCD)** | 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. |
| **Sensitive data** | Data that must be protected against unauthorized disclosure, alteration, or destruction, especially plain-text PINs and cryptographic keys, and includes design characteristics, status information, and so forth. |
| **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. |
| **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. |
| **Software** | The programs and associated data that can be dynamically written and modified. |
| **Split knowledge** | A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. |
| **Subordinate CA and Superior CA** | If one CA issues a certificate for another CA, the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, EPPs or PEDs. Subordinate CAs may also issue certificates to lower-level CAs and issue certificate status lists regarding certificates the subordinate CA has issued. |
| **Symmetric 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. |
| **System software** | The special software (e.g., operating system, compilers, or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data. |
| **Switch** | A node that can route data from a node to other nodes. |
| **Tamper-evident** | A characteristic that provides evidence that an attack has been attempted. |
| **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. |

| Term | Definition |
|---|---|
| **Tampering** | The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data. |
| **TDEA** | See *Triple Data Encryption Algorithm.* |
| **TECB** | TDEA electronic code book. |
| **Terminal** | A device/system that initiates a transaction. |
| **Transaction** | A series of messages to perform a predefined function. |
| **Triple Data Encryption Algorithm (TDEA)** | An algorithm specified in ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. |
| **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. |
| **Trustworthy system** | A combination of computer hardware and software that:<br>▪ Are reasonably secure from intrusion and misuse;<br>▪ Provide a reasonable level of availability, reliability, and correct operation; and<br>▪ Are reasonably suited to performing their intended functions. |
| **Two-factor authentication** | Two-factor authentication (“TFA” or “2FA”) is a system wherein two different factors are used in conjunction for authentication. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three methods: "something you know" (e.g., password or PIN), "something you have" (e.g., smartcard or token), or "something you are" (e.g., fingerprint or iris scan). |
| **Unattended acceptance terminal (UAT)** | A cardholder-operated device that reads, captures, and transmits card information in an unattended environment including, but not limited to, the following:<br>▪ ATM<br>▪ Automated Fuel Dispenser<br>▪ Ticketing Machine<br>▪ Vending Machine |
| **Unattended payment terminal (UPT)** | A POS POI device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as:<br>▪ Automated fuel dispensers<br>▪ Kiosks<br>▪ Self-service devices—ticketing/vending or car parking terminals. |
| **Unprotected memory** | Data retained within components, devices, and recording media that reside outside the cryptographic boundary of a secure cryptographic device. |
| **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. |

| Term | Definition |
|---|---|
| **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.* |
| **Zeroize** | The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data. |