



Payment Card Industry: PIN Security Requirements

Version 2.0

January 2008



Payment Card Industry: PIN Security Requirements

Table of Contents

Overview	2
OBJECTIVE 1	2
OBJECTIVE 2	2
OBJECTIVE 3	3
OBJECTIVE 4	3
OBJECTIVE 5	4
OBJECTIVE 6	4
OBJECTIVE 7	4
PIN Security Requirements—Technical Reference	6
Introduction	6
ANSI, EMV, ISO, FIPS, NIST and PCI Standards	6
Requirement/Standards Cross-Reference	8
Normative Annex A - Symmetric Key Distribution using Asymmetric Techniques	25
Normative Annex B - Key Injection Facilities	37
Appendix A - VISA Specific Requirements	75
General Requirements	75
PIN Security Requirement #1	75
Self-Audit Procedures	76
Appendix B - Forms	78
PIN Security Requirements Self-Audit Compliance Statement	79
PIN Security Requirements Self-Audit Processing Environment	81
PIN Security Requirements Self-Audit Exception Form	83
Appendix C - PIN Security Requirements Self-Audit	84
Objective 1	84
Objective 2	85
Objective 3	86
Objective 4	87
Objective 5	88
Objective 6	89
Objective 7	90
Glossary	91

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 were derived from existing Visa and MasterCard documentation and finalized by a working group formed by the major payment card organizations.

The 32 requirements presented in this document are organized into seven logically related groups, which are 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.

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 Members or non-members who operate key injection facilities on behalf of other members, see Normative Annex B

The words *must* and *shall* indicate a mandatory requirement. Statements that do not contain these words indicate that these are best practices that are recommended, but not mandated.

The effective date for this document is 1 January 2008.

See Appendices A, B and C for Visa specific forms and requirements.

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 are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. TRSMs 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 are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.
2. Cardholder PINs are processed in accordance with approved standards.
 - a. All cardholder PINs processed online are 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 are 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 are not 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 are generated using an approved random or pseudo-random process.
6. Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.
7. Documented procedures exist and are demonstrably in use for all key generation processing.

OBJECTIVE 3

Keys are conveyed or transmitted in a secure manner.

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

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

9. Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:
 - a. Under the continuous supervision of a person with authorized access to this component, or
 - b. Locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or
 - c. In a physically secure TRSM.
10. All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.
11. Documented procedures exist and are 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. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.
13. The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are 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 are 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 exist and are 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.
18. Procedures 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 are only used for their sole intended purpose and are never 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. Keys used for enciphering PIN-Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.
22. Procedures exist and are 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 are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot 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 are securely destroyed.
25. Access to secret and private cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.
26. Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.
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 exist and are 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 (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.

30. Procedures 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 TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following:
 - a. Dual access controls are required to enable the key encryption function.
 - b. Physical protection of the equipment (e.g., locked access to it) under dual control.
32. Documented procedures exist and are 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

Effective Date: 1 January 2008

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. However, defining the schedule for the migration from Single-DES to Triple-DES is reserved to the payment brands.

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.

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

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

- **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 X9.52:** Triple Data Encryption Algorithm: Modes of Operation
- **EMV:** Integrated Circuit Card Specification for Payment Systems, version 4.1 (June 2004)—Book 2: Security and Key Management
- **FIPS PUB 140–2:** Security Requirements for Cryptographic Modules.
- **ISO 9564–1:** Personal Identification Number Management and Security, Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems
- **ISO 9564–2:** Personal Identification Number Management, Part 2: Approved Algorithms for PIN Encipherment
- **ISO 9564–3):** Personal Identification Number Management and Security, Part 3: Requirements for offline PIN handling in ATM and POS systems
- **ISO 11568–1:** Banking - Key Management (Retail), Part 1: Principles
- **ISO 11568–2:** Banking - Key Management (Retail), Part 2: Symmetric ciphers, their key management and life cycle
- **ISO 11568–4:** Banking Key Management (Retail), Part 4: Key management techniques using public key cryptosystems
- **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 13491-1:** Banking—Secure Cryptographic Devices (Retail), Part 1: Concepts, Requirements, and Evaluation Methods
- **ISO 13491-2:** Banking—Secure Cryptographic Devices (Retail), Part 2: Compliance Checklists for Devices used in Financial Transactions.
- **ISO TR19038:** Guidelines on Triple DES Modes of Operation.
- **NIST Special Publication 800-22:** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- **Payment Card Industry (PCI):** Encrypting PIN PAD (EPP) Security Requirements Manual
- **Payment Card Industry (PCI):** Encrypting PIN PAD (EPP) Derived Test Requirements
- **Payment Card Industry (PCI):** POS PIN Entry Device Security Requirements Manual
- **Payment Card Industry (PCI):** POS PIN Entry Device Derived Test Requirements

Requirement/Standards Cross-Reference

PIN Security Requirement	International/Industry Standard(s)
<p>1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. TRSMs 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.</p> <p>All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.</p>	<p>A Tamper-Resistant Security Module (TRSM) must meet the requirements of a Physically Secure Device as defined in ISO 9564-1. 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 TRSM can be so certified 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). A TRSM (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.</p> <p>A TRSM 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.</p> <p>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 cleartext (unenciphered) PIN travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.</p> <p><i>See Appendix A for Visa specific requirements.</i></p>
<p>2 Cardholder PINs are processed in accordance with approved standards.</p> <p>a. All cardholder PINs processed online are</p>	<p>Online PIN translation must only occur using one of the allowed key management methods: DUKPT, Fixed Key, Master Key/Session Key.</p> <p>Online PINs must be encrypted using the TDEA Electronic Code Book (TECB) mode of operation as described in ANSI X9.52. For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in ANSI X9.52.</p>

PIN Security Requirement	International/Industry Standard(s)									
<p>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.</p>										
<p>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.</p>	<p>See section 7 of Book 2 of the EMV IC Card Specifications for Payment Systems and ISO 9564.</p> <table border="1" data-bbox="553 1045 1414 1850"> <thead> <tr> <th data-bbox="553 1045 841 1203">PIN submission method</th> <th data-bbox="841 1045 1128 1203">PED and IC reader integrated as a device meeting the requirements of 6.3 of ISO 9564-1</th> <th data-bbox="1128 1045 1414 1203">PED and IC reader not integrated as a device meeting the requirements of 6.3 of ISO 9564-1</th> </tr> </thead> <tbody> <tr> <td data-bbox="553 1203 841 1696"> <p>1. Enciphered PIN block submitted to the IC</p> </td> <td data-bbox="841 1203 1128 1696"> <p>The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p> </td> <td data-bbox="1128 1203 1414 1696"> <p>The PIN block shall be enciphered between the PED and the IC reader in accordance with ISO 9564-1 or enciphered using an authenticated encipherment key of the IC. The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p> </td> </tr> <tr> <td data-bbox="553 1696 841 1850"> <p>2. Plain text PIN block submitted to the IC</p> </td> <td data-bbox="841 1696 1128 1850"> <p>No encipherment is required.</p> </td> <td data-bbox="1128 1696 1414 1850"> <p>The PIN block shall be enciphered from the PED to the IC reader in accordance with ISO 9564-1.</p> </td> </tr> </tbody> </table>	PIN submission method	PED and IC reader integrated as a device meeting the requirements of 6.3 of ISO 9564-1	PED and IC reader not integrated as a device meeting the requirements of 6.3 of ISO 9564-1	<p>1. Enciphered PIN block submitted to the IC</p>	<p>The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p>	<p>The PIN block shall be enciphered between the PED and the IC reader in accordance with ISO 9564-1 or enciphered using an authenticated encipherment key of the IC. The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p>	<p>2. Plain text PIN block submitted to the IC</p>	<p>No encipherment is required.</p>	<p>The PIN block shall be enciphered from the PED to the IC reader in accordance with ISO 9564-1.</p>
PIN submission method	PED and IC reader integrated as a device meeting the requirements of 6.3 of ISO 9564-1	PED and IC reader not integrated as a device meeting the requirements of 6.3 of ISO 9564-1								
<p>1. Enciphered PIN block submitted to the IC</p>	<p>The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p>	<p>The PIN block shall be enciphered between the PED and the IC reader in accordance with ISO 9564-1 or enciphered using an authenticated encipherment key of the IC. The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.</p>								
<p>2. Plain text PIN block submitted to the IC</p>	<p>No encipherment is required.</p>	<p>The PIN block shall be enciphered from the PED to the IC reader in accordance with ISO 9564-1.</p>								
<p>3. For online</p>	<p>For secure transmission of the PIN from the point of PIN entry to the</p>									

PIN Security Requirement

International/Industry Standard(s)

interchange transactions, PINs are 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. Other ISO approved formats may be used.

card issuer, the encrypted PIN block format must comply with **ISO 9564-1 format 0, ISO 9564-1 format 1, or ISO 9564-1 format 3**. For ISO format 0 and 3, the cleartext 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 cipherblock (the reversibly encrypted PIN block). **ISO format 3** is the recommended format.

ISO format 1 and format 2 are formed by the concatenation of two fields: the plain text PIN field and the filler field.

PIN 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.

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.

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.

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 formats to ISO 0 format, or from ISO 3 format to ISO 3 format) must not allow a change of PAN.

The following illustrates translations from formats 0, 1 and 3:

Translation		ISO Format 0	ISO Format 1	ISO Format 3
From \ To				
ISO Format 0		CHANGE OF PAN NOT PERMITTED	NOT PERMITTED	CHANGE OF PAN NOT PERMITTED
ISO Format 1		PAN INPUT	PERMITTED	PAN INPUT
ISO Format 3		CHANGE OF PAN NOT PERMITTED	NOT PERMITTED	CHANGE OF PAN NOT PERMITTED

4. PINs are not stored except as part of a store-

Transactions may be stored and forwarded under certain conditions as noted in **ISO 9564-1**. When such conditions are present, any store-and-forward transaction PIN encrypted using a fixed key or

PIN Security Requirement	International/Industry Standard(s)
and-forward transaction, and only for the minimum time necessary.	<p>master /session key management method must be stored in encrypted form using a unique key not used for any other purpose. PINs encrypted using DUKPT do not require the use of a unique key for storage in a store and forward environment.</p> <p>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 <i>PCI Data Security Standards</i>.</p>
5. All keys and key components are generated using an approved random or pseudo-random process.	<p>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.</p> <p>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.</p>
6. Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	<p>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 cleartext key or key component as it is transferred between the key generation TRSM and the device or medium receiving the key or key component.</p> <p>Multi-use/purpose computing systems shall not be used for key generation where any cleartext secret or private key or component thereof appears in unprotected memory.</p> <p>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.</p> <p>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.</p>
7. Documented procedures exist and are demonstrably in use for all key generation	<p>Written key creation procedures must exist and all affected parties (key custodians, supervisory staff, technical management, etc.) are aware of those procedures. All key creation events must be documented.</p>

PIN Security Requirement	International/Industry Standard(s)
<p>processing.</p> <p>8. Secret or private keys are transferred by:</p> <p>a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, or</p> <p>b. Transmitting the key in ciphertext form.</p> <p>Public keys must be conveyed in a manner that protects their integrity and authenticity.</p>	<p>Specific techniques exist in how keys must be transferred in order to maintain their integrity. An encryption key, typically Key Encryption Keys (KEKs), must be transferred by physically forwarding the separate components of the key using different communication channels or transmitted in ciphertext form. Key components must be transferred in either tamper-evident packaging or within a TRSM. No person shall have access to any cleartext key during the transport process.</p> <p>A person with access to one component of a key, or to the media conveying this component, must not have access to any other component of this key or to any other medium conveying any other component of this key.</p> <p>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.</p> <p>Public keys must use a mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received.</p>
<p>9. Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:</p> <p>a. Under the continuous supervision of a person with authorized access to this component, or</p> <p>b. Locked in a security</p>	<p>Key components are the separate parts of a cleartext 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 a TRSM, 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 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.</p> <p>Procedures must require that plaintext key components stored in tamper-evident envelopes that show signs of tampering must result in the destruction and replacement of the set of components, as well</p>

PIN Security Requirement	International/Industry Standard(s)
<p>container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or</p> <p>c. In a physically secure TRSM.</p>	<p>as any keys encrypted under this key.</p> <p>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 packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components upon receipt.</p> <p>Pre-numbered, tamper evident bags shall be used for the conveyance of cleartext key components. Out of band mechanisms must exist to verify receipt of the appropriate bag numbers.</p>
<p>10. All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.</p>	<p>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.</p> <p>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.</p>
<p>11. Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.</p>	<p>Written procedures must exist and all affected parties are aware of those procedures. Conveyance or receipt of keys managed as components or otherwise outside a TRSM must be documented.</p>
<p>12. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.</p>	<p>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.</p> <p>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 or AES using a key size of at least 128 bits.</p> <p>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.</p> <p>Any other TRSM loaded with the same key components must</p>

PIN Security Requirement	International/Industry Standard(s)
	<p>combine all entered key components using the identical process.</p> <p>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.</p> <p>A public key technique for the distribution of symmetric secret keys must:</p> <ul style="list-style-type: none"> ▪ Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA). ▪ Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. ▪ Provide for mutual device authentication for both the host and the PED, 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. ▪ Meet all applicable requirements described in Annex A of this document.
<p>13. The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.</p>	<p>TRSM equipment must be inspected to detect evidence of monitoring and to ensure that the key loading occurs under dual control.</p> <p>A TRSM must transfer a plaintext 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).</p> <p>Plaintext keys and key components must be transferred into a TRSM 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 prior tampering which could lead to the disclosure of keys or sensitive data.</p> <p>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) results in either of the following:</p> <ul style="list-style-type: none"> ▪ 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, <i>or</i> ▪ All traces of the component are erased or otherwise

PIN Security Requirement	International/Industry Standard(s)
	<p>destroyed from the electronic medium.</p> <p>For keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:</p> <ul style="list-style-type: none"> ▪ The key-loading device is a physically secure TRSM, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; <i>and</i> ▪ The key-loading device is 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; <i>and</i> ▪ The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another TRSM. Such personnel must ensure that a key-recording device is not inserted between the TRSMs; <i>and</i> ▪ The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred. <p>The media upon which a component resides must be physically safeguarded at all times.</p> <p>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.</p> <p>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 is in the physical possession of only one entity for the minimum practical time until the component is entered into a TRSM.</p> <p>If the component is in human readable form (e.g., printed within a PIN-mailer type document), it is only visible 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 a TRSM.</p> <p>Printed key component documents are not opened until just prior to entry.</p> <p>The component is never 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.</p>
<p>14. All hardware and passwords used for key loading are</p>	<p>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</p>

PIN Security Requirement	International/Industry Standard(s)
managed under dual control.	<p>activities maintained for audit purposes. All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.</p> <p>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.</p>
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.	<p>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.</p> <p>The public key must have its authenticity and integrity ensured. A plaintext public key must only exist within a certificate, PKCS #10 or a secure cryptographic device. Public keys not stored in certificates, PKCS #10s or in a secure cryptographic device must be stored encrypted, or have a MAC (Message Authentication Code) created using the algorithm defined in ISO 9807, in order to ensure authenticity and integrity.</p>
16. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	<p>Written procedures must exist and all parties involved in cryptographic key loading are aware of those procedures. All key loading events must be documented.</p>
17. Unique secret cryptographic keys must be in use for each identifiable link between host computer systems.	<p>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.</p> <p>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).</p>
18. Procedures exist to prevent or detect the unauthorized substitution	<p>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, must be prevented. This will reduce the risk of an adversary substituting a key known only to them. These procedures must include investigating multiple</p>

PIN Security Requirement	International/Industry Standard(s)
(unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	<p>synchronization errors.</p> <p>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.</p>
19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	<p>Encryption keys must only be used 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 to be used also significantly strengthens the security of the underlying system.</p> <p>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.</p> <p>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.</p>
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.	<p>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.</p> <p>In a master/session key approach, the master key(s) and all session keys must be unique to each cryptographic device.</p> <p>If a transaction-originating terminal interfaces with more than one acquirer, the transaction-originating terminal TRSM 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.</p> <p>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.</p>
21. Keys used for enciphering PIN-Encryption keys, or for PIN Encryption, must never exist outside	<p>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.</p>

PIN Security Requirement	International/Industry Standard(s)
<p>of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.</p>	<p>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. 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 envelopes) to enable the token's owner to determine if a token was used by another person. In particular, key components for each specific custodian must be stored in separate secure containers.</p> <p>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.</p> <p>Printed or magnetically recorded key components must reside only within tamper-evident sealed envelopes so that the component cannot be ascertained without opening the envelope.</p> <p>DES keys that are used to encipher other keys or to encipher PINs, and which exist outside of a TRSM, must be enciphered using either:</p> <ul style="list-style-type: none"> ▪ The TDEA using at least double length keys or ▪ RSA using a key modulus of at least 1024 bits. <p>A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.</p> <p>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.</p>
<p>22. Procedures exist and are 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</p>	<p>Key components are 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 TRSM has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.</p> <p>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.</p> <p>Procedures must include a documented escalation process and</p>

PIN Security Requirement	International/Industry Standard(s)
the original key.	<p>notification to organizations that currently share or have previously shared the key(s). The procedures should include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, and so forth.</p> <p>The compromise of a key requires 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. Known or suspected substitution of a secret key requires replacement of that key and any associated key encipherment keys. Specific events must be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Missing cryptographic devices. ▪ Tamper-evident seals or envelope numbers or dates and times not agreeing with log entries. ▪ Tamper-evident seals or envelopes that have been opened without authorization or show signs of attempts to open or penetrate. ▪ Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities. <p>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.</p>
23. Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage.	<p>A secret key used to encrypt a PIN 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. However, 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.</p> <p>Variants of an MFK must not be used external to the (logical) configuration that houses the MFK itself.</p>
24. Secret and private keys and key	<p>Instances of keys that are no longer used or that have been replaced by a new key must be destroyed. Keys maintained on paper must be</p>

PIN Security Requirement	International/Industry Standard(s)
<p>components that are no longer used or have been replaced are securely destroyed.</p>	<p>burned, pulped or shredded in a cross-cut shredder. If the key is stored in EEPROM, the key should be overwritten with binary 0s (zeros) a minimum of three times. If the key is stored on EPROM or PROM, the chip should be smashed into many small pieces and scattered. 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.</p> <p>The procedures for destroying keys that are no longer used or that have been replaced by a new key must be documented.</p> <p>Key encipherment key components used for the conveyance of working keys must be destroyed after successful loading and validation as operational.</p>
<p>25. Access to secret and private cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.</p>	<p>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.</p>
<p>26. Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.</p>	<p>At a minimum, the logs must include the date and time in/out, purpose of access, signature of custodian accessing the component, envelope number (if applicable).</p>
<p>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</p>	<p>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). Backups (including cloning) must require a minimum of two authorized individuals to enable the process.</p> <p>Note—it is not a requirement to have backup copies of key components or keys.</p>

PIN Security Requirement	International/Industry Standard(s)
<p>backups must exist only in one of the allowed storage forms for that key.</p>	
<p>28. Documented procedures exist and are demonstrably in use for all key administration operations.</p>	<p>Written procedures must exist and all affected parties are aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as:</p> <ul style="list-style-type: none"> ○ Security awareness training. ○ Role definition - nominated individual with overall responsibility. ○ Background checks for personnel. <p>Management of personnel changes, including revocation of access control and other privileges when personnel move.</p>
<p>29. PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.</p>	<p>HSMs and PEDs must only be placed into service 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.</p> <p>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.</p> <p>Dual control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or backup devices. Procedural controls may exist to support the prevention and detection of substituted cryptographic devices, but cannot supplant the implementation of dual control mechanisms, which may be a combination of physical barriers and logical controls.</p> <p>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 the following:</p> <ol style="list-style-type: none"> 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.

PIN Security Requirement	International/Industry Standard(s)
	<p>b. Cryptographic devices are shipped from the manufacturer's facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs.</p> <p>c. The manufacturer's facility loads into each cryptographic device a secret, device-unique "transport-protection token." The TRSM 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.</p> <p>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.</p> <ul style="list-style-type: none">▪ 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.▪ Controls must exist and be in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed. <p>Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:</p> <ul style="list-style-type: none">▪ protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it, and▪ detect lost or stolen equipment. <p>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.</p> <p>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.</p> <p>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).</p> <p>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.</p>

PIN Security Requirement	International/Industry Standard(s)
	<p>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.</p>
<p>30. Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.</p>	<p>If a TRSM 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.</p> <ul style="list-style-type: none"> ▪ 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). ▪ Key and data storage must be zeroized when a device is decommissioned. <p>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.</p>
<p>31. Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following:</p> <ol style="list-style-type: none"> a. Dual access controls are required to enable the key encryption function. b. Physical protection of 	<p>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.</p> <p>Unauthorized use of secure cryptographic devices (including key loading devices) shall be prevented or detected by:</p> <ul style="list-style-type: none"> • 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; • 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.

PIN Security Requirement	International/Industry Standard(s)
the equipment (e.g., locked access to it) under dual control.	
32. Documented procedures exist and are 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.	<p>Written procedures must exist and all affected parties are 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.</p> <p>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.</p>

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 are 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.

Certification Authority requirements apply to all entities signing public keys, whether in X.509 certificate based schemes or other designs. For purposes of these requirements, a certificate is any digitally signed value containing a public key.

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 1	PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.
No change.	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 are 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) POS PIN Entry Device Derived Test Requirements and the Payment Card Industry (PCI) Encrypting PIN Pad (EPP) Derived Test Requirements. Key-generation methods must meet the current ANSI and ISO standards for the algorithm(s) in question. Secret and private cryptographic keys are unique and are equally likely to be generated. The probability that any two cryptographic keys are identical is negligible.
6. Compromise of the key-generation process is not possible without collusion between at	Key pairs must either be generated by the device which will use the key pair, or if generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device which will use the key pair occurs.

<p>least two trusted individuals.</p>											
<p>Objective 3</p>	<p>Keys are conveyed or transmitted in a secure manner.</p>										
<p>10. All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.</p>	<p>Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used.</p> <p>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:</p> <table border="1" data-bbox="511 604 1328 772"> <thead> <tr> <th>Algorithm</th> <th>DES</th> <th>RSA</th> <th>Elliptic Curve</th> <th>DSA</th> </tr> </thead> <tbody> <tr> <td>Minimum key size in number of bits</td> <td>112</td> <td>1024</td> <td>160</td> <td>1024/160</td> </tr> </tbody> </table> <p>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. AES may also be used with a key size of at least 128 bits.</p> <p>For Diffie-Hellman implementations:</p> <p>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 generates 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 <i>PCI PED POS (EPP) Derived Test Requirements</i>.</p> <p>Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES – see <i>ISO 16609 - Banking -- Requirements for message authentication using symmetric techniques</i> – Method 3 should be used).</p> <p>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.</p>	Algorithm	DES	RSA	Elliptic Curve	DSA	Minimum key size in number of bits	112	1024	160	1024/160
Algorithm	DES	RSA	Elliptic Curve	DSA							
Minimum key size in number of bits	112	1024	160	1024/160							
<p>Objective 4</p>	<p>Key loading to hosts and PIN entry devices is handled in a secure manner.</p>										
<p>15. The loading of keys or key components must</p>	<p>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</p>										

<p>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.</p>	<p>must occur immediately prior to any key establishment. 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.</p> <p>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.</p> <p>Within an implementation design, there shall be no means available for “man in middle” attacks. System implementations must be designed and implemented to prevent replay attacks</p> <p>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.</p>
<p>Objective 5</p>	<p>Keys are used in a manner that prevents or detects their unauthorized usage.</p>
<p>18. Procedures 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.</p>	<p>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.</p> <p>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.</p>
<p>19. Cryptographic keys are only used for their sole intended purpose and are never shared between</p>	<p>Keys 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.</p> <p>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- <i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification</i></p>

<p>production and test systems.</p>	<p><i>Practices Framework</i> for an example of content):</p> <ul style="list-style-type: none"> • 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 cannot be used for any other 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. • CAs that issue certificates to other CAs cannot be used to issue certificates to EPPs or PEDs. • Public keys are only used for either encryption or for verifying digital signatures, but not both (except for EPPs/PEDs). • Private keys can only be used for decryption or for creating digital signatures, but not both (except for EPPs/PEDs). <p>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.</p> <p>CA and KDH private keys cannot be shared between devices except for load balancing and disaster recovery. EPP and POS PED private keys cannot be shared.</p>
<p>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.</p>	<p>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).</p> <p>Key pairs must be unique per device including key distribution hosts (except as otherwise provided for), EPPs and POS PEDs.</p>
<p>Objective 6</p>	<p>Keys are administered in a secure manner.</p>
<p>21. Keys used for</p>	<p>Private keys used to sign certificates, certificate status lists,</p>

<p>enciphering PIN Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.</p>	<p>messages or for secret key protection must only exist in one of the following forms:</p> <ul style="list-style-type: none"> • Within a secure cryptographic device, e.g., a HSM or EPP/PED that meets applicable PCI requirements for such a device • Encrypted using an algorithm and key size of equivalent or greater strength • As components using a recognized (e.g., Shamir) secret sharing scheme
<p>22. Procedures exist and are 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.</p>	<p>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.</p> <p>Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.</p> <p>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</p> <p>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 should 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.</p> <p>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.</p> <p>Minimum cryptographic strength for the CA system shall be:</p> <ul style="list-style-type: none"> • Root – minimum RSA 2048 bits or equivalent • Subordinate CAs, EPP/PED devices and KDHS – minimum RSA 1024 bits or equivalent <p>The following key pair lifecycle shall exist:</p> <ul style="list-style-type: none"> • Expiration of EPP/PED keys within twelve (12) months after the

	<p>expected end-of-life of the device</p> <ul style="list-style-type: none"> • Expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.
<p>25. Access to secret or private cryptographic keys and key material must be limited to a need to-know basis so that the fewest number of key custodians are necessary to enable their effective use.</p>	<p>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.</p> <p>Key component custodians must be provided with a list of responsibilities, and each user must sign a statement acknowledging these concerns before receiving custody of key components or enablers (for example, PINs) for keys or their components. The forms must specifically authorize the custodian and identify the custodian’s responsibilities for safeguarding key components or other keying material entrusted to them.</p> <p>The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include that:</p> <ul style="list-style-type: none"> • 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 only used for certificate issuance, revocation, or both certificate issuance and revocation. Outside network access shall exist <u>only</u> for the purposes of “pushing” certificate status information to relying parties (e.g., EPPs, KDHs, POS PEDs) • 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). • Non-console access requires two-factor authentication. This also pertains to the use of remote console access. • 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 • CA certificate (for EPP/PED/KDH authentication and validity status checking) signing keys must be enabled under multilevel control. • Certificate requests may be vetted (approved) using single user logical access to the RA application. <p>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 split knowledge and dual control. At a minimum, there shall be multi-person control for operational</p>

procedures such that no one person can gain control over the CA signing key(s).

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.

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.

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.

Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.

Logical events are divided into operating system and CA application events. For both events the following will be recorded in the form of an audit record:

- date and time of the event,
- identity of the entity and/or user that caused the event,
- type of event, and
- success or failure of the event.

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.

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:

- Minimum length of six characters using a mix of alphabetic, numeric, and special characters.
- System enforced expiration life not to exceed thirty days.
- System enforced minimum life of at least one day.
- Maximum invalid attempts not to exceed five before suspending the user ID.

	<ul style="list-style-type: none"> • System enforced pass phrase history preventing the reuse of any pass phrase used in the last twelve months. • Initial assigned pass phrases are pre-expired (user must replace at first logon). • Vendor default pass phrases are changed at installation and where applicable, for updates. • 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. • The embedding of pass phrases in shell scripts, command files, communication scripts, etc., is strictly prohibited. <p>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 associated PINs/pass phrases to enable their usage. The PINs/pass phrases must be at least six characters.</p> <p>The on-line Certificate Processing system components must be protected by a firewall(s) and intrusion detection systems from all unauthorized access including casual browsing and deliberate attacks.</p> <p>Firewalls must minimally be configured to:</p> <ul style="list-style-type: none"> • Deny all services not explicitly permitted. • Disable or remove all unnecessary services, protocols, and ports. • Fail to a configuration that denies all services, and requires a firewall administrator to re-enable services after a failure. • Disable source routing on the firewall and external router. • Not accept traffic on its external interfaces that appears to be coming from internal network addresses. • Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action could be taken. • Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc. must be deleted or disabled. <p>Online systems must employ individually or in combination network and host based Intrusion Detection Systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and Web, as well as the intervening segments must be covered.</p>
<p>28. Documented procedures exist and are demonstrably in use for all</p>	<p>CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key distribution systems.</p> <p>The certificate issuing and management authority may consist of one or more devices that are responsible for the issuance, revocation, and</p>

<p>key administration operations.</p>	<p>overall management of certificates and certificate status information.</p> <p>Each CA operator must develop a certification practice statement (CPS) - (See RFC 3647- <i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> 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.</p> <p>Documented procedures exist and are 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.</p> <p>For CA and KDH certificate signing requests, including certificate or key validity status changes (e.g., revocation, suspension, replacement), verification must include validation that:</p> <ul style="list-style-type: none"> • The entity submitting the request is who it claims to be • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate signing request has been transferred from the certificate request's originating entity to the RA in a secure manner. • RAs must 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.
<p>Objective 7</p>	<p>Equipment used to process PINs and keys is managed in a secure manner.</p>
<p>31. Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection</p>	<p>CA and RA database and application servers, and cryptographic devices must reside in a physically secure and monitored environment.</p> <p>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. Documented procedures exist for the granting and revocation of access privileges, which include reviewing manual or electronic logs of accesses. Specifically, Certificate Processing operations must:</p> <ul style="list-style-type: none"> • Operate in a physically secure dedicated room not used for any other business activities but certificate operations (stand-alone). • Provide for the documentation of all access granting, revocation, and review procedures and of specific access authorizations,

<p>takes the form of either or both of the following:</p> <p>a. Dual access controls are required to enable the key encryption function.</p> <p>b. Physical protection of the equipment (e.g., locked access to it) under dual control.</p>	<p>whether logical or physical.</p> <ul style="list-style-type: none">• 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.• Use electronically (e.g., badge and/or biometric) managed dual occupancy.• Allow access only to pre-designated staff with defined business needs and duties. Visitors must be authorized and escorted at all times.• Use CCTV monitoring (motion activated systems that are separate from the intrusion detection system may be used) of the CA operating platform which 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.• 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 forty-five days. Systems using digital recording mechanism must have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent forty-five day period.• Provide for continuous (motion activated systems may be used) lighting for cameras.• 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.• 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 and time in and out and purpose of visit. The person escorting the visitor must also initial the log.• Tie all access control and monitoring systems to an Uninterruptible Power Source (UPS).• Document all alarm events. Under no circumstances shall an individual sign-off on an alarm event in which they were involved.• Establish that the use of any emergency entry or exit mechanism must cause an alarm event.• Require that all alarms for physical intrusion necessitate an active
---	---

	<p>response by personnel assigned security duties within thirty minutes.</p> <ul style="list-style-type: none">• 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, then the process must occur at least quarterly. Documentation of the synchronization must be retained for at least a one-year period.
	<p>Root CAs and their equivalent operations must exist only in a high security environment.</p> <p>CAs and their associated RA servers that issue certificates to Key Distribution Hosts or subordinate CAs must additionally meet the following:</p> <ul style="list-style-type: none">• 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., in a caged environment.• This physically secure environment must have a 24/7 intrusion detection system:<ul style="list-style-type: none">○ The intrusion detection system must have 24-hour monitoring (including UPS).○ The intrusion detection system must include the use of motion sensors.○ The system must be capable of and perform recording and archiving of alarm activity.○ Alarm activity must include unauthorized entry attempts or any deliberate or inadvertent actions that disable the intrusion detection system.○ All logged alarm activity information must be reviewed and resolved.• 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.• Use three layers of physical security in the CA facility with increasing levels of access control for each of the following levels:<ul style="list-style-type: none">Level One Barrier:<p>This level consists of the entrance to the facility. The building or secure facility entrance will only allow the entrance of 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.</p>Level Two Barrier:

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.

Level Three Barrier:

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 should correlate to separate organizational units.

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.

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:

- Name and signature of the individual,
- Participants Organization,
- Date and time in and out,
- Reason for visit.
- 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.

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.

Automated login and logout enforcement of personnel is required at level three. This level 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 thirty seconds. For time of single occupancy exceeding thirty 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. 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.

Key injection systems that do not use secure cryptographic hardware are inherently less secure. 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.

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.

Note: MasterCard does not permit the exposure of clear symmetric cryptographic keys or private asymmetric keys outside of a Tamper Resistant Security Module (TRSM), Host Security Module (HSM), Encrypting PIN Pads (EPPs), or PIN Entry Devices (PEDs). MasterCard does require the exclusive use of PCI lab-tested PIN Entry Devices (PEDs) or Encrypting PIN Pads (EPPs).

MasterCard does not permit the loading of keys from devices that do not comply with the requirements for Tamper Resistant Security Modules as stated in the Control Objectives. Specifically, the use of personal computers or other non-secure devices for key injection as described in requirement #13 is not allowed.

Other requirements related to the physical protection and management of the secure facility still apply.

Requirement/Standards Cross-Reference

Key Injection Facility Security Requirement	International/Industry Standard(S)
<p>1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. TRSMs 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.</p> <p>All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.</p>	<p>Key Injection Facilities must only inject keys into equipment that conforms to the requirements for TRSMs.</p> <p>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 TRSMs.</p> <p>A Tamper-Resistant Security Module (TRSM) must meet the requirements of a Physically Secure Device as defined in ISO 9564-1. 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 TRSM can be so certified 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). A TRSM (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.</p> <p>A TRSM 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.</p> <p>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 cleartext (unenciphered) PIN travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.</p> <p><i>See Appendix A for Visa specific requirements.</i></p>
<p>5. All keys and key components are generated using an</p>	<p>Where the key injection platform includes features that generate keys, those keys must be generated in</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
<p>approved random or pseudo-random process.</p>	<p>compliance with these requirements.</p> <p>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 <i>PCI PIN Security Requirements</i>.</p> <p>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.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <ul style="list-style-type: none"> ▪ 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) POS PIN Entry Device Derived Test Requirements and the Payment Card Industry (PCI) Encrypting PIN Pad (EPP) Derived Test Requirements. ▪ Key-generation methods must meet the current ANSI and ISO standards for the algorithm(s) in question. <p>Secret and private cryptographic keys are unique and are equally likely to be generated. The probability that any two cryptographic keys are identical is negligible.</p>
<p>6. Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.</p>	<p>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.</p> <p>Some key injection platforms use Personal Computer (PC) based software applications <i>without</i> TRSMs for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>of some of the weaknesses could be possible without collusion. Therefore, Key Injection Facilities that use PC-based key loading software platforms <i>without</i> TRSMs must at a minimum implement the compensating controls outlined in requirement #13.</p> <p>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 cleartext key or key component as it is transferred between the key generation TRSM and the device or medium receiving the key or key component.</p> <p>Multi-use/purpose computing systems shall not be used for key generation where any cleartext secret or private key or component thereof appears in unprotected memory.</p> <p>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.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>Key pairs must either be generated by the device which will use the key pair, or if generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device which will use the key pair occurs.</p>
<p>7. Documented procedures exist and are demonstrably in use for all key generation processing.</p>	<p>Written key creation procedures must exist and all affected parties (key custodians, supervisory staff, technical management, etc.) are aware of those procedures. All key creation events performed by a Key Injection Facility must be documented.</p>
<p>8. Secret or private keys are transferred by:</p> <p>a. Physically forwarding the key as at least two separate key shares or full-</p>	<p>Keys conveyed <u>to</u> a Key Injection Facility must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:</p> <ul style="list-style-type: none"> • Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT

Key Injection Facility Security Requirement	International/Industry Standard(S)
<p>length components (hard copy, smart card, TRSM) using different communication channels, or b. Transmitting the key in ciphertext form.</p> <p>Public keys must be conveyed in a manner that protects their integrity and authenticity.</p>	<p>key management method,</p> <ul style="list-style-type: none"> • Key Encryption Keys used to encrypt the BDKeys when the BDKeys are conveyed between entities (e.g., from the BDKey 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), • Terminal Master Keys (TMKs) used in the Master Key/Session Key key management method, • PIN Encryption Keys used in the fixed transaction key method, • Public keys used in remote key establishment and distribution applications. <p>Keys conveyed <i>from</i> a Key Injection Facility (including facilities that are a device manufacturer) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:</p> <ul style="list-style-type: none"> • 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), • Device manufacturer's authentication key loaded into the HSM for supporting certain key establishment and distribution applications protocols (if applicable). <p>Specific techniques exist in how keys must be transferred in order to maintain their integrity. An encryption key, typically Key Encryption Keys (KEKs), must be transferred by physically forwarding the separate components of the key using different communication channels or transmitted in ciphertext form. Key components must be transferred in either tamper-evident packaging or within a TRSM. No person shall have access to any cleartext key during the transport process.</p> <p>A person with access to one component of a key, or to the media conveying this component, must not have access to any other component of this key or to any other medium conveying any other component of this key.</p> <p>Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>components for a specific key on different days using the same communication channel.</p> <p>Public keys must use a mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received.</p>
<p>9. Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:</p> <ul style="list-style-type: none"> a. Under the continuous supervision of a person with authorized access to this component, or b. Locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or c. In a physically secure TRSM. 	<p>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 BDKeys when the BDKeys are conveyed between entities (e.g., from the BDKey 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 BDKeys themselves, and Terminal Master Keys used in the Master Key/Session Key key management method.</p> <p>Key components are the separate parts of a cleartext key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, key components exist for KEKeys, 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 a TRSM, 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.</p> <p>Procedures must require that plaintext key components stored in tamper-evident 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.</p> <p>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</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)														
	<p>component. Mechanisms must exist to ensure that only authorized custodians place key components into tamper-evident packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components upon receipt.</p> <p>Pre-numbered, tamper evident bags shall be used for the conveyance of cleartext key components. Out of band mechanisms must exist to verify receipt of the appropriate bag numbers.</p>														
<p>10. All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.</p>	<p>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 BDKeys when the BDKeys are conveyed between entities (e.g., from the BDKey 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).</p> <p>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.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>Cryptographic algorithms used for key transport, exchange or establishment must use key lengths that are deemed acceptable for the algorithm being used. 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:</p> <table border="1" data-bbox="711 1703 1430 1913"> <thead> <tr> <th data-bbox="711 1703 933 1797" rowspan="2">Algorithm</th> <th colspan="4" data-bbox="933 1703 1430 1751">Elliptic</th> </tr> <tr> <th data-bbox="933 1751 1024 1797">DES</th> <th data-bbox="1024 1751 1122 1797">RSA</th> <th data-bbox="1122 1751 1252 1797">Curve</th> <th data-bbox="1252 1751 1430 1797">DSA</th> </tr> </thead> <tbody> <tr> <td data-bbox="711 1797 933 1913">Minimum key size in number of bits</td> <td data-bbox="933 1797 1024 1913">112</td> <td data-bbox="1024 1797 1122 1913">1024</td> <td data-bbox="1122 1797 1252 1913">160</td> <td data-bbox="1252 1797 1430 1913">1024/160</td> </tr> </tbody> </table>	Algorithm	Elliptic				DES	RSA	Curve	DSA	Minimum key size in number of bits	112	1024	160	1024/160
Algorithm	Elliptic														
	DES	RSA	Curve	DSA											
Minimum key size in number of bits	112	1024	160	1024/160											

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>AES may also be used with a key size of at least 128 bits.</p> <p>For Diffie-Hellman implementations:</p> <ul style="list-style-type: none"> • 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 generates 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 PCI PED POS (EPP) Derived Test Requirements. • 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).
<p>11. Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.</p>	<p>Written procedures must exist and all affected parties are aware of those procedures. Conveyance or receipt of keys managed as components or otherwise outside a TRSM must be documented. All key conveyance events performed by a Key Injection Facility must be documented.</p>
<p>12. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.</p>	<p>Key Injection Facilities must load keys (unencrypted symmetric keys must be loaded as key components) using dual control and split knowledge. Such keys include, but are not limited to:</p> <ul style="list-style-type: none"> • Derived Unique Key Per Transaction (DUKPT) Base Derivation Keys (BDKs) used in the DUKPT key management method, • 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

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>from a merchant to a third party that is injecting keys on their behalf),</p> <ul style="list-style-type: none"> • Terminal Master Keys (TMKs) used in the Master Key/Session Key key management method, • PIN Encryption Keys used in the fixed transaction key method, • Master Keys for Key Injection platforms and systems that include hardware devices (TRSMs) for managing (e.g., generating and storing) the keys used to encrypt other keys for storage in the Key Injection platform system, • Public and private key pairs loaded into the PEDs' Encrypting PIN Pads (EPPs) for supporting remote key establishment and distribution applications, • Digitally signed EPP public key(s) that are signed by a device manufacture's private key and subsequently loaded into the EPP for supporting certain key establishment and distribution applications protocols (if applicable), • Device manufacturer's authentication key loaded into the EPP for supporting certain key establishment and distribution applications protocols (if applicable), <p>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):</p> <ul style="list-style-type: none"> • 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. • 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. • Key injection platform applications that force the entry of multiple key components and the implementation of procedures that involve multiple

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>key custodians that store and access key components under dual control and split knowledge mechanisms.</p> <ul style="list-style-type: none"> • Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry. <p>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.</p> <p>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 or AES using a key size of at least 128 bits.</p> <p>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.</p> <p>Any other TRSM loaded with the same key components must combine all entered key components using the identical process.</p> <p>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.</p> <p>A public key technique for the distribution of symmetric secret keys must:</p> <ul style="list-style-type: none"> • Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA). • Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Provide for mutual device authentication for both the host and the PED, including assurance to the host that the PED actually has (or actually can)

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key.</p> <ul style="list-style-type: none"> • Meet all applicable requirements described in Annex A of this document.
<p>13. The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component. TRSM equipment must be inspected to detect evidence of monitoring and to ensure that the key loading occurs under dual control.</p>	<p>Key Injection Facilities must ensure key loading mechanisms are not subject to disclosure of key components or keys.</p> <p>Some key injection platforms use Personal Computer (PC) based software applications <i>without</i> TRSMs for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. These weaknesses include:</p> <ul style="list-style-type: none"> • XOR'ing of key components is performed in software. • Cleartext keys and components can reside in software during the key loading process. • Some systems require only a single password. • Some systems store the keys (e.g., BDKs, TMKs) on removable diskettes or smart cards. These keys are in the clear with some systems. • 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. • Data can be recorded in the PC's non-volatile storage. • Software Trojan Horses or keyboard sniffers can be installed on PCs. <p>Key Injection Facilities that use PC-based key loading software platforms without TRSMs must minimally implement the following compensating controls:</p> <ul style="list-style-type: none"> • PCs must be: <ul style="list-style-type: none"> ○ Stand-alone (i.e., without modems, not connected to a LAN or WAN, not capable of wireless connections, etc.), ○ Dedicated to only the key loading function (e.g., there must not be any other application software installed), and ○ Located in a physically secure room that is dedicated to key loading activities. • All hardware used in key loading (including the PC)

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Logs of access to the room from a badge access system, ○ Logs of access to the room from a manual sign-in sheet, ○ User sign-on logs on the PC at the operating system level, ○ User sign-on logs on the PC at the application level, ○ Logs of the device IDs and serial numbers that are loaded along with the date and time and the individuals performing the key injection, ○ Video surveillance logs. • Cable attachments and the PC must be examined before each use to ensure the equipment is free from tampering. • The PC must be started from a powered-off position every time key loading activities occur. • The software application must load keys without recording any cleartext values on portable media or other unsecured devices. • Keys must not be stored except within a TRSM. • 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. • The key injection personnel must not have system's

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>administration capability at either the O/S or the application level on the PC.</p> <ul style="list-style-type: none"> • The PC must not be able to boot from external media (e.g., floppies or CDs). It must boot from the hard drive only. • 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. • If the PC application stores keys (e.g., BDKeys or TMKeys) on diskette or smart cards, the diskette and smart cards 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 (note- for DUKPT implementations, the BDKey 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 diskettes or smart cards must ensure the passwords are maintained under dual control and split knowledge. • Manufacturer's default passwords for PC-based applications must be changed. <p>A TRSM must transfer a plaintext 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).</p> <p>Plaintext keys and key components must be transferred into a TRSM 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</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>has not been subject to any prior tampering which could lead to the disclosure of keys or sensitive data. 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) results in either of the following:</p> <ul style="list-style-type: none"> • 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 • All traces of the component are erased or otherwise destroyed from the electronic medium. <p>For keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:</p> <ul style="list-style-type: none"> • The key-loading device is a physically secure TRSM, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; and • The key-loading device is 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 • The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another TRSM. Such personnel must ensure that a key-recording device is not inserted between the TRSMs; and • The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred. <p>The media upon which a component resides must be physically safeguarded at all times.</p> <p>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.</p> <p>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 is in the physical</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>possession of only one entity for the minimum practical time until the component is entered into a TRSM.</p> <p>If the component is in human readable form (e.g., printed within a PIN-mailer type document), it is only visible 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 a TRSM.</p> <p>Printed key component documents are not opened until just prior to entry.</p> <p>The component is never 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.</p>
<p>14. All hardware and passwords used for key loading are managed under dual control.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p>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.</p>	<p>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.</p> <p>The public key must have its authenticity and integrity ensured. A plaintext public key must only exist within a certificate, PKCS #10 or a secure cryptographic device. Public keys not stored in certificates, PKCS #10s or in a secure cryptographic device must be stored encrypted, or have a MAC (Message Authentication Code) created using the algorithm defined in ISO 9807, in order to ensure authenticity and integrity.</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>The devices (EPPs/PEDs and 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. 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.</p> <p>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.</p> <p>Within an implementation design, there shall be no means available for “man in the middle” attacks. System implementations must be designed and implemented to prevent replay attacks.</p> <p>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.</p>
<p>16. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.</p>	<p>Written procedures must exist and all parties involved in cryptographic key loading are aware of those procedures. All key loading events performed by a Key Injection Facility must be documented.</p>
<p>18. Procedures 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.</p>	<p>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:</p> <ul style="list-style-type: none"> • 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

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>loading application, video surveillance of activities in the key injection room, physical access to secret or private cryptographic key components or shares, etc.</p> <ul style="list-style-type: none"> • All devices loaded with keys must be tracked at each key loading session by serial number. • Unloaded devices must be managed in accordance with requirement #29. • 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. <p>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, must be prevented. This will reduce the risk of an adversary substituting a key known only to them. These procedures must include investigating multiple synchronization errors.</p> <p>These procedures must include investigating multiple synchronization errors.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>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 Key Distribution Hosts (KDHs) for key management, normal transaction processing and certificate (entity) status checking.</p> <p>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.</p>
<p>19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.</p>	<p>Key Injection Facilities must have a separate test system for the injection of test keys.</p> <ul style="list-style-type: none"> • Test keys must not be injected using the production platform and test keys must not be injected into production equipment.

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<ul style="list-style-type: none"> • 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. • Keys used for signing of test certificates must be test keys. • Keys used for signing of production certificates must be production keys. <p>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 to be used also significantly strengthens the security of the underlying system.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>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.</p> <p>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-<i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> for an example of content):</p> <ul style="list-style-type: none"> • 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 cannot be used for any other 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-

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>signed roots) may be for combined usage, or may exist as separate keys dedicated to either certificate signing or certificate (entity) status checking.</p> <ul style="list-style-type: none"> • CAs that issue certificates to other CAs cannot be used to issue certificates to EPPs or PEDs. • Public keys are only used for either encryption or for verifying digital signatures, but not both (except for EPPs/PEDs). • Private keys can only be used for decryption or for creating digital signatures, but not both (except for EPPs/PEDs). <p>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.</p> <p>CA and KDH private keys cannot be shared between devices except for load balancing and disaster recovery. EPP and POS PED private keys cannot be shared.</p>
<p>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.</p>	<p>Key Injection Facilities must ensure that unique keys are loaded into each device. The same key(s) must not be loaded into multiple devices.</p> <p>Key Injection Facilities that load DUKPT keys must use separate BDKs for different entities.</p> <p>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 Facility must ensure that any one given key cannot be derived for multiple devices except by chance.</p> <p>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.</p> <p>In a master/session key approach, the master key(s) and all session keys must be unique to each cryptographic device.</p> <p>If a transaction-originating terminal interfaces with more</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>than one Acquirer, the transaction-originating terminal TRSM 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.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>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).</p> <p>Key pairs must be unique per device including key distribution hosts (except as otherwise provided for), EPPs and POS PEDs.</p>
<p>21. Keys used for enciphering PIN-Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.</p>	<p>Key Injection Facilities must ensure that KEKs and PIN Encryption Keys do not exist outside of TRSMs except when encrypted or stored under dual control and split knowledge.</p> <p>Some key injection platforms use Personal Computer (PC) based software applications <i>without</i> TRSMs 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 <i>without</i> TRSMs must minimally implement the compensating controls outlined in requirement #13.</p> <p>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.</p> <p>Components for a specific key that are stored in separate envelopes, but within the same secure</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>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 envelopes) to enable the token's owner to determine if a token was used by another person. In particular, key components for each specific custodian must be stored in separate secure containers.</p> <p>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.</p> <p>Printed or magnetically recorded key components must reside only within tamper-evident sealed envelopes so that the component cannot be ascertained without opening the envelope.</p> <p>DES keys that are used to encipher other keys or to encipher PINs, and which exist outside of a TRSM, must be enciphered using either:</p> <ul style="list-style-type: none"> • The TDEA using at least double length keys or • RSA using a key modulus of at least 1024 bits. <p>A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.</p> <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>Private keys used to sign certificates, certificate status lists, messages or secret key protection must only exist in one of the following forms:</p> <ul style="list-style-type: none"> • Within a secure cryptographic device, e.g. a HSM

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>or EPP/PED that meets applicable PCI requirements for such a device</p> <ul style="list-style-type: none"> • Encrypted using an algorithm and key size of equivalent or greater strength • As components using a recognized (e.g., Shamir) secret sharing scheme
<p>22. Procedures exist and are 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.</p>	<p>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 are aware of those procedures. All key compromise procedures must be documented.</p> <p>Key components are 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 TRSM has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.</p> <p>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.</p> <p>Procedures must include a documented escalation process and notification to organizations that currently share or have previously shared the key(s). The procedures should include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, and so forth.</p> <p>The compromise of a key requires 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.</p> <p>Known or suspected substitution of a secret key requires replacement of that key and any associated key encipherment keys.</p> <p>Specific events must be identified that would indicate a compromise may have occurred. Such events may</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>include, but are not limited to:</p> <ul style="list-style-type: none"> • Missing cryptographic devices. • Tamper-evident seals or envelope numbers or dates and times not agreeing with log entries. • Tamper-evident seals or envelopes that have been opened without authorization or show signs of attempts to open or penetrate. • Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities. <p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <ul style="list-style-type: none"> ▪ 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. ▪ Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs. ▪ 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. ▪ 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 should 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. ▪ The compromised CA must notify any superior or

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>Minimum cryptographic strength for the CA system shall be:</p> <ul style="list-style-type: none"> • Root – minimum RSA 2048 bits or equivalent • Subordinate CAs, EPP/PED devices and KDHS – minimum RSA 1024 bits or equivalent <p>The following key pair lifecycle shall exist:</p> <ul style="list-style-type: none"> • Expiration of EPP/PED keys within twelve (12) months after the expected end-of-life of the device • Expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.
<p>23. Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage.</p>	<p>A secret key used to encrypt a PIN 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. However, 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.</p>
<p>24. Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.</p>	<p>Instances of keys that are no longer used or that have been replaced by a new key must be destroyed. Keys maintained on paper must be burned, pulped or shredded in a cross-cut shredder. If the key is stored in EEPROM, the key should be overwritten with binary 0s (zeros) a minimum of three times. If the key is stored on EPROM or PROM, the chip should be smashed into many small pieces and scattered. 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.</p> <p>The procedures for destroying keys that are no longer used or that have been replaced by a new key must be documented.</p> <p>Key encipherment key components used for the conveyance of working keys must be destroyed after</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	successful loading and validation as operational.
<p>25. Access to secret and private cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.</p>	<p>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.</p> <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>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.</p> <p>Key component custodians must be provided with a list of responsibilities, and each user must sign a statement acknowledging these concerns before receiving custody of key components or enablers (for example, PINs) for keys or their components. The forms must specifically authorize the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them.</p> <p>The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include that:</p> <ul style="list-style-type: none"> • 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 only used 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). • 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).

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<ul style="list-style-type: none"> • Non-console access requires two-factor authentication. This also pertains to the use of remote console access. • 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. • CA certificate (for EPP/PED/KDH authentication and validity status checking) signing keys must be enabled under multilevel control. • Certificate requests may be vetted (approved) using single user logical access to the RA application. <p>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 split knowledge and 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).</p> <p>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.</p> <p>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.</p> <p>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</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>media). The logs must be protected from alteration and destruction, and archived in accordance with all regulatory and legal requirements.</p> <p>Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.</p> <p>Logical events are divided into operating system and CA application events. For both events the following will be recorded in the form of an audit record:</p> <ul style="list-style-type: none"> • Date and time of the event, • Identity of the entity and/or user that caused the event, • Type of event, and • Success or failure of the event. <p>CA application logs must use a digital signature or a symmetric MAC (based on TDES – see <i>ISO 16609 – Banking – Requirements for message authentication using symmetric techniques</i> mechanism for protection from alteration. The signing/MACing key(s) used for this must be protected using a secure cryptographic device.</p> <p>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:</p> <ul style="list-style-type: none"> • Minimum length of six characters using a mix of alphabetic, numeric, and special characters. • System enforced expiration life not to exceed thirty days. • System enforced minimum life of at least one day. • Maximum invalid attempts not to exceed five before suspending the user ID. • System enforced pass phrase history preventing the reuse of any pass phrase used in the last twelve months. • Initial assigned pass phrases are pre-expired (user must replace at first logon). • Vendor default pass phrases are changed at installation and where applicable, for updates. • 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.

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<ul style="list-style-type: none"> • The embedding of pass phrases in shell scripts, command files, communication scripts, etc., is strictly prohibited. <p>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 associated PINs/pass phrases to enable their usage. The PINs/pass phrases must be at least six characters.</p> <p>The on-line Certificate Processing system components must be protected by a firewall(s) and intrusion detection systems from all unauthorized access including casual browsing and deliberate attacks.</p> <p>Firewalls must minimally be configured to:</p> <ul style="list-style-type: none"> • Deny all services not explicitly permitted. • Disable or remove all unnecessary services, protocols and ports. • Fail to a configuration that denies all services, and requires a firewall administrator to re-enable services after a failure. • Disable source routing on the firewall and external router. • Not accept traffic on its external interfaces that appears to be coming from internal network addresses. • Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action could be taken. • Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled. <p>Online systems must employ individually or in combination network and host based Intrusion Detection Systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and Web, as well as the intervening segments must be covered.</p>
<p>26. Logs are kept for any time that keys, key components, or related materials are removed</p>	<p>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</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
<p>from storage or loaded to a TRSM.</p>	<p>materials removed from safes and used in the loading process.</p> <p>At a minimum, the logs must include the date and time in/out, purpose of access, signature of custodian accessing the component, envelope number (if applicable).</p>
<p>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.</p>	<p>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).</p> <p>Backups (including cloning) must require a minimum of two authorized individuals to enable the process.</p> <p><i>Note – it is not a requirement to have backup copies of key components or keys.</i></p>
<p>28. Documented procedures exist and are demonstrably in use for all key administration operations.</p>	<p>Written procedures must exist and all affected parties are aware of those procedures. All activities related to key administration performed by a Key Injection Facility must be documented. This includes all aspects of key administration, as well as:</p> <ul style="list-style-type: none"> ○ Security awareness training. ○ Role definition - nominated individual with overall responsibility. ○ Background checks for personnel. ○ Management of personnel changes, including revocation of access control and other privileges when personnel move. <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <p>CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key distribution systems.</p> <p>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.</p> <p>Each CA operator must develop a certification practice statement (CPS) – (See RFC 3647 – <i>Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> for an example of content that can be reviewed by the payment brands. This may take the form of a declaration by the CA</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>Documented procedures exist and are 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.</p> <p>For CA and KDH certificate signing requests, including certificate or key validity status changes (e.g., revocation, suspension, replacement), verification must include validation that:</p> <ul style="list-style-type: none"> • The entity submitting the request is who it claims to be • The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity • The entity submitting the request has a valid business relationship with the issuing authority (e.g., the vendor) consistent with the certificate being requested. • The certificate signing request has been transferred from the certificate request's originating entity to the RA in a secure manner • RAs must 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.
<p>29. PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.</p>	<p>Key Injection Facilities must ensure that only legitimate, unaltered devices are loaded with cryptographic keys. HSMs and PEDs must only be placed into service 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</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>Dual control mechanisms must exist to prevent substitution of secure cryptographic devices, both in service and spare or backup devices. Procedural controls may exist to support the prevention and detection of substituted cryptographic devices, but cannot supplant the implementation of dual control mechanisms, which may be a combination of physical barriers and logical controls.</p> <p>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 the following:</p> <ol style="list-style-type: none"> 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. b. Cryptographic devices are shipped from the manufacturer’s facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs. c. The manufacturer’s facility loads into each cryptographic device a secret, device-unique “transport-protection token”. The TRSM 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. 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.

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<ul style="list-style-type: none"> ▪ 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. ▪ Controls must exist and be in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed. <p>Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:</p> <ul style="list-style-type: none"> ▪ Protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it, and ▪ Detect lost or stolen equipment. <p>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.</p> <p>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.</p> <p>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).</p> <p>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.</p> <p>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.</p>
<p>30. Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related</p>	<p>Key Injection Facilities must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any TRSMs (e.g., HSM) used in the key injection platform, as well as to any</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
<p>information within any cryptographic devices removed from service.</p>	<p>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.</p> <p>If a Key Injection Facility receives a used device to reload with keys, procedures should 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.)</p> <p>If a TRSM 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.</p> <ul style="list-style-type: none"> ▪ 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). ▪ Key and data storage must be zeroized when a device is decommissioned. <p>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.</p>
<p>31. Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following:</p> <ol style="list-style-type: none"> a. Dual access controls are required to enable the key encryption function. b. Physical protection of the equipment (e.g., locked access to it) under dual control. 	<p>Key Injection Facilities must ensure protection against unauthorized use for TRSMs (e.g., HSMs) used in the key injection platform that are capable of encrypting a key and producing cryptograms of that key.</p> <p>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.</p> <p>Unauthorized use of secure cryptographic devices (including key loading devices) shall be prevented or detected by:</p> <ul style="list-style-type: none"> • The device is at all times either locked or sealed in a tamper-evident cabinet or else is under the

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected;</p> <ul style="list-style-type: none"> • 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. <p>The following requirements apply to Key Injection Facilities participating in remote key establishment and distribution applications:</p> <ul style="list-style-type: none"> • CA and RA database and application servers, and cryptographic devices must reside in a physically secure and monitored environment. • 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. <p>Documented procedures exist for the granting and revocation of access privileges, which include reviewing manual or electronic logs of accesses. Specifically, Certificate Processing operations must:</p> <ul style="list-style-type: none"> ▪ Operate in a physically secure dedicated room not used for any other business activities but certificate operations (stand-alone). ▪ Provide for the documentation of all access granting, revocation, and review procedures and of specific access authorizations, whether logical or physical. ▪ 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. ▪ Use electronically (e.g., badge and/or biometric) managed dual occupancy. ▪ Allow access only to pre-designated staff with defined business needs and duties. Visitors must be authorized and escorted at all times. ▪ Use CCTV monitoring (motion activated systems

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>that are separate from the intrusion detection system may be used) of the CA operating platform which 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.</p> <ul style="list-style-type: none"> ▪ 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 forty-five days. Systems using digital recording mechanism must have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent forty-five day period. ▪ Provide for continuous (motion activated systems may be used) lighting for cameras. ▪ Have a 24/7 intrusion detection system of 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. ▪ 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 and time in and out and purpose of visit. The person escorting the visitor must also initial the log. ▪ Tie all access control and monitoring systems to an Uninterruptible Power Source (UPS). ▪ Document all alarm events. Under no circumstances shall an individual sign-off on an alarm event in which they were involved. ▪ Establish that the use of any emergency entry or exit mechanisms must cause an alarm event. ▪ Require that all alarms for physical intrusion necessitate an active response by personnel assigned security duties within thirty minutes.

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<ul style="list-style-type: none"> ▪ 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, then the process must occur at least quarterly. Documentation of the synchronization must be retained for at least a one-year period. <p>Root CAs and their equivalent operations must exist only in a high security environment.</p> <p>CAs and their associated RA servers that issue certificates to Key Distribution Hosts or subordinate CAs must additionally meet the following:</p> <ul style="list-style-type: none"> ▪ 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., in a caged environment. ▪ This physically secure environment must have a 24/7 intrusion detection system: <ul style="list-style-type: none"> • The intrusion detection system must have 24-hour monitoring (including UPS). • The intrusion detection system must include the use of motion sensors. • The system must be capable of and perform recording and archiving of alarm activity. • Alarm activity must include unauthorized entry attempts or any deliberate or inadvertent actions that disable the intrusion detection system. • All logged alarm activity information must be reviewed and resolved. • One or more cameras must provide continuous (motion activated systems that are separate from eh intrusion detection system may be used) monitoring of entry and exit tot eh physically secure environment. Lighting must exist for the camera images. Recording must be at a minimum of five frames equally every three seconds. • Use three layers of physical security in the CA facility with increasing levels of access control for each of the following levels: <p>Level One Barrier:</p> <p>This level consists of the entrance to the facility.</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>The building or secure facility entrance will only allow the entrance of 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.</p> <p>Level Two Barrier:</p> <p>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.</p> <p>Level Three Barrier:</p> <p>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 should correlate to separate organizational units.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • Name and signature of the individual, • Participants Organization, • Date and time in and out, • Reason for visit. <p>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.</p>

Key Injection Facility Security Requirement	International/Industry Standard(S)
	<p>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.</p> <p>Automated login and logout enforcement of personnel is required at level three. This level 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 thirty seconds. For time of single occupancy exceeding thirty seconds the system must automatically generate an audit event that must be followed up on by security personnel.</p>
<p>32. Documented procedures exist and are 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.</p>	<p>Written procedures must exist and all affected parties are aware of those procedures. Records must be maintained of the tests and inspections performed by Key Injection Facilities given to PIN-processing devices before they are placed into service, as well as devices being decommissioned.</p> <p>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.</p>

Appendix A - VISA Specific Requirements

General Requirements

The effective date for this document is 1 January 2008. At the time of publication, mandatory dates for the implementation of Triple Data Encryption Standard (TDES) key management techniques for PIN encryption vary by Visa region. Please check with the applicable Regional Risk Management group to determine the appropriate effective dates. These dates may also be found at www.visa.com/pin

Until those effective dates, entities that have not implemented TDES do not need to complete exception forms for the TDES portion of applicable questions. All other requirements within those questions must be met (e.g., using single instead of double-length keys and key components).

PIN Security Requirement #1

POS PIN acceptance devices and ATM and Cash Dispensing PIN acceptance devices that accept Visa PIN based transactions are required to be Visa approved and TDES capable in accordance with the following.

PIN Entry Device Testing Requirements¹:

- Effective 1 January 2004, all newly deployed attended POS PIN acceptance device models (including replacement devices) must have passed testing by a PCI-recognized laboratory and be approved by Visa for new deployments.
- Effective 1 October 2005, all newly deployed EPPs, including replacements or those in newly deployed ATMs, must have passed testing by a PCI-recognized laboratory and be approved by Visa for new deployments.
- Effective 1 October 2007, all newly deployed unattended POS PIN acceptance devices must contain an EPP that has passed testing by a PCI recognized laboratory and is approved by Visa for new deployments, and if used for offline PIN acceptance, a laboratory validated and Visa approved secure smart card reader.
- Effective 1 July 2010, all attended POS PIN acceptance device models must have passed testing by a PCI-recognized laboratory and have been approved by Visa.

PIN Entry Device TDES Capability Requirements¹:

- Effective 01 January 2003, all newly deployed ATMs (including replacement devices) must support TDES.
- Effective 01 January 2004, all newly deployed POS PIN acceptance devices (including replacement devices) must support TDES.
- Effective 1 July 2010, Cardholder PINs must be TDES encrypted from all Points-of-Transaction to the Issuer. However, each Visa Region's TDES dates will supersede the global TDES date whenever the Visa Region date precedes the global date.

Note: "Must support" means the device has all the necessary hardware and software required for TDES installed and only requires the loading of a TDES key.

¹ For additional information on the Visa PED Security Requirements, with region specific information, including a listing of approved devices, please refer to www.visa.com/pin.

Self-Audit Procedures

The purpose of this section is to ensure that participants in the electronic interchange system are in compliance with the requirements presented in this manual. To measure compliance, each participant in the transaction processing chain that manages cardholder PINs and encryption keys must be in compliance with the *PIN Security Requirements*.

Principal, sponsoring, and processor members, and any other entity sponsoring agents or third parties, are responsible for verifying that their member group, as a whole, is in full compliance. It is the responsibility of the designated auditing staff of each member group to explore the possible security implications of each unique implementation.

Participants will be notified by their respective Regional Risk Management group whether to submit the *PIN Security Requirements Self-Audit* and *Self-Audit Compliance Statement* **or** only the *Self-Audit Compliance Statement*.

In either case, a *Self-Audit Exception Form* must be filed—if applicable—for each exception. Other supporting documentation may be requested. The annual due date for these documents will be determined by Visa.

Security Self-Audit

The *PIN Security Requirements Self-Audit*, the *Self-Audit Compliance Statement*, applicable *Self-Audit Exception Form(s)*, and the *Self-Audit Processing Environment Form* must be completed and returned at least forty-five (45) days before beginning any card activation and/or processing.

Any time a participant makes substantive security changes; Visa may require re-validation of the participant's compliance with the *PIN Security Requirements*.

Audit Exception Form

For every answer that was not "yes," a *Self-Audit Exception Form* must be completed. This Exception Form identifies why the participant is not in compliance and which actions are being taken to bring the participant into compliance.

When compliance is not possible, Visa contacts the member to review and resolve any exceptions.

Auditor Verification

The *PIN Security Requirements Self-Audit* is to be completed and attested to annually by an internal or independent auditor, as shown on the *Self-Audit Compliance Statement*. The auditor must have sufficient skill and experience to determine compliance; Visa may request validation of the auditor's skill level.

Officer Attestation

In addition to verification by a qualified auditor, Visa requires an attestation of compliance by an Officer of the participant. Visa will notify each participant of the appropriate organizational level for this attestation.

Field Review

At its discretion, Visa may perform an onsite inspection to verify the participant's compliance to the Self-Audit. All auditor work papers from the Self-Audit may be requested and should be retained for a minimum of three years.

Fines

Fines may be imposed when there is failure to complete a *PIN Security Requirements Self-Audit* or a *Self-Audit Compliance Statement* or to respond to a non-compliance notification

An Acquirer:

- Is subject to fines as specified in the VIOR for the failure to submit the *PIN Security Requirements Self-Audit* or the *Self-Audit Compliance Statement*.
- Who fails to respond to a non-compliance Notification following an onsite inspection is subject to fines or to having its acquiring status suspended, as specified in the VIOR, until the response has been received and acknowledged by the applicable regional office.
- Who submits an action plan but does not fulfill its commitments will be required to post a performance bond or provide an escrow amount as specified in the VIOR.

In all cases a member is responsible and subject to fines or other sanctions for the actions or inactions of its agents.

Appendix B - Forms

This appendix contains the forms used to record compliance with the PIN Security Requirements identified in the Self-Audit. The forms included are:

- *PIN Security Requirements Self-Audit Compliance Statement*
- *PIN Security Requirements Self-Audit Processing Environment*
- *PIN Security Requirements Self-Audit Exception Form*

PIN Security Requirements Self-Audit Compliance Statement

This completed statement, along with all Exception Forms, should be returned to the Regional Risk Management group by the specified due date, in accordance with the requirements outlined in the *Visa International Operating Regulations*.

Organization Information

Name

Address

City

State/Province

Country

Postal Code

Visa Business ID (If Member): 10

Name of Sponsoring Institution(s) *(If applicable)*

Organization Contact

Telephone

Fax

Title

Email

Date

Submitted for Year of

Or Start-up Date

Compliance Statement

I, _____
(print or type name and title)

(check one)

- am an **internal auditor** for _____ and I have no operational responsibility for matters referenced in the PIN Security Requirements Self-Audit.
- am an **independent auditor** employed by _____ and hired by _____ to complete the PIN Security Requirements Self-Audit and the Compliance Statement.

I do hereby attest that the above-referenced organization is:

(check one)

- In full compliance** with the PIN Security Requirements Self-Audit.
- Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____ Date: _____

Officer Attestation:

I, _____
(print or type name and title)

I do hereby attest that the above-referenced organization is:

(check one)

- In full compliance** with the PIN Security Requirements Self-Audit.
- Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____ Date: _____

Processing Environment

6. Please use a separate sheet if necessary. Model “families” are adequate (for example, NCR 50xx, 56xx, Diebold 9xx, 106x, 107x, and so forth).

ATM	POS	Manufacturer	Model No.	Approx. Quantity
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			

7. If you process your own PIN-based transactions or PIN-based transactions for others (answered “Yes” to question 2), please answer the following:
- a. CPU/Operating System (release level) platforms used for PIN processing: _____
 - b. Security software: _____
 - c. Application software:
 To drive devices: _____
 For switching: _____
 - d. Host security module(s) used to secure encryption keys:
 Make/models: _____
 Quantity: _____
 - e. Do you have access to the source code for the application software?
 yes no
 - f. Estimated annual number of online PIN-based Interchange transactions for Visa Branded Products (Visa/Plus/Interlink/Visa Electron):
 ATM: _____
 POS: _____

8. Please list any Interchange Networks and/or processors with which you connect:
- _____

PIN Security Requirements Self-Audit Exception Form

You must complete an individual Exception Form for each statement on the PIN Security Self-Audit for which you did not respond "Yes." Your chief/general internal auditor or an independent outside auditor must attest to this form.

Organization Information

Name _____

Date _____

Submitted for Year of _____

Or Start-up Date _____

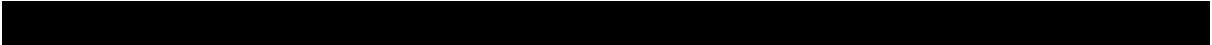
Statement # _____

Explanation of why you cannot answer "Yes" to the above referenced statement:

Describe action plan implemented to correct this situation:

Date expected to be in compliance: _____

Auditor's signature: _____



Appendix C - PIN Security Requirements Self-Audit

Objective 1

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

1.	<p>All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. TRSMs 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.</p> <p>All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
2.	<p>Cardholder PINs are processed in accordance with approved standards.</p> <p>a. All cardholder PINs processed online are 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.</p> <p>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.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
3.	<p>For online interchange transactions, PINs are 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.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
4.	<p>PINs are not 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.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

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 are generated using an approved random or pseudo-random process.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
7.	Documented procedures exist and are demonstrably in use for all key generation processing.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

Objective 3

Keys are conveyed or transmitted in a secure manner.

8.	Secret or private keys are transferred by: <ul style="list-style-type: none"> a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, or b. Transmitting the key in ciphertext form. 	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
Public keys must be conveyed in a manner that protects their integrity and authenticity.				
9.	Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities: <ul style="list-style-type: none"> a. Under the continuous supervision of a person with authorized access to this component, or b. Locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or c. In a physically secure TRSM. 	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
10.	All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

Objective 4

Key Loading To Hosts And PIN Entry Devices Is Handled In A Secure Manner.

12.	Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
13.	The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
14.	All hardware and passwords used for key loading are managed under dual control.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
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.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
16.	Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

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. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 18. Procedures 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. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 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. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
-

Objective 6

Keys are administered in a secure manner.

21.	Keys used for enciphering PIN-Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
22.	Procedures exist and are 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.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
23.	Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
24.	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
25.	Access to secret and private cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
26.	Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
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.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
28.	Documented procedures exist and are demonstrably in use for all key administration operations.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

Objective 7

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

29.	PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
30.	Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
31.	Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following: a. Dual access controls are required to enable the key encryption function. b. Physical protection of the equipment (e.g., locked access to it) under dual control.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
32.	Documented procedures exist and are 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.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

Glossary

Access Controls	Ensuring 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	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 identification card to the cardholder.
Certificate	The public key and identity of an entity together with some other information, rendered unforgeable by signing the certificate with the private key of the certifying authority that issued that certificate.
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. For example, entities that generate, maintain and distribute CRLs can include the Root or subordinate CAs.
Check value	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation which takes as

	input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible.
Ciphertext	Data in its enciphered form.
Cleartext	See Plaintext.
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 plaintext 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, authentication data such as passwords and PINs) appearing in plaintext 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.
Cryptographic key	A parameter used in conjunction with a cryptographic algorithm that determines: <ul style="list-style-type: none"> • The transformation of plaintext data into ciphertext data, • The transformation of ciphertext data into plaintext data, • A digital signature computed from data, • The verification of a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret.
Cryptographic key component	A parameter used in conjunction with other key components in an approved security function to form a plaintext cryptographic key or perform a cryptographic function.
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 ciphertext (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. Derivation keys are normally used in a transaction-receiving (e.g., acquirer) TRSM in a one-to-many relationship to derive or decrypt the Transaction (the derived keys) Keys used by a large number of originating (e.g., terminals) TRSMs.
DES	Data Encryption Standard (see Data Encryption Algorithm). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm.
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), who are operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see "split knowledge."
DUKPT	Derived Unique Key Per Transaction: a key management method that uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction originating TRSM. The unique Transaction Keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.
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.
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, 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.
EPROM	Erasable Programmable Read-Only Memory.
Exclusive-OR	Binary addition without carry, also known as modulo 2 addition, symbolized as “XOR” and defined as: <ul style="list-style-type: none"> • $0 + 0 = 0$ • $0 + 1 = 1$ • $1 + 0 = 1$ • $1 + 1 = 0$
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 which 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, which produce the same hash result. It may be used to reduce a potentially long message into a “hash value” or “message digest” which is sufficiently compact to be input into a digital signature algorithm. A “good” hash is such that the results of applying the function to a (large) set of values in a given domain will be evenly (and randomly) distributed over a smaller range.
Hexadecimal character	A single character in the range 0–9, A-F (upper case), representing a four-bit string.
Initialization Vector	A binary vector used as the input to initialize the algorithm for the encryption of a plaintext 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 members.
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.
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 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., plaintext 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 plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.
Key pair	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 only known 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 processing of data, such as a terminal, acquirer, or switch.

Non-reversible transformation	See Irreversible Transformation.
OCSP	See Online Certificate Status Protocol.
Online Certificate Status Protocol	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.
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.
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 that originates 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 that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or 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.

PIN pad	See PIN Entry Device.
Plaintext	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as cleartext.
Plaintext 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	<p>A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public.</p> <p>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.</p>
PROM	Programmable Read-Only Memory.
Pseudo-random	A value that is statistically random and essentially random and unpredictable although generated by an algorithm.
Public key	<p>A cryptographic key, used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public</p> <p>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.</p>
Public key (asymmetric) cryptography	<p>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.</p> <p>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.</p> <p>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</p>

	<p>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.</p>
Random	<p>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.</p>
ROM	<p>Read-Only Memory.</p>
Root Certification Authority (RCA)	<p>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.</p>
Secret key	<p>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.</p>
Secure Cryptographic Device	<p>See TRSM</p>
Sensitive data	<p>Data which must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs and cryptographic keys, and includes design characteristics, status information, and so forth.</p>
Session key	<p>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.</p>
Shared Secret	<p>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.</p>
Single-length key	<p>A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.</p>
Software	<p>The programs and associated data that can be dynamically written and modified.</p>

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, then 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.
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 codebook.
Terminal	A device/system that initiates a transaction.
Transaction	A series of messages to perform a predefined function.
Triple Data Encryption Algorithm (TDEA)	The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.
Triple Data Encryption Standard (TDES)	See Triple Data Encryption Algorithm.
Triple-length key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.

TRSM	Tamper-Resistant Security Module: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. Also known as a secure cryptographic device.
Trustworthy system	Computer hardware and software which: <ul style="list-style-type: none"> • are reasonably secure from intrusion and misuse; • provide a reasonable level of availability, reliability, and correct operation; and • are reasonably suited to performing their intended functions.
Unattended Acceptance Terminal (UAT)	See Unattended Payment Terminal
Unattended Payment Terminal (UPT)	A cardholder-operated device that reads, captures, and transmits card information in an Unattended Environment, including, but not limited to, the following: <ul style="list-style-type: none"> • ATM • Automated Fuel Dispenser • Ticketing Machine • Vending Machine
Unprotected memory	Components, devices and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a secure cryptographic device.
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.
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.