



# Payment Card Industry (PCI) PIN Security Requirements

---

**Version 2.0**

December 2014

## Document Changes

Date	Version	Description
October 2011	1.0	Initial release of <i>PCI PIN Security Requirements</i>
December 2014	2.0	Initial release of requirements with test procedures

# Table of Contents

<b>Document Changes .....</b>	<b>i</b>
<b>Overview .....</b>	<b>1</b>
<i>Usage Conventions.....</i>	<i>2</i>
<i>Limitations.....</i>	<i>2</i>
<i>Effective Date.....</i>	<i>2</i>
<b>PIN Security Requirements – Technical Reference.....</b>	<b>3</b>
Introduction.....	3
ANSI, EMV, ISO, FIPS, NIST, and PCI Standards .....	3
PIN Security Requirements .....	5
<i>Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure. ....</i>	<i>5</i>
<i>Control 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.....</i>	<i>9</i>
<i>Control Objective 3: Keys are conveyed or transmitted in a secure manner. ....</i>	<i>12</i>
<i>Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner. ....</i>	<i>15</i>
<i>Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage. ....</i>	<i>19</i>
<i>Control Objective 6: Keys are administered in a secure manner. ....</i>	<i>22</i>
<i>Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner. ....</i>	<i>28</i>
<b>Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques.....</b>	<b>33</b>
A1 – Remote Key Distribution Using Asymmetric Techniques Operations: PIN Security Requirements.....	34
<i>Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure. ....</i>	<i>34</i>
<i>Control 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.....</i>	<i>34</i>
<i>Control Objective 3: Keys are conveyed or transmitted in a secure manner. ....</i>	<i>34</i>
<i>Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner. ....</i>	<i>35</i>
<i>Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage. ....</i>	<i>35</i>
<i>Control Objective 6: Keys are administered in a secure manner. ....</i>	<i>36</i>

A2 – Certification and Registration Authority Operations: PIN Security Requirements .....	37
Control Objective 3: Keys are conveyed or transmitted in a secure manner. ....	37
Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner. ....	37
Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage. ....	37
Control Objective 6: Keys are administered in a secure manner. ....	38
Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner. ....	45
<b>Normative Annex B – Key-Injection Facilities .....</b>	<b>49</b>
Introduction .....	49
PIN Security Requirements .....	50
Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure. ....	50
Control 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. ....	51
Control Objective 3: Keys are conveyed or transmitted in a secure manner. ....	54
Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner. ....	58
Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage. ....	65
Control Objective 6: Keys are administered in a secure manner. ....	68
Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner. ....	77
<b>Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms .....</b>	<b>82</b>
<b>Glossary .....</b>	<b>84</b>

## Overview

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

The 33 requirements presented in this document are organized into seven logically related groups, referred to as “Control Objectives.” These requirements are intended for use by all acquiring institutions and agents responsible for PIN transaction processing on the payment card industry participants’ denominated accounts and should be used in conjunction with applicable industry standards. These requirements do not apply to issuers and their agents.

This document:

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

**Note:**

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

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

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

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

Acquiring entities are required to maintain a summary listing of the cryptographic keys used in connection with the acquiring and processing of PIN data. This includes keys used by POI devices, HSMs, and those shared with other internal network nodes or with other organizations that are used for the conveyance of PIN data and associated messages. This listing must include the name/usage (e.g., TMK – POI key-encipherment key, PEK – POI PIN-encipherment key, MFK – HSM Master File Key, KEK-A – Zone key-encipherment key shared with organization A, ZWK-A – PIN-encipherment key shared with organization A, etc.). This also must include keys such as any asymmetric key pairs used for remote key-establishment and distribution as delineated in Annex A, and other keys used in the message flow such as MAC and keys associated with account data encryption. It is not required to include vendor keys such as those used for firmware authentication, but shall include acquirer-controlled private or secret keys used to sign payment applications that handle PIN data, display prompt control data, etc. The algorithm (e.g., AES, TDEA, RSA) used and key size (e.g., 128, 2048) for each key type must also be identified.

This information will be used to facilitate the construct or enhancement of a network schematic detailing transaction flows with the associated key usage to aid the conduct of a PIN security review following the test procedures delineated below.

Whereas PCI SSC validates the new device models (or upgrades) offered by vendors to the marketplace, the actual terms and conditions for the deployment (and removal) of payment security devices in the field—in the card acceptance networks—are defined by the brands that manage such networks. These terms and conditions may include:

- Compliance with a specific SCD standard
- The types of devices
- The time windows for the deployment (and removal) of such devices
- Sunset (retirement) dates for specific models or SCD standards

The lists of device models compliant with a version of the PCI PTS standard can be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) under “Approved Companies & Providers.”

- Device models whose certificates are valid are listed in the list “Approved PIN Transaction Security (PTS) Devices” under the “PIN Acceptance Device” tab and must belong to one of the PCI PTS Approval Classes: PED, EPP, and UPT.
- Device models whose PCI PTS certificates expired are listed in the list “PTS Devices with Expired Approvals.”

For specific considerations, contact the payment brand(s) of interest.

### ***Usage Conventions***

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

### ***Limitations***

If any of the requirements contained in this manual conflict with country, state, or local laws, the country, state, or local law will apply.

The individual payment brands are responsible for defining and managing compliance programs associated with these requirements. Contact the payment brand(s) of interest for any additional criteria.

### ***Effective Date***

The effective date for this document is December 2014. The individual payment brands shall set the effective date for compliance. For further details, contact the payment brand(s) of interest.

# PIN Security Requirements – Technical Reference

## Introduction

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

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

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

**Note:**

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

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

Source	Publication
ANSI	<i>ANSI X3.92: Data Encryption Algorithm</i>
	<i>ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques</i>
	<i>ANSI X9.24 (Part 2): Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys</i>
	<i>ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography</i>
	<i>ANSI X9.44: Key Establishment Using Integer Factorization Cryptography</i>
	<i>ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA</i>
	<i>ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography</i>
	<i>ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms</i>
EMV	<b>EMV: Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management</b>

Source	Publication
FIPS	<i>FIPS PUB 140–2: Security Requirements for Cryptographic Modules</i>
	<i>FIPS PUB 186-4: Digital Signature Standard (DSS)</i>
ISO	<i>ISO 9564: Financial services - Personal Identification Number Management and Security</i>
	<i>ISO 11568: Banking – Key Management (Retail)</i>
	<i>ISO 11770–2: Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques</i>
	<i>ISO 11770–3: Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)</i>
	<i>ISO 13491: Banking – Secure Cryptographic Devices (Retail)</i>
	<i>ISO TR 14742: Financial services - Recommendations on cryptographic algorithms and their use</i>
	<i>ISO 16609: Banking – Requirements for message authentication using symmetric techniques</i>
	<i>ISO 18031: Information technology -- Security techniques -- Random bit generation</i>
	<i>ISO/IEC 18033-3: Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers</i>
	<i>ISO TR 19038: Guidelines on Triple DEA Modes of Operation</i>
NIST	<i>NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications</i>
	<i>NIST Special Publication 800-57: Recommendation for Key Management</i>
	<i>NIST Special Publication 800-131: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i>
PCI SSC	<i>Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements</i>
	<i>Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements</i>
	<i>Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements</i>
	<i>Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Derived Test Requirements</i>

## PIN Security Requirements

**Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.**

**Requirement 1:** All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD.

A secure cryptographic device (SCD) must meet the requirements of a “Physically Secure Device” as defined in ISO 9564. For POI PIN-acceptance devices this is evidenced by their being validated and PCI approved against one of the following:

- One of the versions of the PCI PTS standard, as members of Approval Classes EPP, PED, or UPT (collectively known as POI Devices) and Approval Class HSMs, or
- FIPS 140-2 level 3 or higher

**1-1** The entity acquiring PIN-based transactions is responsible for maintaining an inventory of POI Devices. For each individual device, the minimal information elements that must be reported in the inventory are indicated below (in line with PCI PIN Requirement 30, PCI PIN Requirement 33, and PCI DSS Requirement 9.9.1):

- The device unique identifier
- The company name (vendor) of the device model
- The device model name
- The PCI PTS standard(s) and version with which the model complies
- The PCI PTS Approval Number
- The PCI PTS POI Product Type associated to the device
- The location of device
- The device status (in operation, in warehouse, etc.)
- The date of deployment or installation of the device
- The brand payment schemes accepted by the device
- The acquiring financial institution
- The dates of placement into service, initialization, deployment, use, and decommissioning (where applicable)

The POI Device inventory must include the following summary information

- List of models used
- Total number of devices, broken down by PCI PTS POI Product Type
- Total number of devices, broken down by model
- Total number of devices, broken down by version of the compliance standard met

**Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.**

**1-2** Not used in core requirements and testing procedures.

**1-3** Ensure that all hardware security modules (HSMs) are either:

- FIPS140-2 Level 3 or higher certified, or
- PCI approved.

**1-4** The approval listing must match the deployed devices in the following characteristics:

- Vendor name
- Model name and number
- Hardware version number
- Firmware version number
- For PCI-approved HSMs, any applications resident within the device, including application version number, that were included in the PTS assessment.

**Requirement 2a:** *Cardholder PINs shall be processed in accordance with approved standards.*

- All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.*
- 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 9654.*

**2-1** No procedure shall require or permit the cardholder to disclose the PIN in an oral or written manner.

**2-2** Online PIN translation must only occur using one of the allowed key-management methods: DUKPT, fixed key, master key/session key.

**2-3** Online PINs must be encrypted using an algorithm and key size that is specified in ISO 9564. Currently, the only approved algorithms for online PIN are:

- The TDEA using the electronic code book (TECB) mode of operation, and
- AES as described in ISO 18033-3<sup>1</sup>

For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in ISO 18033-3.

<sup>1</sup> AES is not allowed for use in encrypting PINs until subsequent to publication of ISO 9564 with the prescribed AES PIN format.

**Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.**

**2-4** 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.

See Book 2, Section 7, of the *EMV IC Card Specifications for Payment Systems*, and **ISO 9564**.

PIN submission method	PED and IC reader integrated as a device meeting the requirements of ISO 9564	PED and IC reader not integrated as a device meeting the requirements of ISO 9564
1. Enciphered PIN block submitted to the IC	The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.	The PIN block shall be enciphered between the PED and the IC reader in accordance with <b>ISO 9564</b> 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.
2. Plaintext PIN block submitted to the IC	No encipherment of the PIN block is required.	The PIN block shall be enciphered from the PED to the IC reader in accordance with <b>ISO 9564</b> .

**Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.**

**Requirement 3:** For online interchange transactions, PINs must be only encrypted using ISO 9564–1 PIN-block formats 0, 1, 3 or 4. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.

**3-1** For secure transmission of the PIN from the point of PIN entry to the card issuer, the encrypted PIN-block format must comply with ISO 9564 format 0, ISO 9564 format 1, ISO 9564 format 3 or ISO 9564 format 4.

**3-2** 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.

**3-3** Standard PIN-block formats (i.e., ISO formats 0, 1, 2, 3, and 4) shall not be translated into non-standard PIN-block formats.

PINs enciphered using ISO format 0, ISO format 3, or ISO format 4 must not be translated into any other PIN-block format other than ISO format 0, 3, or 4 except when translated to ISO format 2 as specified in the table below. PINs enciphered using ISO format 1 may be translated into ISO format 0, 3, or 4, but must not be translated back into ISO format 1. ISO format 1 may be translated into ISO format 2 as specified in the table below.

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, 3, or 4 (including translations from ISO format 0 to ISO format 0, from ISO format 3 to ISO format 3, or from ISO format 4 to ISO format 4) must not allow a change of PAN. The following illustrates translations from formats 0, 1, 3 and 4:

**Note:** This translation restriction is not applicable to surrogate PANs used in tokenization implementations.

Translation			
From ↓ \ To →	ISO Format 0, 3, 4	ISO Format 1	ISO Format 2
ISO Format 0, 3, 4	Permitted anywhere without change of PAN Change of PAN only permitted in sensitive state for card issuance	Not permitted	Permitted for submission to an IC card
ISO Format 1	Permitted	Permitted	Permitted for submission to an IC card
ISO Format 2	Not permitted	Not permitted	Permitted for submission to an IC card

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

**4-1** Transactions may be stored and forwarded under certain conditions as noted in ISO 9564. PIN blocks, even encrypted, must not be retained in transaction journals or logs. PIN blocks are required in messages sent for authorization, but must not be retained for any subsequent verification of the transaction. PIN blocks may be temporarily stored as a system-recovery mechanism in order to recover authorization processing. For the storage of other data elements, see the *PCI Data Security Standards*.

**Control 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.**

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

**5-1** 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. Cryptographic keys or key components must be generated by one of the following:

- An approved key-generation function of a PCI-approved HSM or POI;
- An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or
- An approved random number generator that has been certified by an independent laboratory to comply with *NIST SP800-22*.

*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.*

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

**6-1** Implement security controls, including dual control and tamper protection, to prevent the unauthorized disclosure of keys/key components.

**6-1.1** Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.

**6-1.2** There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.

**Note:** Full-length key components or key shares derived using a recognized key-splitting algorithm are not considered key parts and do not provide any information regarding the actual cryptographic key.

**6-1.3** Devices used for generation of clear-text key components that are output in the clear must be powered off when not in use.

Logically partitioned devices used concurrently for other processes—e.g., providing services simultaneously to host systems, such as for transaction processing—must have key-generation capabilities disabled when not in use and other activities are continuing.

**6-1.4** Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (for example, unnecessary cables).

**6-1.5** Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area. It must not be feasible to observe the key-component/key-generation process whereby clear-text keying material is observable either directly or via camera monitoring.

**Control 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.**

**6-2** Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.

*For example, it is not permitted for the cryptographic key to be passed through the memory of a computer unless it has been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed and used solely for key loading are permitted for use if all other requirements can be met, including those of Requirement 5 and the controls defined in Requirement 13 of Annex B.*

*Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.*

*Single-purpose computers with an installed SCD where clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) meet this requirement. Where the components pass through unprotected memory of the PC, it must meet Requirement 13 of Annex B.*

**6-3** Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that:

- Only approved key custodians can observe their own key component.
- Tampering can be visually detected.

Printers used for this purpose must not be used for other purposes.

**6-4** Any residue that may contain clear-text keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key, to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual.

*Examples of where such key residue may exist include (but are not limited to):*

- *Printing material, including ribbons and paper waste*
- *Memory storage of a key-loading device, after loading the key to a different device or system*
- *Other types of displaying or recording*

**6-5** Asymmetric-key pairs must either be:

- Generated by the device that will use the key pair; or
- If generated externally, the private key of the key pair and all related critical security parameters (for example, secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.
- Devices used for key generation or key injection are securely stored when not in use.

**Control 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.***

**6-6** Policy and procedures must exist to ensure that key components are prohibited from being transmitted across insecure channels. These include but are not limited to:

- Dictating verbally keys or components
- Recording key or component values on voicemail
- Faxing, e-mailing, or otherwise conveying clear-text secret or private keys or components
- Conveying clear-text private or secret keys or their components without containing them within tamper-evident, authenticable packaging
- Writing key or component values into startup instructions
- Taping key or component values to or inside devices
- Writing key or component values in procedure manuals

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

**7-1** Written key-creation procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of those procedures. Procedures for creating all keys must be documented.

**7-2** Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKeys.

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**Requirement 8:** Secret or private keys shall be transferred by:

- a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or
- b. Transmitting the key in ciphertext form.

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

**8-1** Keys must be transferred either encrypted or—if clear text—as two or more components using different communication channels or within an SCD.

Note this does not apply to keys installed in POI devices meeting Requirement 1 when shipped from the key-injection facility.

Clear-text key components may be conveyed in SCDs or using tamper-evident, authenticable packaging.

- Where key components are transmitted in clear-text using pre-numbered tamper-evident, authenticable mailers:
  - Components/shares must be conveyed using at least two separate communication channels, such as different courier services. Components/shares sufficient to form the key must not be conveyed using the same communication channel.
  - Ensure that details of the serial number of the package are conveyed separately from the package itself.
  - Ensure that documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material.
- Where an SCD is used for components, the mechanisms or data (e.g., PIN) to obtain the key component from the SCD must be conveyed using a separate communication from the SCD channel, or it must be conveyed in the same manner as a paper component. SCDs must be inspected for signs of tampering.
- Where an SCD (HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering.

Components of encryption keys must be conveyed 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.

**8-2** A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key.

*E.g., in an  $m$ -of- $n$  scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e.,  $m = 3$ ) can be used to derive the key, no single individual can have access to more than two components/shares.*

**8-3** E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) has already been encrypted in accordance with these requirements—i.e., in an SCD. This is due to the existence of these key values in unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear text of any encrypted text or files conveyed through those systems.

Other similar mechanisms, such as SMS, fax, or telephone shall not be used to convey clear-text key values.

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**8-4** Public keys must be conveyed in a manner that protects their integrity and authenticity.

Examples of acceptable methods include:

- Use of public-key certificates as defined in Annex A that are created by a trusted CA that meets the requirements of Annex A.
- A hash of the public key sent by a separate channel (for example, mail)
- Using a MAC (message authentication code) created using the algorithm defined in ISO 16609
- Be within an SCD

**Note:** *Self-signed certificates must not be used as the sole method of authentication.*

**Requirement 9:** *During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.*

*Sending and receiving entities are equally responsible for the physical protection of the materials involved.*

**9-1** Any single clear-text secret or private key component/share must at all times be either:

- Under the continuous supervision of a person with authorized access to this component,
- Locked in a security container (including pre-numbered tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or
- Contained within a physically secure SCD.

**Note:** 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

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**9-2** Packaging or mailers (i.e., pre-numbered tamper-evident packaging) containing clear-text key components are examined for evidence of tampering before being opened. Any sign of package tampering must result in the destruction and replacement of:

- The set of components
- Any keys encrypted under this (combined) key

**9-3** No one but the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.

**9-4** Mechanisms must exist to ensure that only authorized custodians:

- Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal.
- Check tamper-evident packaging upon receipt for signs of tamper prior to opening tamper-evident, authenticable packaging containing key components.
- Check the serial number of the tamper-evident packing upon receipt of a component package.

**9-5** Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers.

**Note:** *Numbered courier bags are not sufficient for this purpose.*

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

**10-1** All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be (at least) as strong as the key being sent, as delineated in Annex C, except as noted below for RSA keys used for key transport and for TDEA keys.

- DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
- A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength.
- TDEA keys shall not be used to protect AES keys.
- TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.
- RSA keys used to transmit or convey other keys must have bit strength of at least 80 bits.
- RSA keys encrypting keys greater in strength than 80 bits shall have bit strength at least 112 bits.

**Note:** *Entities that are in the process of migrating from older devices to PCI devices approved against version 3 or higher of the PCI POI Security Requirements—and thus have a mixed portfolio of devices—may use RSA key sizes less than 2048 and use SHA-1 to help facilitate the migration. However, in all cases, version 3 or higher devices must implement RSA using key sizes of 2048 or higher and SHA-2 within 24 months of the publication of these requirements when used for key distribution using asymmetric techniques in accordance with Annex A.*

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

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

**11-1** Written procedures must exist and be known to all affected parties.

**11-2** Methods used for the conveyance or receipt of keys must be documented.

### **Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.**

**Requirement 12:** Secret and private keys must be input into hardware (host) security modules (HSMs) and PIN entry devices (PEDs) in a secure manner.

- a. Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge.
- b. Key-establishment techniques using public-key cryptography must be implemented securely.

**12-1** The loading of secret or private keys, when from the individual key components or shares, must be performed using the principles of dual control and split knowledge.

**Note:** Manual key loading may involve the use of media such as paper, smart cards, or other physical tokens.

**12-2** Procedures must be established that will prohibit any one person from having access to components sufficient to form an encryption key when components are removed from and returned to storage for key loading.

**12-3** The loading of clear-text cryptographic keys using a key-loading device, requires dual control to authorize any key-loading session. It shall not be possible for a single person to use the key-loading device to load clear keys alone.

Dual control must be implemented using one or more of, but not limited to, the following techniques:

- Two or more passwords of five characters or more (vendor default values must be changed)
- Multiple cryptographic tokens (such as smartcards), or physical keys
- Physical access controls

**Note that for devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.**

**12-4** Key components for symmetric keys must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components. (For example, via XOR'ing of full-length components.)

The resulting key must only exist within the SCD.

**Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two 8-hexadecimal character halves to form a 16-hexadecimal secret key.**

**Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.**

**12-5** Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.

**12-6** Any other SCD loaded with the same key components must combine all entered key components using the identical process.

**12-7** The initial terminal master key (TMK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key may use techniques described in this documents such as:

- Asymmetric techniques
- Manual techniques
- The existing TMK to encrypt the replacement TMK for download

Keys shall not be reloaded by any methodology in the event of a compromised device, and must be withdrawn from use.

**12-8** If key-establishment protocols using public-key cryptography are used to distribute secret keys, these must meet the requirements detailed in Annex A of this document. For example:

A public-key technique for the distribution of symmetric secret keys must:

- Use public and private key lengths that are in accordance with Annex C 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 POI device or host-to-host if applicable, including assurance to the host that the POI device actually has (or actually can) compute the session key, and that no entity other than the POI device specifically identified can possibly compute the session key.

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

**13-1** Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that:

- Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of clear-text key components.
- There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys.
- The SCD must be inspected prior to use to ensure that it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying material.
- SCDs must be inspected to detect evidence of monitoring and to ensure dual control procedures are not circumvented during key loading.
- An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are uniquely identified by the device.

**13-2** Only SCDs shall be used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility, as delineated in this requirement. For example, ATM controller (computer) keyboards shall never be used for the loading of clear-text secret or private keys or their components.

**Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.**

**13-3** The loading of plaintext secret or private key components from an electronic medium—e.g., smart card, thumb drive, fob or other devices used for data transport—to a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following:

- The electronic media are placed into secure storage and managed under dual control (only if there is a possibility they will be required for future re-loading of the component into the cryptographic device); or
- All traces of the component are erased or otherwise destroyed from the electronic media in accordance with Requirement 24.

**13-4** For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:

**13-4.1** The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.

**13-4.2** The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.

**13-4.3** The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.

**13-4.4** The key-loading device must not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred.

**13-5** Any media (electronic or otherwise) containing secret or private key components used for loading cryptographic keys must be maintained in a secure storage location and accessible only to authorized custodian(s). When removed from the secure storage location, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process.

The media upon which a component resides must be physically safeguarded at all times when removed from secure storage.

Key components that can be read (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are never used in a manner that would result in the component being displayed in clear text to a non-custodian for that component.

**13-6** If the component is in human-readable form (e.g., printed within a PIN-mailer type document), it must be visible only to the designated component custodian and only for the duration of time required for this person to privately enter the key component into an SCD.

**13-7** Written or printed key-component documents must not be opened until immediately prior to use.

**13-8** A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key.

*E.g., in an  $m$ -of- $n$  scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e.,  $m = 3$ ) can be used to derive the key, no single individual can have access to more than two components/shares.*

#### **Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.**

**Requirement 14:** *All hardware and access/authentication mechanisms (e.g., passwords) used for key loading must be managed under the principle of dual control.*

**14-1** Any hardware and passwords used in the key-loading function must be controlled and maintained in a secure environment under dual control. Resources (e.g., passwords and associated hardware) must be managed such that no single individual has the capability to enable key loading of clear-text keys or their components. This is not to imply that individual access authentication mechanisms must be managed under dual control.

**Note:** *Where key-loading is performed for POIs, the secure environment is defined in Annex B.*

**14-2** All cable attachments where clear-text keying material traverses must be examined before each key-loading operation to ensure they have not been tampered with or compromised.

**14-3** Key-loading equipment usage must be monitored and a log of all key-loading activities maintained for audit purposes containing at a minimum date, time, personnel involved, and number of devices keys are loaded to.

**14-4** Any physical tokens (e.g., brass keys or chip cards) used to enable key-loading must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control. These tokens must be secured in a manner similar to key components, including the use of access-control logs for when removed or placed into secure storage.

**14-5** Default passwords or PINs used to enforce dual-control must be changed, and documented procedures must exist to require that these password/PINs be changed when assigned personnel change.

**Requirement 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.*

**15-1** A cryptographic-based validation mechanism must be in place to ensure the authenticity and integrity of keys and/or their components (for example, testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See ISO 11568. Where check values are used, recorded or displayed key-component check values and key check values shall not exceed six hexadecimal characters in length.

**15-2** The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted in accordance with Annex C, or if in plaintext form, must:

- Be within a certificate as defined in Annex A; or
- Be within a PKCS#10; or
- Be within an SCD; or
- Have a MAC (message authentication code) created using the algorithm defined in ISO 16609.

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

**16-1** Documented key-loading procedures must exist for all devices (e.g., HSMs and POIs), and all parties involved in cryptographic key-loading must be aware of those procedures.

**Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.**

**16-2** All key-loading events must be documented. Audit trails must be in place for all key-loading events.

**Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 17:** *Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations or logically separate systems within the same organization.*

**17-1** Where two organizations or logically separate systems 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 or logically separate systems and must not be given to any other organization or logically separate systems.

**Requirement 18:** *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.*

**18-1** Synchronization errors must be monitored to help reduce the risk of an adversary's substituting a key known only to them. Procedures must exist and be followed for investigating repeated synchronization errors for online processes such as online key exchanges or transmission or processing of PIN-based transactions.

**Note:** *Multiple synchronization errors in PIN translation may be caused by the unauthorized replacement or substitution of one stored key for another, or the replacement or substitution of any portion of a TDEA key, whether encrypted or unencrypted.*

**18-2** To prevent or detect usage of a compromised key, key-component packaging, or containers 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.

**18-3** Effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself,
- A digital signature computed over that same data,
- An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 19:** *Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*

**19-1** Encryption keys must be used only for the purpose they were intended (i.e., key-encryption keys must not to be used as PIN-encryption keys, PIN-encryption keys must not be used for account data, etc.). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.

**19-2** Private keys must only be used as follows:

- For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating POI devices).
- Private keys shall never be used to encrypt other keys.

**19-3** Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).

**19-4** Keys must never be shared or substituted between production and test/development systems:

- Key used for production must never be present or used in a test system, and
- Keys used for testing must never be present or used in a production system.

**Note:** *For logically partitioned HSMs and computing platforms, if one or more logical partitions of a physical device are used for production and one or more other logical partitions are used for testing, including QA or similar, the entire configuration must be managed and controlled as production.*

**19-5** If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.

At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.

**Note this does not apply to HSMs that are never intended to be used for production.**

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 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 (e.g., PED) that processes PINs must be unique (except by chance) to that device.*

**20-1** POI devices must each implement unique secret and private keys for any function directly or indirectly related to PIN protection. These keys must be known only in that device and in hardware security modules (HSMS) 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.

*This means not only the PIN-encryption key(s), but also keys that are used to protect other keys, firmware-authentication keys, payment-application authentication and display-prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.*

*POI private keys must not exist anywhere but the specific POI they belong to, except where generated external to the POI and prior to the injection into the POI.*

**20-2** If a transaction-originating terminal (for example POI device) interfaces with more than one acquiring organization, the transaction-originating terminal SCD must have a completely different and unique key or set of keys for each acquiring organization. These different keys, or sets of keys, must be totally independent and not variants of one another.

**20-3** Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device.

This requirement refers to the use of a single “base” key to derive master keys for many different POIs, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys once loaded, for example, as done with DUKPT.

**20-4** Entities processing or injecting DUKPT or other key-derivation methodologies must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques:

- Different BDKeys for each financial institution
- Different BDKeys by injection vendor (e.g., ESO), terminal manufacturer, or terminal model
- Different BDKeys by geographic region, market segment, platform, or sales unit

Injection vendors must use at least one unique Base Derivation Key (BDK) per acquiring organization, and must be able to support segmentation of multiple BDKeys of acquiring organizations.

## **Control Objective 6: Keys are administered in a secure manner.**

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

**21-1** Secret or private keys must only exist in one or more of the following forms

- At least two separate key shares or full-length components
- Encrypted with a key of equal or greater strength as delineated in Annex C
- Contained within a secure cryptographic device

**21-2** Wherever key components are used, they have the following properties:

**21-2.1** Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.

**21-2.2** Construction of the cryptographic key requires the use of at least two key components/shares.

**21-2.3** Each key component/share has one or more specified authorized custodians.

**21-2.4** Procedures exist to ensure any custodian never has access to sufficient key components or shares of a secret or private key to reconstruct a cryptographic key.

*For example, in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian must not then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.*

*In an m-of-n scheme where n=5 and where three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (for example, component A and component B), as a second custodian (with, in this example, component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*

**21-3** Key components must be stored as follows:

**Control Objective 6: Keys are administered in a secure manner.**

**21-3.1** Key components that exist in clear text outside of an SCD must be sealed in opaque, pre-numbered tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging.

**Note:** *Tamper-evident, authenticable packaging—opacity may be envelopes within tamper-evident packaging—used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to “read” the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.*

**21-3.2** Key components for each specific custodian must be stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).

**Note:** *Furniture-based locks or containers with a limited set of unique keys—for example, desk drawers—are not sufficient to meet this requirement. 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.*

**21-3.3** If a key component is stored on a token, and an access code (e.g., a PIN or similar access-control mechanism) is used to access the token, only that token’s owner (or designated backup(s)) must have possession of both the token and its access code.

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

**22-1** Procedures for known or suspected compromised keys must include the following:

**22-1.1** Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.

**22-1.2** If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.

**22-1.3** A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s).

**Note:** *The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.*

*Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.*

## **Control Objective 6: Keys are administered in a secure manner.**

**22-1.4** A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including:

- Identification of key personnel
- A damage assessment including, where necessary, the engagement of outside consultants
- Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.

**22-1.5** Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to:

- Missing secure cryptographic devices
- Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries
- Tamper-evident seals or authenticable 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
- Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation

**22-2** If attempts to load a secret key or key component into an KLD or POI 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 from or otherwise destroyed in the original KLD or POI.

**Requirement 23:** *Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.*

*Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.*

*Keys generated using a non-reversible process, such as key-derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*

**23-1** Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes, but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from PIN keys.

**Note:** *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*

**23-2** An MFK used by host processing systems for encipherment of keys for local storage—and variants of the MFK—must not be used external to the (logical) configuration that houses the MFK itself. For example, MFKs and their variants used by host processing systems for encipherment of keys for local storage shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration.

*A logical configuration is defined as one where all the components form a system used to undertake a particular task and are managed and controlled under a single operational and security policy.*

**Control Objective 6: Keys are administered in a secure manner.**

**23-3** Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys (e.g., PEKs) from key-encrypting keys.

Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or working keys with different purposes from another working key.

**Note:** Using transforms of keys across different levels of a key hierarchy—for example, generating a PEK from a key-encrypting key—increases the risk of exposure of each of those keys.

*It is acceptable to use one “working” key to generate multiple reversible transforms to be used for different working keys, such as a PIN key, MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.*

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

**24-1** Instances of secret or private keys, and their key components, that are no longer used or that have been replaced by a new key must be destroyed.

**24-2** The procedures for destroying keys or key components that are no longer used or that have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered. This must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient.

**Note:** Key destruction for keys installed in HSMs and POI devices is addressed in Requirement 31.

**24-2.1** Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic DB backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO-9564 or ISO-11568.

*For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.*

**24-2.2** The key-destruction process must be observed by a third party other than the custodians of any component of that key. I.e., the third party must not be a key custodian for any part of the key being destroyed.

The third-party witness must sign an affidavit of destruction.

**24-2.3** Key components for keys other than the HSM MFK that have been successfully loaded and confirmed as operational must also be destroyed, unless the HSM does not store the encrypted values on a DB but only stores the subordinate keys internal to the HSM. BDKs used in KLDs may also be stored as components where necessary to reload the KLD.

## **Control Objective 6: Keys are administered in a secure manner.**

**Requirement 25:** Access to secret and private cryptographic keys and key material must be:

- a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and
- b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.

**25-1** To reduce the opportunity for key compromise, limit the number of key custodians to the minimum required for operational efficiency.

For example:

**25-1.1** Designate key custodian(s) for each component, such that the fewest number (e.g., a primary and a backup) of key custodians are assigned as necessary to enable effective key management. Key custodians must be employees or contracted personnel.

**25-1.2** Document this designation by having each custodian and backup custodian sign a key-custodian form.

**25-1.3** Each key-custodian form provides the following:

- Specific authorization for the custodian
- Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them
- Signature of the custodian acknowledging their responsibilities
- An effective date for the custodian's access
- Signature of management authorizing the access

**25-1.4** In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual except as noted below for organizations of insufficient size.

*For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual.*

The components collectively held by an individual and his or her direct reports shall not constitute a quorum (or shall not provide any information about the value of the key that is not derivable from a single component).

When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented.

Organizations that are of such insufficient size that they cannot support the reporting-structure requirement must ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian), receive explicit training to instruct them from sharing key components with their direct manager, and must sign key-custodian agreements that includes an attestation to the requirement.

## **Control Objective 6: Keys are administered in a secure manner.**

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

**26-1** Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. These logs must be archived for a minimum of two years subsequent to key destruction.

At a minimum, logs must include the following:

- Date and time in/out
- Key-component identifier
- Purpose of access
- Name and signature of custodian accessing the component
- Tamper-evident package number (if applicable)

**Requirement 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.*

**Note:** *It is not a requirement to have backup copies of key components or keys.*

**27-1** If backup copies of secret and/or private keys exist, confirm that they are maintained in accordance with the same requirements as are followed for the primary keys.

**27-2** If backup copies are created, the following must be in place:

- Creation (including cloning) of top-level keys, e.g., MFKs, must require a minimum of two authorized individuals to enable the process.
- All requirements applicable for the original keys also apply to any backup copies of keys and their components.

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

**28-1** Written procedures must exist, and all affected parties must be aware of those procedures. All activities related to key administration must be documented. This includes all aspects of key administration, as well as:

- 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

## **Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

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

**29-1** Secure cryptographic devices—such as HSMs and POI devices (e.g., PEDs and ATMs)—must be placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering and has or is not otherwise been subject to misuse prior to deployment.

**29-1.1** Controls must be implemented to protect POIs and other SCDs from unauthorized access up to point of deployment.

Controls must include the following:

**29-1.1.1** Access to all POIs and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection.

**29-1.1.2** POIs and other SCDs must not use default keys or data (such as keys that are pre-installed for testing purposes) or passwords.

**29-1.1.3** All personnel with access to POIs and other SCDs **prior to deployment** are documented in a formal list and authorized by management. A documented security policy must exist that specifies personnel with authorized access to all secure cryptographic devices. This includes documentation of all personnel with access to POIs and other SCDs as authorized by management. The list of authorized personnel is reviewed at least annually.

**29-2** Implement a documented “chain of custody” to ensure that all devices are controlled from receipt through to placement into service.

The chain of custody must include records to identify responsible personnel for each interaction with the devices.

## **Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**29-3** Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the following:

- Transportation using a trusted courier service (for example, via bonded carrier). The devices are then securely stored until key-insertion and deployment occurs.
- Use of physically secure and trackable packaging (for example, pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored in such packaging, or in secure storage, until key insertion and deployment occurs.
- A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. The SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key, and the device is further protected until deployment.
- Each cryptographic device is carefully inspected and tested immediately prior to key-insertion and deployment 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 access or modifications. (**Note:** *Unauthorized access includes that by customs officials.*)
  - 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. (**Note:** *this control must be used in conjunction with one of the other methods.*)
  - Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.

**29-4** Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs but must not supplant the implementation of dual-control mechanisms.

**29-4.1** HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained.

**Note:** *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. An example of how serial numbers may be documented by the sender includes but is not limited to the manufacturer's invoice or similar document.*

**29-4.2** 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, PIN-block format translation functionality are in accordance with Requirement 3, or non-ISO PIN-block formats must not be supported without a defined documented and approved business need.*

HSMs used for acquiring functions shall not be configured to output clear-text PINs.

**29-4.3** When HSMs are connected to online systems, controls are in place to prevent the use of an HSM to perform privileged or sensitive functions that are not available during routine HSM operations.

*Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**29-4.4** Inspect and test all HSMS—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised.

Processes must include:

**29-4.4.1** Running self-tests to ensure the correct operation of the device

**29-4.4.2** Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised

**29-4.4.3** Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed

**29-4.4.4** Maintaining records of the tests and inspections, and retaining records for at least one year

**29-5** Maintain HSMS in tamper-evident packaging or in secure storage until ready for installation.

**Requirement 30: Physical and logical protections must exist for deployed POI devices**

**30.1** POI devices must be secured throughout the device lifecycle. The responsible entity must:

- Maintain inventory-control and monitoring procedures to accurately track POI devices in their possession.
- Physically secure POI devices awaiting deployment or otherwise not in use.
- Implement procedures to prevent and detect the unauthorized alteration or replacement of POI devices in possession during deployment.
- Ensure that POI devices are physically secured or otherwise controlled to prevent unauthorized access, modification, or substitution while devices are deployed for use. This includes both attended and unattended devices (for example, kiosks, “pay-at-the-pump,” etc.).
- Prevent unauthorized physical access to devices undergoing repair or maintenance while in their possession.

**30.2** Secure device-management processes must be implemented. The responsible entity must:

- Securely maintain POI devices being returned, replaced, or disposed of, and provide related instructions to third-party providers performing this service.
- Protect POI devices from known vulnerabilities and implement procedures for secure updates to devices.
- Provide auditable logs of any changes to critical functions of the POI device(s).
- Define and implement procedures for merchants on detecting and reporting tampered POI devices, including missing devices.
- Implement mechanisms to monitor and respond to suspicious activity on POI devices deployed at merchant locations.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**Requirement 31:** *Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.*

**31-1** Procedures are in place to ensure that any SCDs to be removed from service—e.g., retired or returned for repair—are not intercepted or used in an unauthorized manner, including that all keys and key material stored within the device must be rendered irrecoverable.

Processes must include the following:

**Note:** *Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*

**31-1.1** HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.

**31-1.2** Key are rendered irrecoverable (for example, zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed under dual-control to prevent the disclosure of any sensitive data or keys.

**31-1.3** SCDs being decommissioned are tested and inspected to ensure keys have been rendered irrecoverable.

**31-1.4** Affected entities are notified before devices are returned.

**31-1.5** Devices are tracked during the return process.

**31-1.6** Records of the tests and inspections are maintained for at least one year.

**Requirement 32:** *Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:*

- a. *Dual access controls required to enable the key-encryption function*
- b. *Physical protection of the equipment (e.g., locked access to it) under dual control*
- c. *Restriction of logical access to the equipment*

**32-1** For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, procedures must be documented and implemented to protect against unauthorized access and use.

Required procedures and processes include the following:

## **Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**32-1.1** Devices must not be authorized for use except under the dual control of at least two authorized people.

**Note:** Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords, or for physical access via a physical lock that requires two individuals, each with a different high-security key. For devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.

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.

**32-1.2** Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.

**32-1.3** Dual control must be implemented for the following:

- To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing;
- To place the device into a state that allows for the input or output of clear-text key components;
- For all access to key-loading devices (KLDs).

**32-1.4** Devices must not use default passwords.

**32-1.5** To detect any unauthorized use, devices are at all times within a secure room and either:

- Locked in a secure cabinet and/or sealed in tamper-evident packaging, or
- Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected.

**Requirement 33:** Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., POI devices supporting PIN and HSMs) placed into service, initialized, deployed, used, and decommissioned.

**33-1** Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed on PIN-processing devices before they are placed into service, as well as devices being decommissioned.

## Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques

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

These requirements pertain to two distinct areas covered separately in the two parts of this Annex.

- **A1 – Remote Key-Distribution Using Asymmetric Techniques Operations:** Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key distribution using asymmetric techniques
- **A2 – Certification and Registration Authority Operations:** Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.
  - Certification Authority requirements apply to all entities (acquirers, manufacturers, and other third parties) signing public keys to be used for remote distribution of cryptographic keys, whether in X.509 certificate-based schemes or other designs, to allow for the required authentication of these signed public keys. For purposes of these requirements, a certificate is any digitally signed value containing a public key, where the term “digitally signed” refers to a cryptographic method used that enforces the integrity and authenticity of a block of data through the cryptographic processing of that block of data with a private key. The CA requirements apply only to methods that allow for the distribution and use of such signed public keys to multiple systems, and as such do not apply to systems that apply symmetric cryptography to keys for authentication (such as through the use of MACs).
  - The Certification Authority requirements are not intended to be applied to devices that sign their own keys, nor to key-loading systems where the key loading is not performed remotely and authentication is provided by another method—such as properly implemented dual control and key-loading device(s)—even if these systems involve the use of certificates.

The control objectives and security requirements are delineated as found in the preceding “PIN Security Requirement – Technical Reference” section of this document, and are in addition to requirements for those entities performing transaction processing.

Unless otherwise specified, the term Certification Authority (CA) refers to any CA in the hierarchy, Root or SubCa.

## A1 – Remote Key Distribution Using Asymmetric Techniques Operations: PIN Security Requirements

**Control Objective 1:** *PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.*

No additional security requirements added for “Symmetric Key Distribution using Asymmetric Techniques.”

**Control 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.*

No additional security requirements added for “Symmetric Key Distribution using Asymmetric Techniques.”

**Control Objective 3:** *Keys are conveyed or transmitted in a secure manner.*

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

**10-2** All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.

**10-3** Key sizes and algorithms must be in accordance with Annex C.

**Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**Requirement 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.*

**15-3** Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange, or key establishment with POIs. POIs and key-distribution hosts (KDHs) using public-key schemes must validate authentication credentials of other such devices involved in the communication immediately prior to any key transport, exchange, or establishment.

Mutual authentication of the sending and receiving devices must be performed.

**Note:** *Examples of this kind of validation include checking current certificate revocation lists or embedding valid authorized KDH certificates in devices and disallowing communication with unauthorized KDHs, as delineated by techniques defined in the Technical FAQs for PCI PTS POI Security Requirements.*

**15-5** Key-establishment and distribution procedures must be designed such that:

- Within an implementation design, there shall be no means available for “man-in-the-middle” attacks—e.g., through binding of the KDH certificate upon the initial communication.
- System implementations must be designed and implemented to prevent replay attacks—e.g., through the use of random nonces.

**15-6** 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. The process must ensure that once keys are injected they are no longer available for injection into other POI devices—i.e., key pairs are unique per POI device.

**Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 18:** *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.*

**18-4** POIs shall only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate-issuing authority generates the key pair on behalf of the POI); and with KDHs for key management, normal transaction processing, and certificate (entity) status checking.

**18-5** KDHs shall only communicate with POIs for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.

**Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 19:** *Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*

**19-6** Key pairs must not be reused for certificate renewal or replacement—i.e., new key pairs must be generated.

Each key pair must result in only one certificate.

**19-7** KDH private keys must not be shared between devices except for load balancing and disaster recovery.

**19-8** POI private keys must not be shared between devices.

**Control Objective 6: Keys are administered in a secure manner.**

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

**21-4** Private keys used to sign certificates, certificate status lists, messages, or for key protection must exist only in one or more of the following forms:

- Within a secure cryptographic device that meets applicable PCI requirements for such a device,
- Encrypted using an algorithm and key size of equivalent or greater strength, or
- As components using a recognized (e.g., Shamir) secret-sharing scheme.

## A2 – Certification and Registration Authority Operations: PIN Security Requirements

**Control Objective 3:** *Keys are conveyed or transmitted in a secure manner.*

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

**10-2** All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.

**10-3** Key sizes and algorithms must be in accordance with Annex C.

**Control Objective 4:** *Key-loading to hosts and PIN entry devices is handled in a secure manner.*

**Requirement 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.*

**15-6** 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. The process must ensure that once keys are injected they are no longer available for injection into other POI devices—i.e., key pairs are unique per POI device.

**Control Objective 5:** *Keys are used in a manner that prevents or detects their unauthorized usage.*

**Requirement 19:** *Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems*

**19-5** If a business rationale exists, a production platform (HSMs and servers/standalone computers) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the CA and RA server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.

At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.

**19-6** Key pairs must not be reused for certificate renewal or replacement—i.e., new key pairs must be generated.

Each key pair must result in only one certificate.

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**19-9** Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose—that is, keys must be used in accordance with their certificate policy. See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.

**19-9.1** CA certificate signature keys, certificate (entity) status checking (for example, Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorized host lists in encryption devices must not be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates.

**Note:** *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.*

**19-9.2** CAs that issue certificates to other CAs must not be used to issue certificates to POIs.

**19-10** 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.

**19-11** CA private keys must not be shared between devices except for load balancing and disaster recovery.

### **Control Objective 6: Keys are administered in a secure manner.**

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

**21-4** Private keys used to sign certificates, certificate status lists, messages, or for key protection must exist only in one or more of the following forms:

- Within a secure cryptographic device that meets applicable PCI requirements for such a device,
- Encrypted using an algorithm and key size of equivalent or greater strength, or
- As components using a recognized (e.g., Shamir) secret-sharing scheme.

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

**22-6** Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.

### **Control Objective 6: Keys are administered in a secure manner.**

**22-7** Mechanisms must be in place to respond to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke or otherwise invalidate the usage of subordinate certificates, and notification of affected entities.

**22-7.1** 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.

**22-7.2** In the event of confirming a compromise, the CA must determine whether to revoke and reissue all signed certificates with a newly generated signing key

**22-7.3** Mechanisms (for example, time stamping) must exist to prevent the usage of fraudulent certificates, once identified.

**22-7.4** The compromised CA must notify any superior or subordinate CAs of the compromise. The compromise damage analysis must include a determination of whether subordinate CAs and KDHS must have their certificates reissued and distributed to them or be notified to apply for new certificates.

**22-8** Minimum cryptographic strength for the CA system shall be:

- Root and subordinate CAs have a minimum RSA 2048 bits or equivalent;
- EPP/PED devices and KDHS have a minimum RSA 1024 bits or equivalent.

*Effective 1 January 2017, KDHS must use a minimum RSA 2048 bits or equivalent.*

The key-pair lifecycle shall result in expiration of KDH keys every five years, unless another mechanism exists to prevent the use of a compromised KDH private key.

**Requirement 25:** Access to secret or private cryptographic keys and key material must be:

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

**25-2** All user access to material that can be used to construct secret and private keys (such as key components) must be directly attributable to an individual user (for example, through the use of unique IDs).

**25-2.1** All user access must be restricted to actions authorized for that role.

**Note:** Examples of how access can be restricted include the use of CA software and operating-system and procedural controls.

## **Control Objective 6: Keys are administered in a secure manner.**

**25-3** The system enforces an explicit and well-defined certificate security policy and certification practice statement. This must include the following:

**25-3.1** CA systems that issue certificates to other CAs and KDHS must be operated offline using a dedicated closed network (not a network segment).

- The network must only be used for certificate issuance and/or revocation.
- Outside network access shall exist only for the purposes of “pushing” certificate-status information to relying parties (for example, KDHS).

**25-3.2** CA or Registration Authority (RA) software updates must not be done over the network (local console access must be used for CA or RA software updates).

**25-3.3** Non-console access must use two-factor authentication. This also applies to the use of remote console access.

**25-3.4** Non-console 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.

**Note:** Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.

**25-3.5** CA certificate (for POI/KDH authentication and validity status checking) signing keys must only be enabled under at least dual control.

**Note:** Certificate requests may be vetted (approved) using single user logical access to the RA application.

**25-4** The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as “dual control.” At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).

**25-5** All CA systems that are not operated strictly offline must be hardened to prevent insecure network access, to include:

- Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, telnet, ftp, etc.) must be removed or disabled.
- Unnecessary ports must also be disabled.
- Documentation must exist to support the enablement of all active services and ports.

**25-5.1** All vendor-default IDs must be changed, removed, or disabled unless necessary for a documented and specific business reason.

Vendor default IDs that are required as owners of objects or processes or for installation of patches and upgrades must only be enabled when required and otherwise must be disabled from login.

**25-5.2** Vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step must be changed, removed, or disabled before installing a system on the network.

## **Control Objective 6: Keys are administered in a secure manner.**

**25-6** Audit trails must include but not be limited to the following:

- All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, and destruction and certificate generation or revocation
- The identity of the person authorizing the operation
- The identities of all persons handling any key material (such as key components or keys stored in portable devices or media)
- Protection of the logs from alteration and destruction

---

**25-6.1** Audit logs must be archived for a minimum of two years.

---

**25-6.2** Records pertaining to certificate issuance and revocation must, at a minimum, be retained for the life of the associated certificate.

---

**25-6.3** Logical events are divided into operating-system and CA application events. For both, the following must 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.

---

**25-7** CA application logs must use a digital signature or a symmetric MAC (based on one of the methods stated in *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*) mechanism for detection of alteration.

The signing/MACing key(s) used for this must be protected using a secure cryptographic device in accordance with the key-management requirements stipulated in this document.

---

**25-7.1** Certificate-processing system components operated online must be protected by a firewall(s) from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to:

- Deny all services not explicitly permitted.
- Disable or remove all unnecessary services, protocols, and ports.
- Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure.
- Disable source routing on the firewall.
- 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 can be taken.
- Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled.

**Control Objective 6: Keys are administered in a secure manner.**

**25-7.2** Online certificate-processing 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.

**25-8** Implement user-authentication management for all system components as follows:

**25-8.1** Initial, assigned passphrases are pre-expired (user must replace at first logon).

**25-8.2** Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.

**25-8.3** If passwords are used, system-enforced expiration life must not exceed 30 days and a minimum life at least one day.

**25-8.4** Passwords must have a minimum length of eight characters using a mix of alphabetic, numeric, and special characters.

**25-8.5** Limit repeated access attempts by locking out the user ID after not more than five attempts.

**25-8.6** Authentication parameters must require a system-enforced passphrase history, preventing the reuse of any passphrase used in the last 12 months.

**25-8.7** Passwords 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.

**25-8.8** The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.

**25-8.9** Where log-on security tokens (for example, smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage. The PIN/passphrase must be at least eight decimal digits in length, or equivalent.

**Note:** Log-on security tokens (for example, smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.

**25-9** Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.

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

**28-2** CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.

---

**Control Objective 6: Keys are administered in a secure manner.**

**28-3** Each CA operator must develop a certification practice statement (CPS). (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content.)

- The CPS must be consistent with the requirements described within this document.
- The CA shall operate in accordance with its CPS.

**Note:** 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.

---

**28-4** Each CA operator must develop a certificate policy. (See RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework for an example of content.)

---

### **Control Objective 6: Keys are administered in a secure manner.**

**28-5** 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 where the certificate request is not generated with the same secure area. These procedures must include at a minimum, two or more of the following for KDH certificate requests:

- Verification of the certificate applicant's possession of the associated private key through the use of a digitally signed certificate request pursuant to PKCS #10 or another cryptographically-equivalent demonstration;
- Determination that the organization exists by using at least one third-party identity-proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization;
- Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant to confirm that the organization has authorized the certificate application, confirmation of the employment of the representative submitting the certificate application on behalf of the certificate applicant, and confirmation of the authority of the representative to act on behalf of the certificate applicant;
- Confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the certificate applicant's representative to confirm that the person named as representative has submitted the certificate application.

**28-5.1** For CA and KDH certificate-signing requests, including certificate or key-validity status changes—for example, revocation, suspension, replacement—verification must include validation that:

- 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 (for example, 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.

**28-5.2** 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.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**Requirement 32:** Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:

- 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.
- c. Restriction of logical access to the equipment

**32-2.1** The certificate-processing operations center must implement a three-tier physical security boundary, as follows:

- Level One Barrier – Consists of the entrance to the facility.
- Level Two Barrier – Secures the entrance beyond the foyer/reception area to the CA facility.
- Level Three Barrier – Provides access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices.

**Level 1 Barrier**

**32-2.2** The entrance to the CA facility/building must include the following controls:

**32-2.2.1** The facility entrance only allows authorized personnel to enter the facility.

**32-2.2.2** The facility has a guarded entrance or a foyer with a receptionist. No entry is allowed for visitors if the entryway is not staffed—i.e., only authorized personnel who badge or otherwise authenticate themselves can enter when entryway is unstaffed.

**32-2.2.3** Visitors (guests) to the facility must be authorized and be registered in a logbook.

**Level 2 Barrier**

**32-2.3** The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.

**32-2.3.1** Visitors must be authorized and escorted at all times within the Level 2 environment.

**32-2.3.2** Access logs must record all personnel entering the Level 2 environment.

**Note:** The logs may be electronic, manual, or both.

**32-2.4** The Level 2 entrance must be monitored by a video-recording system.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**Level 3 Barrier**

**32-2.5** The Level 3 environment must consist of a physically secure, dedicated room not used for any other business activities but certificate operations.

**Note:** All certificate-processing operations must operate in the Level 3 environment.

**32-2.5.1** Doors to the Level 3 area must have locking mechanisms.

**32-2.5.2** The Level 3 environment must be enclosed on all sides (including the ceiling and flooring areas) using techniques such as true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars.

*For example, the Level 3 environment may be implemented within a “caged” environment.*

**32-2.6** Documented procedures must exist for:

- Granting, revocation, and review of access privileges by an authorized officer of the entity operating the CA
- Specific access authorizations, whether logical or physical

**32-2.6.1** All authorized personnel with access through the Level 3 barrier must:

- Have successfully completed a background security check.
- Be assigned resources (staff, dedicated personnel) of the CA operator with defined business needs and duties.

**Note:** This requirement applies to all personnel with pre-designated access to the Level 3 environment.

**32-2.6.2** Other personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.

**32-2.7** The Level 3 environment must require dual-control access and dual-occupancy such that the room is never occupied by one person for more than thirty (30) seconds—i.e., one person may never be in the room for more than 30 seconds alone.

*For example: The Level 3 room is never occupied by one person except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.*

**32-2.7.1** The mechanism for enforcing dual-control and dual-occupancy must be automated.

**32-2.7.2** The system must enforce anti-pass-back.

**32-2.7.3** Dual occupancy requirements are managed using electronic (for example, badge and/or biometric) systems.

**32-2.7.4** Any time a single occupancy exceeds 30 seconds, the system must automatically generate an alarm and audit event that is followed up by security personnel.

**32-2.8** Access to the Level 3 room must create an audit event, which must be logged.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**32-2.8.1** Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel

**32-2.9** The Level 3 environment must be monitored as follows:

**32-2.9.1** A minimum of one or more cameras must provide continuous monitoring (for example, CCTV system) of the Level 3 environment, including the entry and exit.

**Note:** Motion-activated systems that are separate from the intrusion-detection system may be used to activate recording activity.

**32-2.9.2** The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.

**32-2.9.3** Continuous or motion-activated, appropriate lighting must be provided for the cameras.

**Note:** Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (for example, if infrared cameras are used).

**32-2.9.4** Surveillance cameras must be configured to prevent the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data. Cameras must not be able to be remotely adjusted to zoom in or otherwise observe the aforementioned.

**32-2.9.5** Personnel with access to the Level 3 environment must not have access to the media (for example, VCR tapes, digital-recording systems, etc.) containing the recorded surveillance data.

**32-2.9.6** Images recorded from the CCTV system must be securely archived for a period of no less than 45 days.

If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.

**32-2.9.7** CCTV images must be backed up daily. The backup recording must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users (personnel accessing the secure area) and administrators of the system. Alternatively, backups may be stored in other facilities via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements.

**32-3** The environment must have continuous (24/7) intrusion-detection systems in place, which protects the secure area by motion detectors when unoccupied.

**32-3.1** Any windows in the secure area must be locked and protected by alarmed sensors.

**32-3.2** Any windows or glass walls must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.

**32-3.3** The intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have performed an authenticated exit of the secure area. The system must be configured to activate within 30 seconds.

**32-3.4** Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**32-4** All personnel (including CA personnel and visitors) must sign an access logbook when entering the Level 3 environment.

**Note:** This log is in addition to those provided by the access-control system.

**32-4.1** The access log must include the following details:

- Name and signature of the individual
- Organization
- Date and time in and out
- Reason for access or purpose of visit
- For visitor access, the initials of the person escorting the visitor

**32-4.2** The logbook must be maintained within the Level 3 secure environment.

**32-5** All access-control and monitoring systems (including intrusion-detection systems) are powered through an uninterruptible power source (UPS).

**32-6** All alarm events must be documented.

**32-6.1** An individual must not sign off on an alarm event in which they were involved.

**32-6.2** The use of any emergency entry or exit mechanism must cause an alarm event.

**32-6.3** All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.

**32-7** A process must be implemented for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs. It must be ensured that synchronization errors between CCTV, intrusion detection, and access control cannot exceed one minute.

**Note:** This may be done by either automated or manual mechanisms.

**32-7.1** If a manual synchronization process is used, synchronization must occur at least quarterly; and documentation of the synchronization must be retained for at least a one-year period.

## Normative Annex B – Key-Injection Facilities

### Key-Injection Facility Security Requirements Technical Reference

#### Introduction

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

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

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

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

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

**Note:**

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

## PIN Security Requirements

**Control Objective 1:** *PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.*

**Requirement 1:** *All cardholder-entered PINs must be processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD.*

**1-2** Key-injection facilities must only inject keys into equipment that conforms to the requirements for SCDs.

Key-injection platforms and systems shall include hardware devices for managing (e.g., generating and storing) the keys that conform to the requirements for SCDs.

**1-3** Ensure that all hardware security modules (HSMs) are either:

- FIPS140-2 Level 3 or higher certified, or
- PCI approved.

**1-4** The approval listing must match the deployed devices in the following characteristics:

- Vendor name
- Model name and number
- Hardware version number
- Firmware version number
- For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment

**1-5** The KIF platform provider maintains documentation detailing the distributed KIF architecture and key-management flows. The platform provider must:

- Maintain current documentation that describes or illustrates the architecture of the KIF, including all distributed KIF functionality.
- Maintain documentation detailing the flow of keys from the key generation, through the distributed functionality to the destination device. The documentation should indicate how personnel interaction and inventory management is integrated into the flow.

**Control 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.*

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

**5-1** 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. Cryptographic keys or key components must be generated by one of the following:

- An approved key-generation function of a PCI-approved HSM or POI
- An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM
- An approved random number generator that has been certified by an independent laboratory to comply with *NIST SP 800-22*

**Note:** *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.*

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

**6-1** Implement security controls, including dual control and tamper protection to prevent the unauthorized disclosure of keys/key components.

**6-1.1** Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.

**6-1.2** There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.

**Note:** *Full-length key components or key shares derived using a recognized key-splitting algorithm are not considered key parts and do not provide any information regarding the actual cryptographic key.*

**6-1.3** Devices used for generation of clear-text key components that are output in the clear must be powered off when not in use. Logically partitioned devices used concurrently for other processes—e.g., providing services simultaneously to host systems, such as for transaction processing—must have key-generation capabilities disabled when not in use and other activities are continuing.

**6-1.4** Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (for example, unnecessary cables).

**6-1.5** Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area. It must not be feasible to observe the key-component/key-generation process whereby clear-text keying material is observable either directly or via camera monitoring.

**Control 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.**

**6-2** Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.

*For example, it is not permitted for the cryptographic key to be passed through the memory of a computer unless it has been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed and used solely for key loading are permitted for use if all other requirements can be met, including those of Requirement 5 and the controls defined in Requirement 13 of Annex B.*

*Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.*

*Single-purpose computers with an installed SCD where clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) meet this requirement. Where the components pass through unprotected memory of the PC, it must meet Requirement 13 of Annex B.*

**Note:** See Requirement 13.

**6-3** Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that:

- Only approved key custodians can observe their own key component.
- Tampering can be visually detected.

Printers used for this purpose must not be used for other purposes.

**6-4** Any residue that may contain clear-text keys or components must be destroyed or securely deleted—depending on media—immediately after generation of that key, to prevent disclosure of a key or the disclosure of a key component to an unauthorized individual.

*Examples of where such key residue may exist include (but are not limited to):*

- *Printing material, including ribbons and paper waste*
- *Memory storage of a key-loading device, after loading the key to a different device or system*
- *Other types of displaying or recording*

**6-5** Asymmetric-key pairs must either be:

- Generated by the device that will use the key pair; or
- If generated externally, the private key of the key pair and all related critical security parameters (for example, secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.
- Devices used for key generation or key injection are securely stored when not in use.

**Control 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.*

**6-6** Policy and procedures must exist to ensure that key components are prohibited from being transmitted across insecure channels. These include but are not limited to:

- Dictating verbally keys or components
- Recording key or component values on voicemail
- Faxing, e-mailing, or otherwise conveying clear-text secret or private keys or components
- Conveying clear-text private or secret key components without containing them within tamper-evident, authenticable packaging
- Writing key or component values into startup instructions
- Taping key or component values to or inside devices
- Writing key or component values in procedure manuals

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

**7-1** Written key-creation procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of those procedures. All key-creation events performed by a key-injection facility must be documented. Procedures for creating all keys must be documented.

**7-2** Logs must exist for the generation of higher-level keys such as KEKs exchanged with other organizations and MFKs and BDKs.

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**Requirement 8:** Secret or private keys must be transferred by:

- a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or
- b. Transmitting the key in ciphertext form.

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

Keys conveyed **to** a key-injection facility must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:

- 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 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;
- Private asymmetric keys for use in remote key-loading systems.

Keys conveyed **from** a key-injection facility (including facilities that are device manufacturers) must be conveyed in compliance with these requirements. Such keys can include, but are not limited to:

- Digitally signed HSM-authentication public key(s) 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).

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**8-1** Keys must be transferred either encrypted or—if clear text—as two or more components using different communication channels or within an SCD.

*Note this does not apply to keys installed in POI devices meeting Requirement 1 when shipped from the key-injection facility.*

Clear-text key components may be transferred in SCDs or using tamper-evident, authenticable packaging.

- Where key components are transmitted in clear-text using tamper-evident, authenticable mailers:
  - Components/shares must be conveyed using at least two separate communication channels, such as different courier services. Components/shares sufficient to form the key must not be conveyed using the same communication channel.
  - Ensure that details of the serial number of the package are conveyed transmitted separately from the package itself.
  - Documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material.
- Where SCDs are used to convey components, the mechanisms or data (e.g., PIN) to obtain the key component from the SCD must be conveyed using a separate communication channel from the SCD, or it must be conveyed in the same manner as a paper component. SCDs must be inspected for signs of tampering.
- Where an SCD (HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual-control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering.

**Note:** *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.*

**8-2** A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares sufficient to form the necessary threshold to derive the key.

*E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e.,  $m = 3$ ) can be used to derive the key, no single individual can have access to more than two components/shares.*

**8-3** E-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted, unless the key (or component) has already been encrypted in accordance with these requirements—i.e., in an SCD. This is due to the existence of these key values in unprotected memory just prior to encryption or subsequent to decryption. In addition, corporate e-mail systems allow the recovery by support staff of the clear text of any encrypted text or files conveyed through those systems.

Other similar mechanisms, such as SMS, fax, or telephone shall not be used to convey clear-text key values.

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**8-4** Public keys must be conveyed in a manner that protects their integrity and authenticity.

Examples of acceptable methods include:

- Use of public-key certificates as defined in Annex A that are created by a trusted CA that meets the requirements of Annex A.
- A hash of the public key sent by a separate channel (for example, mail)
- Using a MAC (message authentication code) created using the algorithm defined in ISO 16609
- Be within an SCD

**Note:** *Self-signed certificates must not be used as the sole method of authentication.*

**Requirement 9:** *During its transmission, conveyance, or movement between any two organizational entities, any single unencrypted secret or private key component must at all times be protected.*

*Sending and receiving entities are equally responsible for the physical protection of the materials involved.*

*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 BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf), or key components for the BDKeys themselves, and terminal master keys used in the master key/session key key-management method.*

**9-1** Any single clear-text secret or private key component/share must at all times be either:

- Under the continuous supervision of a person with authorized access to this component, or
- Locked in a security container (including tamper-evident, authenticable packaging) in such a way that unauthorized access to it would be detected, or
- Contained within a physically secure SCD.

**Note:** *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.*

**9-2** Packaging or mailers (i.e., pre-numbered tamper-evident packaging) containing clear-text key components are examined for evidence of tampering before being opened. Any sign of package tampering must result in the destruction and replacement of:

- The set of components
- Any keys encrypted under this (combined) key

**9-3** No one but the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.

### **Control Objective 3: Keys are conveyed or transmitted in a secure manner.**

**9-4** Mechanisms must exist to ensure that only authorized custodians:

- Place key components into pre-numbered tamper-evident, authenticable packaging for transmittal.
- Check tamper-evident packaging upon receipt for signs of tamper prior to opening the tamper-evident, authenticable packaging containing key components.
- Check the serial number of the tamper-evident packing upon receipt of a component package.

**9-5** Pre-numbered, tamper-evident, authenticable bags shall be used for the conveyance of clear-text key components. Out-of-band mechanisms must be used to verify receipt of the appropriate bag numbers.

**Note:** *Numbered courier bags are not sufficient for this purpose*

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

*Key-encryption keys used to convey keys to a key-injection facility must be (at least) as strong as any key transmitted or conveyed. Such keys include but are not limited to, 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).*

**10-1** All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be (at least) as strong as the key being sent, as delineated in Annex C except as noted below for RSA keys used for key transport and for TDEA keys.

- DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.
- A double- or triple-length DEA key must not be encrypted with a DEA key of a lesser strength.
- TDEA keys shall not be used to protect AES keys.
- TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.
- RSA keys used to transmit or convey other keys must have bit strength of at least 80 bits.
- RSA keys encrypting keys greater in strength than 80 bits shall have bit strength at least 112 bits.

**Note:** *Entities that are in the process of migrating from older devices to PCI devices approved against version 3 or higher of the PCI POI Security Requirements—and thus have a mixed portfolio of devices—they may use RSA key sizes less than 2048 and use SHA-1 to help facilitate the migration. However, in all cases, version 3 or higher devices must implement RSA using key sizes of 2048 or higher and SHA-2 within 24 months of the publication of these requirements when used for key distribution using asymmetric techniques in accordance with Annex A.*

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

**11-1** Written procedures must exist and be known to all affected parties.

**11-2** Methods used for the conveyance or receipt of keys must be documented.

#### **Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

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

Key-injection facilities must load keys using dual control and for clear-text secret and private keys, split knowledge. Such keys include, but are not limited to:

- 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 from a merchant to a third party that is injecting keys 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;
- Master keys for key-injection platforms and systems that include hardware devices (SCDs) for managing (e.g., generating and storing) the keys used to encrypt other keys for storage in the key-injection platform system;
- Public and private key pairs loaded into the POIs for supporting remote key-establishment and distribution applications;
- Digitally signed POI public key(s) signed by a device manufacturer's private key and subsequently loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable). Dual control is not necessary where other mechanisms exist to validate the authenticity of the key, such as the presence in the device of an authentication key;
- Device manufacturer's authentication key (e.g., vendor root CA public key) loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable).

**12-1** The loading of secret or private keys, when loaded from the individual key components, must be managed using the principles of dual control and split knowledge.

**Note:** Manual key loading may involve the use of media such as paper, smart cards, or other physical tokens.

**12-2** Procedures must be established that will prohibit any one person from having access to components sufficient to form an encryption key when components are removed from and returned to storage for key loading.

**Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**12-3** The loading of clear-text cryptographic keys using a key-loading device requires dual control to authorize any key-loading session. It shall not be possible for a single person to use the key-loading device to load clear keys alone.

Dual control must be implemented using one or more of, but not limited to, the following techniques:

- Two or more passwords of five characters or more (vendor default values must be changed),
- Multiple cryptographic tokens (such as smartcards), or physical keys,
- Physical access controls

*Note that for devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.*

**12-4** Key components for symmetric keys must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components. (For example, via XOR'ing of full-length components.)

*Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two 8-hexadecimal character halves to form a 16-hexadecimal secret key.*

The resulting key must only exist within the SCD.

**12-5** Hardware security module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA (including parity bits) or AES using a key size of at least 128 bits.

**12-6** Any other SCD loaded with the same key components must combine all entered key components using the identical process.

**12-7** The initial terminal master key (TMK) must be loaded to the device using either asymmetric key-loading techniques or manual techniques—e.g., the device keypad, IC cards, key-loading device, etc. Subsequent loading of the terminal master key may use techniques described in this documents such as:

- Asymmetric techniques
- Manual techniques
- The existing TMK to encrypt the replacement TMK for download.

Keys shall not be reloaded by any methodology in the event of a compromised device, and must be withdrawn from use.

#### **Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**12-8** If key-establishment protocols using public-key cryptography are used to distribute secret keys, these must meet the requirements detailed in Annex A of this document. For example:

A public-key technique for the distribution of symmetric secret keys must:

- Use public and private key lengths that are in accordance with Annex C 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 POI device or host-to-host if applicable, including assurance to the host that the POI device actually has (or actually can) compute the session key and that no entity other than the POI device specifically identified can possibly compute the session key.

**12-9** Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (for example, POIs and other SCDs).

**Note:** Such controls may include but are not limited to:

- *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 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 custodians who store and access key components under dual-control and split-knowledge mechanisms.*
- *Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry.*

#### **Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

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

*Key-injection facilities must ensure key-loading mechanisms are not subject to disclosure of key components or keys.*

*Some key-injection platforms use personal-computer (PC)-based software applications, whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. These weaknesses include:*

- *XOR'ing of key components is performed in software.*
- *Clear-text 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., BDKeys, TMKeys) on removable media 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.*

**13-1** Clear-text secret and private keys and key components must be transferred into an SCD only when it can be ensured that:

- Any cameras present in the environment must be positioned to ensure they cannot monitor the entering of clear-text key components.
- There is not any mechanism at the interface between the conveyance medium and the SCD that might disclose the transferred keys.
- The SCD must be inspected prior to use to ensure that it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying materials.
- SCDs must be inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading.
- An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are uniquely identified by the device.

**13-2** Only SCDs shall be used in the loading of clear-text secret or private keys or their components outside of a secure key-loading facility, as delineated in this Annex. For example, ATM controller (computer) keyboards shall never be used for the loading of clear-text secret or private keys or their components.

**13-3** The loading of secret or private key components from an electronic medium to a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following:

- The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-loading of the component into the cryptographic device); or
- All traces of the component are erased or otherwise destroyed from the electronic medium.

**Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**13-4** For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:

**13-4.1** The key-loading device must be a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.

**13-4.2** The key-loading device must be under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.

**13-4.3** The key-loading device must be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.

**13-4.4** The key-loading device must not retain any information that might disclose the key that was installed in the device or a key that it has successfully transferred.

**13-5** Any media (electronic or otherwise) containing secret or private key components used for loading cryptographic keys must be maintained in a secure storage location and accessible only to authorized custodian(s).

When removed from the secure storage location, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process.

The media upon which a component resides must be physically safeguarded at all times when removed from secure storage.

Key components that can be read/displayed (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are never used in a manner that would result in the component being displayed in clear text to a non-custodian for that component.

**13-6** If the component is in human-readable form (e.g., printed within a PIN-mailer type document), it must be visible only to the designated component custodian and only for the duration of time required for this person to privately enter the key component into an SCD.

**13-7** Written or printed key-component documents must not be opened until immediately prior to use.

**13-8** A person with access to any component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key.

*E.g., in an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such that any three key components or shares (i.e.,  $m = 3$ ) can be used to derive the key, no single individual can have access to more than two components/shares.*

**13-9** Key-injection facilities that use PC-based key-loading software platforms or similar devices (e.g., modified PEDs) that allow clear-text secret and/or private keys and/or their components to exist in unprotected memory outside the secure boundary of an SCD must minimally implement the following additional controls:

**Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**13-9.1** PCs and similar devices must be:

- Standalone (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.

**13-9.2** All hardware used in key loading (including the PC) must be managed under dual control. Key-injection must not occur unless there are minimally two individuals in the key-injection room at all times during the process. If a situation arises that would cause only one person to be in the room, all individuals must exit until at least two can be inside.

**13-9.3** 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 (no less frequently than weekly) 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:

- 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 with a minimum retention period of 45 days.

**13-9.4** Additionally:

**13-9.4.1** Cable attachments and the key-loading device must be examined before each use to ensure the equipment is free from tampering.

**13-9.4.2** The key-loading device must be started from a powered-off position every time key-loading activities occur.

**13-9.4.3** The software application must load keys without recording any clear-text values on portable media or other unsecured devices.

**13-9.4.4** Clear-text keys must not be stored except within an SCD.

**13-9.4.5** 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.

**13-9.4.6** The key-injection personnel must not have system-administration capability at either the O/S or the application level on the PC.

**13-9.4.7** The PC must not be able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.

#### **Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**13-9.4.8** 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.

**13-9.4.9** If the PC application stores clear-text key components (e.g., BDKs or TMKs) on portable electronic media (e.g., smart cards), the media must be secured as components under dual control when not in use. The key components must 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 BDK should be loaded from components each time and this requires manual tracking of the device ID counter and serial numbers from the previous key-loading session. Key-injection facilities with PC applications that require passwords to be used to initiate decryption of keys on portable electronic media (e.g., smart cards) must ensure the passwords are maintained under dual control and split knowledge.

**13-9.4.10** Manufacturer's default passwords for PC-based applications must be changed.

**Requirement 14:** All hardware and access/authentication mechanisms (e.g., passwords) used for key loading must be managed under the principle of dual control.

*Key-injection facilities must ensure that the key-injection application passwords and associated user IDs are managed in such a way as to enforce dual control. Also, the hardware used for key-injection must be managed under dual control. Vendor default passwords must be changed.*

**14-1** Any hardware and passwords used in the key-loading function must be controlled and maintained in a secure environment under dual control. Resources (e.g., passwords and associated hardware) must be managed such that no single individual has the capability to enable key loading. This is not to imply that individual access authentication mechanisms must be managed under dual control.

**14-2** All cable attachments must be examined before each key-loading operation to ensure they have not been tampered with or compromised.

**14-3** Key-loading equipment usage must be monitored and a log of all key-loading activities maintained for audit purposes containing at a minimum date, time, personnel involved, and number of devices keys are loaded to.

**14-4** Any physical tokens (e.g., brass keys or chip cards) used to enable key-loading must not be in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control. These tokens must be secured in a manner similar to key components including the use of access-control logs for when removed or placed into secure storage.

**Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.**

**14-5** Default password or PINs used to enforce dual-control must be changed, and documented procedures must exist to require that these password/PINs be changed when assigned personnel change.

**Requirement 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.*

**15-1** A cryptographic-based validation mechanism must be in place to ensure the authenticity and integrity of keys and/or their components (for example, testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded). See ISO 11568. Where check values are used, recorded, or displayed, key-component check values and key check values shall not exceed six hexadecimal characters in length.

**15-2** The public key must have its authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plaintext form, must:

- Be within a certificate as defined in Annex A; or
- Be within a PKCS#10; or
- Be within an SCD; or
- Have a MAC (message authentication code) created using the algorithm defined in ISO 16609.

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

**16-1** Documented key-loading procedures must exist for all devices (e.g., HSMs and POIs), and all parties involved in cryptographic key-loading must be aware of those procedures.

**16-2** All key-loading events must be documented. Audit trails must be in place for all key-loading events.

**Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**Requirement 18:** *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.*

**18-2** To prevent or detect usage of a compromised key, key-component packaging or containers 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.

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**18-3** Effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself;
- A digital signature computed over that same data;
- An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.

**18-4** Controls must be in place to prevent and detect the loading of unencrypted private and secret keys or their components by any one single person.

**Note:** Controls include physical access to the room, logical access to the key-loading application, video surveillance of activities in the key-injection room, physical access to secret or private cryptographic key components or shares, etc.

**18-5** 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:

- All devices loaded with keys must be tracked at each key-loading session by serial number.
- Key-injection facilities must use something unique about the POI (for example, logical identifiers) when deriving the key (for example, DUKPT, TMK) injected into it.

**Requirement 19:** Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.

- Where test keys are used, key-injection facilities must use a separate test system for the injection of test keys.
- Test keys must not be injected using the production platform, and test keys must not be injected into production equipment.
- 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.

**19-1** Encryption keys must be used only for the purpose they were intended (i.e., key-encryption keys must not to be used as PIN-encryption keys, PIN-encryption keys must not be used for account data, etc.). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**19-2** Private keys must only be used as follows:

- For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating POI devices).
- Private keys shall never be used to encrypt other keys.

**19-3** Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).

**19-4** Keys must never be shared or substituted between production and test/development systems:

- Key used for production keys must never be present or used in a test system, and
- Keys used for testing keys must never be present or used in a production system.

**19-5** If a business rationale exists, a production platform (HSM and server/standalone computer) may be temporarily used for test purposes. However, all keying material must be deleted from the HSM(s) and the key-injection server/computer platforms prior to testing. Subsequent to completion of testing, all keying materials must be deleted, the server/computer platforms must be wiped and rebuilt from read-only media, and the relevant production keying material restored using the principles of dual control and split knowledge as stated in these requirements.

At all times the HSMs and servers/computers must be physically and logically secured in accordance with these requirements.

*Note this does not apply to HSMs that are never intended to be used for production.*

**Requirement 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 (e.g., PED) that processes PINs must be unique (except by chance) to that device.*

**20-1** POI devices must implement unique secret and private keys for any function directly or indirectly related to PIN protection. These keys must be known only in that device and in hardware security modules (HSMs) 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.

This means that not only the PIN-encryption key(s), but also keys that are used to protect other keys: firmware-authentication keys, payment application authentication, and display prompt control keys. As stated in the requirement, this does not apply to public keys resident in the device.

**20-2** If a transaction-originating terminal (for example POI device) interfaces with more than one acquiring organization, the transaction-originating terminal SCD must have a completely different and unique key or set of keys for each acquiring organization. These different keys, or sets of keys, must be totally independent and not variants of one another.

**20-3** Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device.

This requirement refers to the use of a single “base” key to derive master keys for many different POIs, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys once loaded, for example, as done with DUKPT.

### **Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.**

**20-4** Entities processing or injecting DUKPT or other key-derivation methodologies must incorporate a segmentation strategy in their environments. Segmentation must use one or more of the following techniques:

- Different BDKeys for each financial institution
- Different BDKeys by injection vendor (e.g., ESO), terminal manufacturer, or terminal model
- Different BDKeys by geographic region, market segment, platform, or sales unit

Injection vendors must use at least one unique Base Derivation Key (BDK) per acquiring organization, and must be able to support segmentation of multiple BDKeys of acquiring organizations.

**20-5** Key-injection facilities that load DUKPT keys for various POI types for the same entity must use separate BDKeys 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.

#### **20-6 Remote Key-Establishment and Distribution Applications**

The following requirements apply to key-injection facilities participating in remote key-establishment and distribution applications:

- Keys must be uniquely identifiable in all hosts and POI Devices (e.g., EPPs/PEDs). Keys must be identifiable via cryptographically verifiable means (e.g., through the use of digital signatures or key check values).
- Key pairs must be unique per POI device (e.g., EPPs and PEDs).

### **Control Objective 6: Keys are administered in a secure manner.**

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

*Key-injection facilities must ensure that KEKs and PIN-encryption keys do not exist outside of SCDs except when encrypted or stored under dual control and split knowledge.*

*Some key-injection platforms use personal-computer (PC)-based software applications or similar devices whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD for loading keys. Such systems do not therefore meet this requirement. Such systems have inherent weaknesses that, if exploited, may cause the unauthorized disclosure of components and/or keys. The exploitation of some of the weaknesses could be possible without collusion. Therefore, key-injection facilities that use PC-based key-loading software platforms whereby clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of an SCD must minimally implement the compensating controls outlined in Requirement 13.*

## **Control Objective 6: Keys are administered in a secure manner.**

**21-1** Secret or private keys must only exist in one or more of the following forms:

- At least two separate key shares or full-length components
- Encrypted with a key of equal or greater strength as delineated in Annex C
- Contained within a secure cryptographic device

**21-2** Wherever key components are used, they have the following properties:

**21-2.1** Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.

**21-2.2** Construction of the cryptographic key requires the use of at least two key components/shares.

**21-2.3** Each key component/share has one or more specified authorized custodians.

**21-2.4** Procedures exist to ensure any custodian never has access to sufficient key components or shares of a secret or private key to reconstruct a cryptographic key.

*For example, in an  $m$ -of- $n$  scheme (which must use a recognized secret-sharing scheme such as Shamir), where only two of any three components are required to reconstruct the cryptographic key, a custodian must not have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian must not then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.*

*In an  $m$ -of- $n$  scheme where  $n=5$  and where all three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (for example, component A and component B), as a second custodian (with, in this example, component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*

**21-3** Key components must be stored as follows:

**21-3.1** Key components that exist in clear text outside of an SCD must be sealed in opaque, pre-numbered tamper-evident, authenticable packaging that prevents the determination of the key component without noticeable damage to the packaging.

**Note:** *Tamper-evident, authenticable packaging (opacity may be envelopes within tamper-evident packaging) used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to “read” the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.*

**21-3.2** Key components for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s).

**Note:** *Furniture-based locks or containers with a limited set of unique keys—for example, desk drawers—are not sufficient to meet this requirement.*

*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.*

## **Control Objective 6: Keys are administered in a secure manner.**

**21-3.3** If a key component is stored on a token, and an access code (e.g., a PIN or similar access-control mechanism) is used to access the token, only that token's owner (or designated backup(s)) must have possession of both the token and its access code.

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

*Key-injection facilities must have written procedures to follow in the event of compromise of any key associated with the key-injection platform and process. Written procedures must exist, and all parties involved in cryptographic key loading must be aware of those procedures. All key-compromise procedures must be documented.*

**22-1** Procedures for known or suspected compromised keys must include the following:

**22-1.1** Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.

**22-1.2** If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.

**22-1.3** A secret or private cryptographic key must be replaced with a new key whenever the compromise of the original key is known. Suspected compromises must be assessed and the analysis formally documented. If compromise is confirmed, the key must be replaced. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant or an irreversible transformation of the original key. Compromised keys must not be used to facilitate replacement with a new key(s).

**Note:** *The compromise of a key must result in the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key.*

*Known or suspected substitution of a secret key must result in the replacement of that key and any associated key-encipherment keys.*

**22-1.4** A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including:

- Identification of key personnel
- A damage assessment including, where necessary, the engagement of outside consultants
- Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.

**22-1.5** Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to:

- Missing secure cryptographic devices
- Tamper-evident seals or authenticable envelope numbers or dates and times not agreeing with log entries
- Tamper-evident seals or authenticable 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
- Failure to document that a secret or private key has been managed using the principles of dual control and split knowledge from its date of creation

## **Control Objective 6: Keys are administered in a secure manner.**

**22-2** If attempts to load a secret key or key component into a KLD or POI 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 from or otherwise destroyed in the original KLD or POI

**Requirement 23:** *Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key.*

*Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage.*

*Keys generated using a non-reversible process, such as key-derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.*

**23-1** Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. Variants of the same key may be used for different purposes, but must not be used at different levels of the key hierarchy. For example, reversible transformations must not generate key-encipherment keys from PIN keys.

**Note:** *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*

**23-2** An MFK used by host processing systems for encipherment of keys for local storage—and variants of the MFK—must not be used external to the (logical) configuration that houses the MFK itself. For example, MFKs and their variants used by host processing systems for encipherment of keys for local storage shall not be used for other purposes, such as key conveyance between platforms that are not part of the same logical configuration.

**23-3** Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate working keys (e.g., PEKs) from key-encrypting keys.

Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or working keys with different purposes from another working key.

**Note:** *Using transforms of keys across different levels of a key hierarchy—for example, generating a PEK key from a key-encrypting key—increases the risk of exposure of each of those keys.*

*It is acceptable to use one “working” key to generate multiple reversible transforms to be used for different working keys, such as a PIN key, MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.*

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

**24-1** Instances of secret or private keys, and their key components, that are no longer used or that have been replaced by a new key must be destroyed.

## **Control Objective 6: Keys are administered in a secure manner.**

**24-2** The procedures for destroying keys or key components that are no longer used or that have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered. This must be accomplished by use of a cross-cut shredder, pulping or burning. Strip-shredding is not sufficient.

**Note:** Key destruction for keys installed in HSMs and POI devices is addressed in Requirement 31.

**24-2.1** Keys on all other storage media types in all permissible forms—physically secured, enciphered (except for electronic DB backups of cryptograms), or components—must be destroyed following the procedures outlined in ISO-9564 or ISO-11568.

*For example, keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.*

**24-2.2** The key-destruction process must be observed by a third party other than the custodians of any component of that key. I.e., the third party must not be a key custodian for any part of the key being destroyed.

The third-party witness must sign an affidavit of destruction.

**24-2.3** Key components for keys other than the HSM MFK that have been successfully loaded and confirmed as operational must also be destroyed, unless the HSM does not store the encrypted values on a database but only stores the subordinate keys internal to the HSM. BDKs used in KLDs may also be stored as components where necessary to reload the KLD.

**Requirement 25:** Access to secret and private cryptographic keys and key material must be:

- a. Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and
- b. Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.

**25-1** To reduce the opportunity for key compromise, limit the number of key custodians to the minimum required for operational efficiency.

For example:

**25-1.1** Designate key custodian(s) for each component, such that the fewest number (e.g., a primary and a backup) of key custodians are assigned as necessary to enable effective key management. Key custodians must be employees or contracted personnel

**25-1.2** Document this designation by having each custodian and backup custodian sign a key-custodian form.

**25-1.3** Each key-custodian form provides the following:

- Specific authorization for the custodian
- Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them
- Signature of the custodian acknowledging their responsibilities
- An effective date for the custodian's access
- Signature of management authorizing the access

**Control Objective 6: Keys are administered in a secure manner.**

**25-1.4** In order for key custodians to be free from undue influence in discharging their custodial duties, key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual.

*For example, for a key managed as three components, at least two individuals report to different individuals. In an m-of-n scheme (which must use a recognized secret-sharing scheme such as Shamir), such as three of five key shares to form the key, key custodians sufficient to form the threshold necessary to form the key must not report to the same individual.*

The components collectively held by an individual and his or her direct reports shall not constitute a quorum (or shall not provide any information about the value of the key that is not derivable from a single component).

When the overall organization is of insufficient size such that the reporting structure cannot support this requirement, procedural controls can be implemented.

Organizations that are of such insufficient size that they cannot support the reporting-structure requirement must ensure key custodians do not report to each other (i.e., the manager cannot also be a key custodian), receive explicit training to instruct them from sharing key components with their direct manager and must sign key-custodian agreements that includes an attestation to the requirement.

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

*Key-injection facilities must maintain logs for the key management of all keys and keying material used in all key-loading sessions. These include keys and materials removed from safes and used in the loading process.*

**26-1** Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD. These logs must be archived for a minimum of two years subsequent to key destruction.

At a minimum, logs must include the following:

- Date and time in/out
- Key-component identifier
- Purpose of access
- Name and signature of custodian accessing the component
- Tamper-evident package number (if applicable)

**Requirement 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.*

**Note:** *It is not a requirement to have backup copies of key components or keys.*

**27-1** If backup copies of secret and/or private keys exist, confirm that they are maintained in accordance with the same requirements as are followed for the primary keys.

## **Control Objective 6: Keys are administered in a secure manner.**

**27-2** If backup copies are created, the following must be in place:

- Creation (including cloning) must require a minimum of two authorized individuals to enable the process.
- All requirements applicable for the original keys also apply to any backup copies of keys and their components.

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

**28-1** Written procedures must exist, and all affected parties must be aware of those procedures. All activities related to key administration performed by a key-injection facilities must be documented. This includes all aspects of key administration, as well as:

- 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

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

*Key-injection facilities must ensure that only legitimate, unaltered devices are loaded with cryptographic keys.*

*Secure areas must be established for the inventory of PEDs that have not had keys injected. The area must have extended walls from the real floor to the real ceiling using sheetrock, wire mesh, or equivalent. Equivalence can be steel cages extending floor to real ceiling. The cages can have a steel cage top in lieu of the sides extending to the real ceiling. The cages must have locks (with logs) or badge control with logging for entry.*

**29-1** Secure cryptographic devices—such as HSMs and POI devices (e.g., PEDs and ATMs)—must be placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering and has not otherwise been subject to misuse prior to deployment.

**29-1.1** Controls must be implemented to protect POIs and other SCDs from unauthorized access up to point of deployment.

Controls must include the following:

**29-1.1.1** Access to all POIs and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection.

**29-1.1.2** POIs and other SCDs must not use default keys or data (such as keys that are pre-installed for testing purposes) or passwords.

### **Control Objective 6: Keys are administered in a secure manner.**

**29-1.1.3** All personnel with access to POIs and other SCDs **prior to deployment** are documented in a formal list and authorized by management. A documented security policy must exist that specifies personnel with authorized access to all secure cryptographic devices. This includes documentation of all personnel with access to POIs and other SCDs as authorized by management. The list of authorized personnel is reviewed at least annually.

**29-2** Implement a documented “chain of custody” to ensure that all devices are controlled from receipt through to placement into service.

The chain of custody must include records to identify responsible personnel for each interaction with the devices.

**29-3** Implement physical protection of devices from the manufacturer’s facility up to the point of key-insertion and deployment, through one or more of the following.

- Transportation using a trusted courier service (for example, via bonded carrier). The devices are then securely stored until key-insertion and deployment occurs.
- Use of physically secure and trackable packaging (for example, pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored in such packaging, or in secure storage, until key insertion and deployment occurs.
- A secret, device-unique “transport-protection token” is loaded into the secure storage area of each device at the manufacturer’s facility. Before key-insertion, the SCD used for key-insertion verifies the presence of the correct “transport-protection token” before overwriting this value with the initial key, and the device is further protected until deployment.
- Each cryptographic device is carefully inspected and tested immediately prior to key-insertion and deployment 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 access or modifications. (**Note:** *Unauthorized access includes that by customs officials.*)
  - 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. (Note: This control must be used in conjunction with one of the other methods.)
  - Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.

## **Control Objective 6: Keys are administered in a secure manner.**

**29-4** Dual-control mechanisms must exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle. Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted HSMs but must not supplant the implementation of dual-control mechanisms.

**29-4.1** HSM serial numbers must be compared to the serial numbers documented by the sender (sent using a different communication channel from the device) to ensure device substitution has not occurred. A record of device serial-number verification must be maintained.

*Note: 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. An example of how serial numbers may be documented by the sender includes but is not limited to the manufacturer's invoice or similar document*

**29-4.2** 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, PIN-block format translation functionality are in accordance with Requirement 3, or non-ISO PIN-block formats must not be supported without a defined documented and approved business need.*

**HSMs used for acquiring functions shall not be configured to output clear-text PINs.**

**29-4.3** When HSMs are connected to online systems, controls are in place to prevent the use of an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.

**29-4.4** Inspect and test all HSMs—either new or retrieved from secure storage—prior to installation to verify devices have not been tampered with or compromised.

Processes must include:

**29-4.4.1** Running self-tests to ensure the correct operation of the device

**29-4.4.2** Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised

**29-4.4.3** Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed

**29-4.4.4** Maintaining records of the tests and inspections, and retaining records for at least one year

**29-5** Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.

## **Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

### **Requirement 30:** Physical and logical protections must exist for deployed POI devices

*Key-injection facilities must ensure protection against unauthorized use of SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.*

**30-3** Processes must exist to ensure that key injection operations are performed and reconciled on an inventory of pre-authorized devices.

Processes must include the following:

- Each production run must be associated with a predefined inventory of identified POI devices to be injected or initialized with keys.
- Unauthorized personnel must not be able to modify this inventory without detection.
- All POI devices to be initialized with keys on a production run must be identified and accounted for against the inventory.
- Unauthorized POI devices submitted for injection or initialized must be rejected by the injection platform and investigated.
- Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices must be identified and accounted for against the inventory.

**Note:** *The KIF platform must ensure that only authorized devices can ever be injected or initialized with authorized keys. Processes must prevent (1) substitution of an authorized device with an unauthorized device, and (2) insertion of an unauthorized device into a production run.*

### **Requirement 31:** Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.

*Key-injection facilities must have procedures to ensure keys are destroyed in cryptographic devices removed from service. This applies to any SCDs (e.g., HSM) used in the key-injection platform, as well as to any devices that have been loaded with keys and securely stored or warehoused on site that are subsequently deemed to be unnecessary and never to be placed into service.*

*If a key-injection facility receives a used device to reload with keys, procedures shall ensure that old keys that may be in the device are destroyed prior to loading of new keys. (The used device should have had its keys destroyed when it was removed from service, but this is a prudent secondary check that the keys were destroyed.)*

**31-1** Procedures are in place to ensure that any SCDs to be removed from service—e.g., retired, or returned for repair—are not intercepted or used in an unauthorized manner, including that all keys and key material stored within the device must be rendered irrecoverable.

Processes must include the following:

**Note:** *Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the Master File Key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*

**31-1.1** HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.

**31-1.2** Keys are rendered irrecoverable (for example, zeroized) for SCDs. If data cannot be rendered irrecoverable, devices must be physically destroyed prior to leaving the dual-control area to prevent the disclosure of any sensitive data or keys.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**31-1.3** SCDs being decommissioned are tested and inspected to ensure keys have been rendered irrecoverable.

**31-1.4** Affected entities are notified before devices are returned.

**31-1.5** Devices are tracked during the return process.

**31-1.6** Records of the tests and inspections maintained for at least one year.

**Requirement 32:** Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following:

- a. Dual access controls required to enable the key-encryption function
- b. Physical protection of the equipment (e.g., locked access to it) under dual control
- c. Restriction of logical access to the equipment

*Key-injection facilities must ensure protection against unauthorized use for SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.*

**32-1** For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, procedures must be documented and implemented to protect against unauthorized access and use.

Required procedures and processes include the following:

**32-1.1** Devices must not be authorized for use except under the dual control of at least two authorized people.

**Note:** Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords at least five characters in length, or for physical access via a physical lock that requires two individuals, each with a different high-security key.

*For devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.*

*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.*

**32-1.2** Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.

**32-1.3** Dual control must be implemented for the following:

- To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing;
- To place the device into a state that allows for the input or output of clear-text key components;
- For all access to key-loading devices (KLDs)

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**32-1.4** Devices must not use default passwords.

**32-1.5** To detect any unauthorized use, devices are at all times within a secure room and either:

- Locked in a secure cabinet and/or sealed in tamper-evident packaging, or
- Under the continuous supervision of at least two authorized people who ensure that any unauthorized use of the device would be detected.

**Note:** POI devices may be secured by storage in the dual-control access key injection room.

*Functionality of a key-injection facility may be located at a single physical location or distributed over a number of physical locations. Distributed KIF functionality may include key generation, CA functionality, key distribution and key injection. In order to mitigate the expanded attack surface of a distributed KIF, specific controls apply to a distributed architecture. If any secret or private keys or their components/shares appear in the clear outside of a SCD, Requirement 32-10 for a secure room must be met.*

**32-9** Distributed functionality of the KIF that is used for generation and transfer of keys must communicate via mutually authenticated channels. All key transfers between distributed KIF functions must meet the requirements of Control Objective 3.

**32-9.1** The KIF must ensure that keys are transmitted between KIF components in accordance with Control Objective 3.

**32-9.2** The KIF must implement mutually authenticated channels for communication between distributed KIF functions—for example, between a host used to generate keys and a host used to distribute keys.

**32-9.3** The KIF must ensure that injection of enciphered secret or private keys into POI devices meets the requirements of Control Objective 4.

**32-9.4** The channel for mutual authentication is established using the requirements of Control Objective 4.

**32-9.5** The KIF must implement a mutually authenticated channel for establishment of enciphered secret or private keys between POI devices and an HSM at the KIF.

**32-9.6** Mutual authentication of the sending and receiving devices must be performed.

- KIFs must validate authentication credentials of a POI prior to any key transport, exchange, or establishment with that device.
- POI devices must validate authentication credentials of KDHS prior to any key transport, exchange, or establishment with that device.
- When a KLD is used as an intermediate device to establish keys between POIs and a KIF HSM it must not be possible to insert an unauthorized SCD into the flow without detection.

**32-9.7** Mechanisms must exist to prevent a non-authorized host from injecting keys into POIs or an unauthorized POI from establishing a key with a legitimate KIF component.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**32-10** The KIF must implement a physically secure area (secure room) for key injection where any secret or private keys or their components/shares appear in the clear outside of an SCD.

The secure room for key injection must include the following:

**32-10.1** The secure area must have walls made of solid materials. In addition, if the solid walls do not extend from the real floor to the real ceiling, the secure area must have extended walls from the real floor to the real ceiling using sheetrock or wire mesh.

**32-10.2** Any windows into the secure room must be locked and protected by alarmed sensors.

**32-10.3** Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.

**32-10.4** A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.

**32-10.5** An electronic access control system (for example, badge and/or biometrics) must be in place that enforces:

- Dual-access requirements for entry into the secure area, and
- Anti-pass-back requirements.

**32-10.6** The badge-control system must support generation of an alarm when one person remains alone in the secure area for more than 30 seconds.

**Note:** Examples of alarm-generation mechanisms include but are not limited to motion detectors, login/logout controls, biometrics, badge sensors, etc.

**32-10.7** CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be motion-activated. The recording must continue for at least a minute after the last pixel of activity subsides.

**32-10.8** Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.

**32-10.9** The CCTV server and digital storage must be secured in a separate secure area that is not accessible to personnel who have access to the key-injection area.

**32-10.10** The CCTV cameras must be positioned to monitor:

- The entrance door,
- SCDs, both pre and post key injection,
- Any safes that are present, and
- The equipment used for key injection.

**32-10.11** CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials.

**Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.**

**Requirement 33:** Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., POI devices supporting PIN and HSMS) placed into service, initialized, deployed, used, and decommissioned.

**33-1** Written procedures must exist, and all affected parties must be aware of those procedures. Records must be maintained of the tests and inspections performed by key-injection facilities on PIN-processing devices before they are placed into service, as well as devices being decommissioned.

---

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

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange, or establishment and for data protection:<sup>2</sup>

Algorithm	DES	RSA	Elliptic Curve	DSA	AES
Minimum key size in number of bits:	112	1024	224	2048/224	128

The strength of a cryptographic key is a measure of the expected work effort an attacker would have to spend to discover the key. Cryptographic strength is measured in "bits of security" (see, e.g., *NIST SP 800-57 Part 1*). While the concept of bits of security originated with symmetric encryption algorithms, it extends to asymmetric algorithms as well. In neither case do the bits of security necessarily equal the length of the key.

The following table, which is consistent with *NIST SP 800-57 Part 1*, Table 2, and with *ISO TR-14742*, lists the cryptographic strength of the most common key lengths for the relevant symmetric and asymmetric cryptographic algorithms. The RSA key size below 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.

Bits of security	Symmetric encryption algorithms	RSA	Elliptic Curve	DSA/D-H
80	Double-length TDES <sup>(§)</sup>	1024	160	1024/160
112	Double-length TDEA <sup>(§)</sup> Triple-length TDEA	2048	224	2048/224
128	AES-128	3072	256	3072/256
192	AES-192	7680	384	7680/384
256	AES-256	15360	512	15360/512

(§): The bit-strength of a double-length TDEA key depends on the availability to a potential attacker of pairs of plaintext and corresponding ciphertext enciphered with the key. A double-length TDEA key may only be assessed to have 112 bits of security if very few (less than 500) pairs

<sup>2</sup> The requirement for longer DH, ECDH, ECC and DSA keys reflects an industry transition to longer key lengths (see *NIST SP800-131A*) without any requirement for legacy support.

of 8-byte blocks of plaintext and corresponding ciphertext could possibly become available to an attacker. One example is when double-length TDEA is used with session keys such as in DUKPT, and each session encrypts less than 4 kilobytes of data.

In general, the weakest algorithm and key size used to provide cryptographic protection determines the strength of the protection. For example, if a 2048-bit RSA key is used to encipher an AES-128 key, henceforth that AES key will only have 112-bit strength, not 128-bit. Intuitively this is because once you break the key encryption key, you have access to the encrypted key. The strength hence reflects the expected amount of effort an attacker needs to spend in order to discover the key.

This applies to any key-encipherment keys used for the protection of secret or private keys that are stored, or for keys used to encrypt any secret or private keys for loading or transport.

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

For implementations using Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH):

1. **DH implementations** – Entities must securely generate and distribute the system-wide parameters: generator  $g$ , prime number  $p$  and parameter  $q$ , the large prime factor of  $(p - 1)$ . Parameter  $p$  must be at least 2048 bits long, and parameter  $q$  must be at least 224 bits long. Each entity shall generate a private key  $x$  and a public key  $y$  using the domain parameters  $(p, q, g)$ .
2. **ECDH implementations** – Entities must securely generate and distribute the system-wide parameters. Entities may generate the elliptic curve domain parameters or use a recommended curve (See *FIPS186-4*). The elliptic curve specified by the domain parameters must be at least as secure as P-224. Each entity shall generate a private key  $d$  and a public key  $Q$  using the specified elliptic curve domain parameters. (See *FIPS186-4* for methods of generating  $d$  and  $Q$ ).
3. Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
4. Entities must authenticate the DH or ECDH public keys using DSA, ECDSA, a certificate, or a symmetric MAC (see *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques*). One of the following: MAC algorithm 1 using padding method 3, MAC algorithm 5 using padding method 4 should be used.

## Glossary

Term	Definition
<b>Access controls</b>	Controls to ensure that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
<b>Acquirer</b>	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.
<b>Advanced Encryption Algorithm (AES)</b>	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
<b>Algorithm</b>	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
<b>ANSI</b>	American National Standards Institute, a U.S. standards accreditation organization.
<b>Asymmetric cryptography (techniques)</b>	See <i>Public-key cryptography</i> .
<b>ATM</b>	Automated teller machine. An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks.
<b>Authentication</b>	The process for establishing unambiguously the identity of an entity, process, organization or person.
<b>Authorization</b>	The right granted to a user to access an object, resource or function.
<b>Authorize</b>	To permit or give authority to a user to communicate with or make use of an object, resource or function.
<b>Authorized key custodian</b>	Having a signed key-custodian agreement and a written authorization for the specific operation.
<b>Base (master) Derivation Key (BDK)</b>	See <i>Derivation key</i> .
<b>Cardholder</b>	An individual to whom a card is issued or who is authorized to use the card.
<b>Card issuer</b>	The institution or its agent that issues the payment card to the cardholder.
<b>Certificate</b>	For purposes of these requirements, a certificate is any digitally signed value containing a public key.

Term	Definition
<b>Certificate revocation</b>	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.
<b>Certificate Revocation List (CRL)</b>	A list of revoked certificates. Entities that generate, maintain, and distribute CRLs can include, for example, the root or subordinate CAs.
<b>Certification authority (CA)</b>	For purposes of these requirements, a certification authority is any entity signing public keys, whether in X.509 certificate based schemes or other designs for use in connection with the remote distribution of symmetric keys using asymmetric techniques.
<b>Check value</b>	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key must not be feasible.
<b>Cipher text</b>	Data in its enciphered form.
<b>Clear text</b>	See <i>Plaintext</i> .
<b>Communicating nodes</b>	Two entities (usually institutions) sending and receiving transactions. This is to include alternate processing sites either owned or contracted by either communicating entity.
<b>Compromise</b>	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).
<b>Computationally infeasible</b>	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it.
<b>Credentials</b>	Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key.
<b>Critical security parameters (CSP)</b>	Security-related information (e.g., cryptographic keys or 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.
<b>Cryptographic boundary</b>	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.

Term	Definition
<b>Cryptographic key</b>	<p>A parameter used in conjunction with a cryptographic algorithm that determines:</p> <ul style="list-style-type: none"> <li>• The transformation of plaintext data into ciphertext data,</li> <li>• The transformation of ciphertext data into plaintext data,</li> <li>• A digital signature computed from data,</li> <li>• The verification of a digital signature computed from data,</li> <li>• An authentication code computed from data, or</li> <li>• An exchange agreement of a shared secret.</li> </ul>
<b>Cryptographic key component</b>	<p>One of at least two parameters having the characteristics (for example, format, randomness) of a cryptographic key that is combined with one or more like parameters, for example, by means of modulo-2 addition, to form a cryptographic key. Throughout this document, key component may be used interchangeably with secret share or key fragment.</p>
<b>Customers</b>	<p>Customers are financial institutions that:</p> <ul style="list-style-type: none"> <li>• Offer payment cards for one or more of the participating payment brands (issuers);</li> <li>• Accept such payment cards for cash disbursement and directly or indirectly enter the resulting transaction receipt into interchange (acquirers); or</li> <li>• Offer financial services to merchants or authorized third parties who accept such payment cards for merchandise, services, or cash disbursement, and directly or indirectly enter the resulting transaction receipt into interchange (acquirers).</li> </ul>
<b>Data Encryption Algorithm (DEA)</b>	<p>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.</p>
<b>Decipher</b>	<p>See <i>Decrypt</i>.</p>
<b>Decrypt</b>	<p>A process of transforming cipher text (unreadable) into plain text (readable).</p>

Term	Definition
<b>Derivation key</b>	<p>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.</p> <p>Derivation keys are normally used in a transaction-receiving (e.g., acquirer) SCD in a one-to-many relationship to derive or decrypt the transaction keys (the derived keys) used by a large number of originating (e.g., terminals) SCDs.</p>
<b>DES</b>	<p>Data Encryption Standard (see <i>Data Encryption Algorithm</i>). 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.</p>
<b>Digital signature</b>	<p>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.</p>
<b>Double-length key</b>	<p>A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDEA cryptographic algorithm.</p>
<b>Dual control</b>	<p>A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities.</p> <p>No single person can gain control of a protected item or process.</p> <p>Also see <i>Split knowledge</i>.</p>
<b>DUKPT (Derived Unique Key Per Transaction)</b>	<p>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.</p>
<b>ECB</b>	<p>Electronic codebook.</p>
<b>Electronic code book (ECB) operation</b>	<p>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.</p>
<b>EEPROM</b>	<p>Electronically erasable programmable read-only memory.</p>
<b>Electronic key entry</b>	<p>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.</p>

Term	Definition
<b>Encipher</b>	See <i>Encrypt</i> .
<b>Encrypt</b>	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.
<b>Encrypting PIN pad (EPP)</b>	<p>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.</p> <p>Encrypting PIN pads require integration into UPTs or ATMs.</p>
<b>EPROM</b>	Erasable programmable read-only memory.
<b>Exclusive-OR</b>	<p>Binary addition without carry, also known as “modulo 2 addition,” symbolized as “XOR” and defined as:</p> <ul style="list-style-type: none"> <li>• <math>0 + 0 = 0</math></li> <li>• <math>0 + 1 = 1</math></li> <li>• <math>1 + 0 = 1</math></li> <li>• <math>1 + 1 = 0</math></li> </ul>
<b>FIPS</b>	Federal Information Processing Standard.
<b>Firmware</b>	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.
<b>Hardware (host) security module</b>	An SCD that provides a set of secure cryptographic services, including but not limited to key generation, cryptogram creation, PIN translation and certificate signing

Term	Definition
<b>Hash</b>	<p>A (mathematical) function that is a non-secret algorithm, which takes any arbitrary-length message as input and produces a fixed-length hash result.</p> <p>Approved hash functions satisfy the following properties:</p> <ol style="list-style-type: none"> <li>1) One-Way – It is computationally infeasible to find any input that maps to any pre-specified output.</li> <li>2) Collision Resistant – It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output.</li> </ol> <p>It may be used to reduce a potentially long message into a “hash value” or “message digest” that 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.</p>
<b>Hexadecimal character</b>	A single character in the range 0–9, A-F (upper case), representing a four-bit string.
<b>Initialization vector</b>	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.
<b>Integrity</b>	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
<b>Interchange</b>	The exchange of clearing records between financial institution customers.
<b>Interface</b>	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.
<b>Irreversible transformation</b>	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.
<b>ISO</b>	International Organization for Standardization. An international standards setting organization composed of representatives from various national standards organizations.
<b>Issuer</b>	The institution holding the account identified by the primary account number (PAN).
<b>Key</b>	See <i>Cryptographic key</i> .
<b>Key agreement</b>	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.

Term	Definition
<b>Key backup</b>	Storage of a protected copy of a key during its operational use.
<b>Key bundle</b>	The three cryptographic keys (K1, K2, K3) used with a TDEA mode. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle must never be used separately for any other purpose.
<b>Key component</b>	See <i>Cryptographic key component</i> .
<b>Key derivation process</b>	A process, which derives one or more session keys from a shared secret and (possibly) other public information.
<b>Key destruction</b>	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.
<b>Key-distribution host (KDH)</b>	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.
<b>Key-encrypting (encipherment or exchange) key</b>	A cryptographic key that is used for the encryption or decryption of other keys.
<b>Key establishment</b>	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
<b>Key generation</b>	Creation of a new key for subsequent use.
<b>Key instance</b>	The occurrence of a key in one of its permissible forms, i.e., plaintext key, key components, enciphered key.
<b>Key-loading</b>	Process by which a key is manually or electronically transferred into a secure cryptographic device.
<b>Key-loading device (KLD)</b>	An SCD that may be used to perform cryptographic injection/loading or code signing.
<b>Key management</b>	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.
<b>Key pair</b>	A key pair comprises the two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is known only to the appropriate entities.

Term	Definition
<b>Key replacement</b>	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.
<b>Key (secret) share</b>	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.
<b>Key storage</b>	Holding of the key in one of the permissible forms.
<b>Key transport</b>	A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
<b>Key usage</b>	Employment of a key for the cryptographic purpose for which it was intended.
<b>Key variant</b>	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.
<b>Keying material</b>	The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships.
<b>Local Master Key (LMK)</b>	See <i>Master File Key</i> .
<b>Manual key-loading</b>	The entry of cryptographic keys into a secure cryptographic device from a printed form, using devices such as buttons, thumb wheels, or a keyboard.
<b>Master derivation key (MDK)</b>	See <i>Derivation key</i> .
<b>Master File Key (MFK)</b>	This is a symmetric key used to encrypt other cryptographic keys which are to be stored outside of the Hardware Security Module (HSM).
<b>Master key</b>	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a master key. This may be further defined as a Master File Key used at a host or a terminal master key for use at a terminal, e.g., a PED.
<b>Message</b>	A communication containing one or more transactions or related information.
<b>Node</b>	Any point in a network that does some form of data processing, such as a terminal, acquirer, or switch.
<b>Non-reversible transformation</b>	See <i>Irreversible transformation</i> .

Term	Definition
<b>Online Certificate Status Protocol (OCSP)</b>	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.
<b>Offline PIN verification</b>	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.
<b>Online PIN verification</b>	A process used to verify the cardholder's identity by sending an encrypted PIN value to the issuer for validation in an authorization request.
<b>Out-of-band notification</b>	Notification using a communication means independent of the primary communications means.
<b>PAN</b>	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
<b>Password</b>	A string of characters used to authenticate an identity or to verify access authorization.
<b>Personal identification number (PIN)</b>	A numeric personal identification code that authenticates a cardholder in an authorization request originating at a terminal with authorization-only or data-capture-only capability. A PIN consists only of decimal digits.
<b>Physical protection</b>	The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.
<b>Physically secure environment</b>	An environment equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or purpose-built room with continuous access control, physical security protection, and monitoring.
<b>PIN</b>	See <i>Personal identification number</i> .
<b>PIN-encipherment key (PEK)</b>	A PEK is a cryptographic key that is used for the encryption or decryption of PINs.
<b>PIN entry device (PED)</b>	A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor, and storage for PIN processing sufficiently secure for the key-management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell and is a complete terminal that can be provided to a merchant "as is" to undertake PIN-related transactions. This may include either attended or unattended POS POI terminals.

Term	Definition
<b>PIN pad</b>	See <i>PIN entry device</i> .
<b>Plain text</b>	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as clear text.
<b>Plaintext key</b>	An unencrypted cryptographic key, which is used in its current form.
<b>Point of interaction (POI)</b>	An electronic-transaction-acceptance product. A POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. Thereby the POI may be attended or unattended. POI transactions include IC, magnetic-stripe, and contactless payment-card-based payment transactions.
<b>Private key</b>	<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>
<b>PROM</b>	Programmable read-only memory.
<b>Pseudo-random</b>	A value that is statistically random and essentially random and unpredictable although generated by an algorithm.
<b>Public key</b>	<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>

Term	Definition
<b>Public key (asymmetric) cryptography</b>	<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 exist asymmetric cryptosystems (e.g., RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation, and where used, the four elementary transformations and the corresponding keys should be kept separate.</p>
<b>Random</b>	<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>
<b>Registration authority (RA)</b>	<p>An entity that performs registration services on behalf of a certification authority (CA). Registration authorities (RAs) work with a particular certification authority (CA) to vet requests for certificates that will then be issued by the certification authority.</p>
<b>ROM</b>	<p>Read-only memory.</p>
<b>Root certification authority (RCA)</b>	<p>The RCA is the top-level certification authority in a public key infrastructure. An RCA is a CA that 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>
<b>Secret key</b>	<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>
<b>Secure cryptographic device (SCD)</b>	<p>A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms.</p>

Term	Definition
<b>Sensitive data</b>	Data that must be protected against unauthorized disclosure, alteration, or destruction, especially plaintext PINs and cryptographic keys, and includes design characteristics, status information, and so forth.
<b>Session key</b>	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.
<b>Shared secret</b>	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.
<b>Single-length key</b>	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DEA cryptographic algorithm.
<b>Software</b>	The programs and associated data that can be dynamically written and modified.
<b>Split knowledge</b>	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. The information needed to perform a process such as key formation is split among two or more people. No individual has enough information to gain knowledge of any part of the actual key that is formed.
<b>Subordinate CA and Superior CA</b>	If one CA issues a certificate for another CA, the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, EPPs or PEDs. Subordinate CAs may also issue certificates to lower-level CAs and issue certificate status lists regarding certificates the subordinate CA has issued.
<b>Symmetric (secret) key</b>	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
<b>System software</b>	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.
<b>Switch</b>	A node that can route data from a node to other nodes.
<b>Tamper detection</b>	The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.
<b>Tamper-evident</b>	A characteristic that provides evidence that an attack has been attempted.
<b>Tamper-resistant</b>	A characteristic that provides passive physical protection against an attack.

Term	Definition
<b>Tamper-responsive</b>	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
<b>Tampering</b>	The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data.
<b>TDEA</b>	See <i>Triple Data Encryption Algorithm</i> .
<b>TECB</b>	TDEA electronic code book.
<b>Terminal</b>	A device/system that initiates a transaction.
<b>Terminal Master Key (TMK)</b>	This is a symmetric key used to encrypt other cryptographic keys at the point of interaction.
<b>Transaction</b>	A series of messages to perform a predefined function.
<b>Triple Data Encryption Algorithm (TDEA)</b>	An algorithm specified in <i>ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers</i> .
<b>Triple Data Encryption Standard (TDES)</b>	See <i>Triple Data Encryption Algorithm</i> .
<b>Triple-length key</b>	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDEA cryptographic algorithm.
<b>Trustworthy system</b>	<p>A combination of computer hardware and software that:</p> <ul style="list-style-type: none"> <li>• Are reasonably secure from intrusion and misuse;</li> <li>• Provide a reasonable level of availability, reliability, and correct operation; and</li> <li>• Are reasonably suited to performing their intended functions.</li> </ul>
<b>Two-factor authentication</b>	Two-factor authentication (“TFA” or “2FA”) is a system wherein two different factors are used in conjunction for authentication. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three methods: "something you know" (e.g., password or PIN), "something you have" (e.g., smartcard or token), or "something you are" (e.g., fingerprint or iris scan).

Term	Definition
<b>Unattended acceptance terminal (UAT)</b>	<p>A cardholder-operated device that reads, captures, and transmits card information in an unattended environment including, but not limited to, the following:</p> <ul style="list-style-type: none"> <li>• ATM</li> <li>• Automated Fuel Dispenser</li> <li>• Ticketing Machine</li> <li>• Vending Machine</li> </ul>
<b>Unattended payment terminal (UPT)</b>	<p>A POS POI device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as:</p> <ul style="list-style-type: none"> <li>• Automated fuel dispensers</li> <li>• Kiosks</li> <li>• Self-service devices—ticketing/vending or car parking terminals.</li> </ul>
<b>Unprotected memory</b>	<p>Data retained within components, devices, and recording media that reside outside the cryptographic boundary of a secure cryptographic device.</p>
<b>Variant of a key</b>	<p>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.</p>
<b>Verification</b>	<p>The process of associating and/or checking a unique characteristic.</p>
<b>Working key</b>	<p>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.</p>
<b>XOR</b>	<p>See <i>Exclusive-Or</i>.</p>
<b>Zeroize</b>	<p>The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.</p>
<b>Zone master key</b>	<p>See <i>Key-encrypting key</i>.</p>