Payment Card Industry (PCI)

PIN Security

Requirements and Testing Procedures

Version 2.0

December 2014

Document Changes

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

Table of Contents

Overview

This document contains a complete set of requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals. These PIN Security Requirements are based on the industry standards referenced in the "PIN Security Requirements – Technical Reference" section 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.pcisecuritystadandards.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-DEA (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	*ANSI X3.92: Data Encryption Algorithm*
	ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
	ANSI X9.24 (Part 2): Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
	ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
	ANSI X9.44: Key Establishment Using Integer Factorization Cryptography
	ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA
	ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
	ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
EMV	***EMV:** Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management*

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

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

PIN Security Requirements	Testing Procedures
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 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.) *(continued on next page)*	**1-1** Procedures applicable to POI devices (PCI PTS standards): **1-1.a** Obtain the POI Device Inventory. Check for the correct population of the fields **1-1.b** Compare the inventory against the list of approved PTS devices at www.pcisecuritystandards.org to determine which POI devices used are PCI approved and are listed, with a valid PCI approval number on the PCI SSC website. **1-1.c** For devices in the inventory identified as PCI approved, verify that all of the following POI device characteristics in the inventory listing match the PCI PTS listing. • Vendor name • Model name/number • Hardware version number • Firmware version number • Name and application version number of any applications resident within the device that were included in the PTS assessment

Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	
PIN Security Requirements	**Testing Procedures**
• 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	**1-1.d** For a sample of the PCI-approved devices, verify that the device displays the firmware version and either displays or has a label with the hardware version number. ***Note:*** *PCI-approved devices must show the version numbers of hardware and firmware like they have been approved and they are shown in the list of approved devices. The hardware number must be shown on a label attached to the device. The firmware and application version numbers, and optionally the hardware version number, must be shown on the display or printed during startup or on request. This includes all modules addressed in testing, including SRED and Open Protocols.* *For unattended devices, the focal point is the PIN-entry vehicle.*
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.	**1-3.a** For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3, or higher. Refer http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.
	1-3.b Examine documented procedures and interview personnel to verify that all decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified above.

Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	
PIN Security Requirements	**Testing Procedures**
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.	**1-4.a** For all PCI-approved HSMs used, examine HSM devices and review the *PCI SSC List of Approved PCI PTS Devices* to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • Any applications, including application version number, resident within the device which were included in the PTS assessment
	1-4.b For all FIPS-approved HSMs used, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number
Requirement 2a: *Cardholder PINs shall be processed in accordance with approved standards.* *a. All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys.* *b. All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the* EMV IC Card Specifications for Payment Systems *and ISO 9654.*	
2-1 No procedure shall require or permit the cardholder to disclose the PIN in an oral or written manner.	**2-1** Interview responsible personnel to determine that no procedures require or permit the cardholder to disclose their PIN in an oral or written manner.

Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	
PIN Security Requirements	**Testing Procedures**
2-2 Online PIN translation must only occur using one of the allowed key-management methods: DUKPT, fixed key, master key/session key.	**2-2.a** Interview responsible personnel to determine key-management methods used for online PIN acquisition.
	2-2.b Review system documentation to determine key-management methods used within each zone—e.g., terminal to host, host to next node, etc.
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 [1] For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in ISO 18033-3.	**2-3.a** Interview responsible personnel to determine encryption algorithms utilized in connection with "not-on-us" acquisitions of PIN blocks.
	2-3.b Examine system documentation to verify information provided during the aforementioned interviews: • For internally developed systems, review system design documentation or source code for type of key (algorithm) and key sizes used to encrypt the PIN blocks. Examine the point in the code where the calls are made to the hardware security module. • For application packages, examine parameter files (e.g., the Base24 KEYF file) to determine type of key (algorithm) and key sizes used to encrypt PIN blocks.
	2-3.c Examine the HSM configuration to ensure that the PIN translation encryption algorithms are only TDEA and/or AES.
	2-3.d Examine the algorithm type parameter (to ensure it denotes TDEA and/or AES) and hardware-encryption-required parameter (to ensure it indicates hardware encryption—not software encryption) on every terminal link, network link, and if applicable, internal path (i.e., if using an intermediate key) for the host application.

[1] 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.

PIN Security Requirements	Testing Procedures
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**.	**2-4.a** Interview the responsible personnel to determine which POI devices identified in Requirement 1 are used for offline PIN acquiring.
	2-4.b Validate that the POI devices used for offline PIN, including both the ICCR and the PED, where non-integrated, are approved for "Offline PIN" on the PTS Approved Devices Listing at www.pcisecuritystandards.org

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 **ISO 9564** 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 **ISO 9564**.

Control Objective 1:	***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***	
PIN Security Requirements		**Testing Procedures**
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.		**3-1.a** Interview responsible personnel to determine the PIN-block format(s) utilized for "not-on-us" traffic from point of acquisition through routing of the transaction to another entity. Develop or obtain a network schematic to illustrate.
		3-1.b Examine system documentation to verify information provided during interviews. This is mandatory, especially if personnel have indicated the use of a compliant PIN-block format: • For internally developed systems, review system design documentation or source code for type of PIN-block format(s) used. • For application packages, examine parameter files where the PIN-block format is specified (e.g., the KEYF file for Base 24). Verify the format is ISO Formats 0, 1, 3, or 4 as the online PIN-block type for compliance.
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.		**3-2.a** For any non-PCI-approved devices identified in Requirement 1, and for which the ICC card reader is not integrated in the PIN entry device, Interview applicable personnel to determine that PINs enciphered only for transmission between the PIN entry device and the ICCR use one of the PIN-block formats specified in ISO 9564. If format 2 is used, verify that a unique-key-per-transaction method in accordance with ISO 11568 is used.
		3-2.b Review device documentation to validate that the device functions as described above. ***Note:*** *PCI-approved devices are validated to this; nevertheless, personnel must still be interviewed to validate the implementation.*

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

PIN Security Requirements	Testing Procedures
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.*	**3-3.a** Verify the following, using information obtained in the prior step: • ISO PIN-block formats are not translated into non-ISO formats. • ISO PIN-block formats 0, 3, and 4 are not translated into any PIN-block formats other than 0, 3, or 4 except for submission to an IC payment card. • If ISO format 1 is translated to ISO format 0, 3, or 4, it is not translated back to ISO format 1. • ISO format 1 is only translated to ISO format 2 for submission to an IC payment card. • PIN-block translations from ISO format 0, 3, or 4 to any of ISO format 0, 3, or 4 do not support a change in PAN.
	3-3.b The PIN block shall be submitted to the IC enciphered using an authenticated encipherment key of the IC.

Translation

To → / From ↓	**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

Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.	
PIN Security Requirements	**Testing Procedures**
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*.	**4-1** Interview appropriate personnel to determine whether PINs are stored or retained for some period of time as part of a store-and-forward environment. Based upon that, perform the following steps as necessary: • Examine transaction journals/logs to determine the presence of PIN blocks. If present, PIN blocks—whether enciphered or not—must be masked before the record is logged. For environments using online transaction monitors (e.g., CICS), specifically note how management is ensuring that PINs are not stored in online transaction journals. • For entities that drive POS devices, examine documentation (operating procedures) to verify the disposition of PIN blocks when communication links are down.

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.***

PIN Security Requirements	Testing Procedures
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.*	**5-1.a** Examine key-management policy document and to verify that it requires that all devices used to generate cryptographic keys meet one of the following: • An approved key-generation function of a PCI–approved HSM • 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 qualified laboratory according to *NIST SP 800-22.*
	5-1.b Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: • An approved key-generation function of a PCI-approved HSM • 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 qualified laboratory according to *NIST SP 800-22.*
	5-1.c Verify devices used for key generation are those as noted above, including validation of the firmware used.

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.***

PIN Security Requirements	Testing Procedures
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** Perform the following:
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.	**6-1.1.a** Examine documented procedures to verify the following. • Any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.
	6-1.1.b Observe key-generation processes and interview responsible personnel to verify: • Any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key. • There is no mechanism including connectivity that might disclose a clear-text key or key component between the key-generation device 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.*	**6-1.2.a** Observe the process from end-to-end to verify there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.
	6-1.2.b Examine key-generation logs to verify that at least two individuals performed the key-generation processes.

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.

PIN Security Requirements	Testing Procedures
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.	**6-1.3** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate clear-text key components are powered off when not in use; or • If logically partitioned for concurrent use in other processes, the key-generation capabilities are 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).	**6-1.4.a** Review documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering, prior to use.
	6-1.4.b Observe key-generation set-up processes for all key types to verify that key-generation equipment is inspected prior to use, to ensure equipment does not show any signs of tampering.
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.	**6-1.5.a** Examine documentation to verify that physical security controls are defined to ensure the key component/key-generation process cannot be observed or accessed by unauthorized personnel.
	6-1.5.b Observe the physical security controls to verify that key-component/key-generation process cannot be observed or accessed by unauthorized personnel.
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.*	**6-2.a** Examine documented procedures to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.
	6-2.b Observe generation process and review vendor documentation for each type of key to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.

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.

PIN Security Requirements	Testing Procedures
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.*	**6-2.c** Where single-purpose computers with an installed SCD are used, verify that either: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device), or • Where clear keying material passes through unprotected memory of the PC, the PC requirements of Requirement 13 of Annex B are met
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.	**6-3.a** Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed immediately after printing such that: • Only approved key custodians can observe their own key component. • Tampering can be detected.
	6-3.b Observe processes for printing key components to verify that key components are printed within blind mailers or sealed immediately after printing, such that no one but the authorized custodian ever has physical access to the output.
	6-3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be detected.
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*	**6-4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures are implemented to ensure the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.

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.***

PIN Security Requirements	Testing Procedures
	6-4.b Observe the destruction process of the identified key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.
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.	**6-5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (zeroized) immediately after the transfer to the device that will use the key pair
	6-5.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (for example, zeroized) immediately after the transfer to the device that will use the key pair.

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.

PIN Security Requirements	Testing Procedures
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	**6-6.a** Examine documented policy and procedures to verify that key components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual
	6-6.b From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual

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.***
PIN Security Requirements	**Testing Procedures**
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.	**7-1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations.
	7-1.b Interview those responsible for the key-generation processes (including key custodians, supervisory staff, technical management, etc.) to verify that the documented procedures are known and understood by all affected parties.
	7-1.c Observe key-generation ceremonies, whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.
7-2 Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs.	**7-2.a** Examine documented key-generation procedures to verify that all key-generation events for higher-level keys (e.g., KEKs shared with other organizations or otherwise manually loaded as components, and MFKs and BDKs) must be logged.
	7-2.b Observe demonstrations for the generation of higher-level keys to verify that all key-generation events are logged.
	7-2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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: o 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. o Ensure that details of the serial number of the package are conveyed separately from the package itself. o Ensure that documented procedures exist and are followed to require that the serial numbers be verified prior to the usage of the keying material. *(continued on next page)*	**8-1.a** Determine whether keys are transmitted encrypted, as clear-text components, or within an SCD. **8-1.b** If key components are ever transmitted in clear-text using pre-numbered tamper-evident mailers, perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using pre-numbered tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. • Examine documented procedures to verify that cryptographic-key components are conveyed using different communications channels. • Examine records of key conveyances and interview responsible personnel to verify that cryptographic key components are conveyed using different communications channels. • Examine documented procedures to verify that serial numbers are verified prior to the usage of the keying material.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
8-1 *(continued)* • 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.	**8-1.c** Where an SCD is used, perform the following: • Examine documented procedures to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels. • Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering. • Examine records of key transfers and interview responsible personnel to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels.
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.*	**8-2.a** Examine documented procedures to verify they include controls to ensure that no single person can ever have access to 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. Verify procedures include: • Any person with access to one component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component or shares sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component of this key that is sufficient to form the necessary threshold to derive the key.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	8-2.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can ever have access to 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. Verify the implemented controls ensure the following: • An individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a key component or key share must not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key.
	8-2.c Examine documented procedures and interview responsible personnel to verify that the method used does not allow for any personnel to have access to all components.
	8-2.d Observe the method used to transport key components to verify that the method does not allow for any personnel to have access to all components.
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.	**8-3** Validate through interviews, observation, and logs that e-mail, SMS, fax, telephone, or similar communication is not used as means to convey secret or private keys or key components.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**8-4** For all methods used to convey public keys, perform the following:
	8-4.a Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity such as: • Use of public-key certificates 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
	8-4.a Validate that self-signed certificates must not be used as the sole method of authentication.
	8-4.a Observe the process for conveying public keys and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**9-1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text key component 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, or • Contained within a physically secure SCD.
	9-1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text key component is at all times either: • Under the continuous supervision of a person with authorized access to this component, or • 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, or • Contained within a physically secure SCD.
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	**9-2.a** Verify documented procedures include requirements for all packaging or mailers containing clear-text key components to be examined for evidence of tampering before being opened.
	9-2.b Interview responsible personnel and observe processes to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being opened.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	9-2.c Verify documented procedures require that any sign of package tampering results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
	9-2.d Interview responsible personnel and observe processes to verify that, if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: • 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.	**9-3.a** Verify that a list(s) of key custodians (and designated backup(s)) authorized to have physical access to key components prior to transmittal or upon receipt of a component is defined and documented.
	9-3.b Observe implemented access controls and processes to verify that only those authorized key custodians (and designated backup(s)) have physical access to key components prior to transmittal or upon receipt.
	9-3.c Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each 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.	**9-4.a** Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packing upon receipt of a component package.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	9-4.b Observe implemented mechanisms and processes to verify that only the authorized key custodians can perform the following: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • 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*	**9-5.c** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.
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. *(continued on following page)*	**10-1.a** Examine documented procedures to verify that all keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
10-1 *(continued)* • 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.*	**10-1.b** Observe key-generation processes to verify that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed. • Interview appropriate personnel and examine documented procedures for the creation of these keys. • Using the table in Annex C, validate the minimum respective key sizes for DEA, RSA, Elliptic Curve, DSA, and Diffie Hellman algorithms where used for key encryption. • Verify that: o 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. o A double- or triple-length DEA key must not be encrypted with a DES key of lesser strength. o TDEA keys are not used to protect AES keys. o TDEA keys shall not be used to encrypt keys greater in strength than 112 bits. o RSA keys used to transmit or convey other keys have bit strength of at least 80 bits. o RSA keys encrypting keys greater in strength than 80 bits have bit strength at least 112 bits. o No key-exchange key is weaker than the cryptographic keys it protects and that it is at least double-length for a DEA key; and if RSA, that it uses a key modulus of at least 1024 bits. For example, verify that if RSA is used to convey triple-length DEA keys, it uses a key modulus of at least 2048 bits. o Any POI device that is version 3 or higher is using RSA with a key size of at least 2048 and SHA-2, where applicable, within 24 months of publication of these requirements. Use as necessary the device inventory used in Requirement 1.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	10-1.c Examine system documentation and configuration files to validate the above, including HSM settings.
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.	**11-1.a** Verify documented procedures exist for all key transmission and conveyance processing.
	11-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.
11-2 Methods used for the conveyance or receipt of keys must be documented.	**11-2** Verify documented procedures include all methods used for the conveyance or receipt of keys.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**12-1.a** Review documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.
	12-1.b Interview appropriate personnel to determine the number of key components for each manually loaded key, the length of the key components, and the methodology used to form the key.
	12-1.c Witness a structured walk-through/demonstration of various key-loading processes for all key types (MFKs, AWKs, TMKs, PEKs, etc. Verify the number and length of the key components to information provided through verbal discussion and written documentation.
	12-1.d Verify that the process includes the entry of individual key components by the designated key custodians.
	12-1.e Ensure key-loading devices can only be accessed and used under dual control.
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.	**12-2**. Examine logs of access to security containers for key components to verify that only the authorized custodian(s) have accessed. Compare the number on the current TEA bag for each component to the last log entry for that component.

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

PIN Security Requirements	Testing Procedures
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.*	**12-3.a** Examine documented procedures for loading of clear-text cryptographic keys, to verify they require dual control to authorize any key-loading session.
	12-3.b For all types of production SCDs, observe processes for loading clear-text cryptographic keys, to verify that dual control is required to authorize any key-loading session. Verify that any passwords used are a minimum of five characters.
	12-3.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.
	12-3.d Ensure that any default dual-control mechanisms (e.g., default passwords—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.
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.*	**12-4.a** Examine documented procedures for combining symmetric-key components and observe processes to verify that key components are combined using a process such that no active bit of the key can be determined without knowledge of the remaining components.
	12-4.b Examine key-component lengths or device configuration settings to verify that key components used to create a key are the same length as the resultant key.
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.	**12-5** Examine vendor documentation describing options for how the HSM MFK is created. Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.	**12-6** Through examination of documented procedures, interviews, and observation, confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**12-7.a** Examine documented procedures for the loading of TMKs to verify that they require asymmetric key-loading techniques or manual techniques for initial loading.
	12-7.b Examine documented procedures to verify that keys are prohibited from reloading or reuse wherever suspected of being compromised and are 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.	**12-8.a** For techniques involving public-key cryptography, examine documentation and develop a schematic to illustrate the process, including the size and sources of the parameters involved, and the mechanisms utilized for mutual device authentication for both the host and the POI.
	12-8.b If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that the remote key requirements detailed in Annex A of this document are met, including: • Use of 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 of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-1** Observe key-loading environments, processes, and mechanisms (for example, terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Ensure that any cameras present are positioned to ensure they cannot monitor the entering of clear-text key components • Review documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that: o SCDs must be inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. o An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are identified by the device. o There is not any mechanism (including cabling) at the interface between the conveyance medium and the SCD device that might disclose the transferred keys. o The SCD is inspected to ensure it has not been subject to any prior tampering, which could lead to the disclosure of clear-text keying material.
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.	**13-2** Verify that only SCDs are 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 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.	
PIN Security Requirements	**Testing Procedures**
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.	**13-3** Examine documented procedures for the loading of secret or private key components from an electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key loading, including: • Instructions for the medium to be 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 • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.
	13-3 Observe key-loading processes to verify that the loading process results in one of the following: • The medium used for key loading 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.
13-4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:	**13-4** Review documented procedures and observe processes for the use of key-loading devices. Perform the following:
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.	**13-4.1** Verify the key-loading device is 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.	**13-4.2** Verify the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-4.3.a** Verify the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD.
	13-4.3.b Verify that authorized personnel inspect the key-loading device prior to use to ensure that a key-recording device has not been 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.	**13-4.4** Verify the key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred. For example, attempt to output the same value more than one time from the device or cause the device to display check values for its contents both before and after injection and compare.
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.	**13-5.a** Interview personnel and observe media locations to verify that the media is maintained in a secure storage location accessible only to custodian(s) authorized to access the key components.
	13-5.b Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices be in the physical possession of only the designated component holder(s). • The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.
	13-5.c Interview designated component holder(s) and examine key-management logs to verify that media or devices removed from secure storage are in the physical possession of only the designated component holder(s).
	13-5.d Interview key-injection personnel and examine logs for the removal of media/devices from secure storage to verify they are removed only for the minimum practical time necessary to complete the key-loading process.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-6** Validate through interview and observation that printed key components are not opened until just prior to entry into the SCD/KLD. Plaintext secret and/or private keys and/or their components are visible only to key custodians for the duration of loading into an SCD/KLD.
13-7 Written or printed key-component documents must not be opened until immediately prior to use.	**13-7.a** Review documented procedures and confirm that printed/written key-component documents are not opened until immediately prior to use.
	13-7.b Observe key-loading processes and verify that printed/written key components are not 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.*	**13-8.a** Examine documented procedures for the use of key components to verify that procedures ensure that any individual custodian only has access to their assigned components and never has access to sufficient key components to reconstruct a cryptographic key.
	13-8.b Examine key-component access controls and access logs to verify that any single authorized custodian can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.
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.*	**14-1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords and associated hardware) used in the key-loading function must be controlled and managed such that no single individual has the capability to enable key loading of clear-text keys or their components.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	14-1.b Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function is controlled and maintained in a secure environment under dual control. • All resources (e.g., passwords and associated hardware) used for key-loading functions are controlled and managed such that no single individual has the capability to enable key loading.
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.	**14-2.a** Review documented procedures to ensure they require that cable attachments be examined prior to key-loading function.
	14-2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to a key-loading function.
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.	**14-3.a** Observe key-loading activities to verify that key-loading equipment usage is monitored.
	14-3.b Verify logs of all key-loading activities are maintained and contain all required information.
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.	**14-4.a** Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key. Verify procedures require that physical tokens 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.
	14-4.b Inspect locations and controls for physical tokens to verify that tokens used to enable key loading are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control.
	14-4.c Review storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.
	14-4.d Verify that access-control logs exist and are in use.
	14-4.e Reconcile storage contents to access-control logs.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**14-5.a** Verify that documented procedures require default passwords or PINs used to enforce dual control are changed.
	14-5.b Verify that documented procedures exist to require that these passwords/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**.**	**15-1.a** Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and/or components.
	15-1.b Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and are verified by the applicable key custodians.
	15-1.c Verify that the methods used for key validation are consistent with ISO 11568—for example, if check values are used, they should return a value of no more than six hexadecimal characters.
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.	**15-2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.
	15-2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.

Control Objective 4: Key-loading to HSMs and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**16-1.a** Verify documented procedures exist for all key-loading operations.
	16-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.
	16-1.c Observe key-loading process for keys loaded as components and verify that the documented procedures are demonstrably in use. This may be done as necessary on test equipment—e.g., for HSMs.
16-2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.	**16-2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**17-1.a** Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations.
	17-1.b For all keys shared between two organizations (including key-encryption keys used to encrypt a PIN-encryption key) perform the following: • Generate or otherwise obtain key-check values for any zone master keys (KEKs) to verify key uniqueness between the two organizations. A random sample may be used where more than ten zone connections are in use. This is not intended to be based on values retained on paper or otherwise sent as part of the original conveyance of the keying material, but rather on values generated from stored zone production keys from the production host database. Cryptopgrams may be used for this purpose if it is verified that the same MFK variant is used to encrypt the KEKs. • If a remote key-establishment and distribution scheme is implemented between networks, examine public keys and/or hash values and/or fingerprints of the keys to verify key uniqueness of the asymmetric-key pairs. • Compare key check values against those for known or default keys to verify that known or default key values are not used.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
***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.*	**18-1.a** Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.
	18-1.b Verify that implemented procedures include: • Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) • Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.
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.	**18-2.a** Verify documented procedures are documented require that key-component packaging/containers showing signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
	18-2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering results in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**18-3** Examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of acceptable methods or an equivalent.
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.	**19-1.a** Examine key-management documentation (e.g., the cryptographic key inventory) and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are defined for a specific purpose.
	19-1.b Using a sample of device types, validate via review of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.
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.	**19-2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are only used: • To create digital signatures or to perform decryption operations. • For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for POI devices). • Private keys are never used to encrypt other keys.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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).	**19-3** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for 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.*	**19-4.a** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and development systems.
	19-4.b Observe processes for generating and loading keys into in production systems to ensure that they are in no way associated with test or development keys.
	19-4.c Observe processes for generating and loading keys into in test systems to ensure that they are in no way associated with production keys.
	19-4.d Compare check, hash, cryptogram, or fingerprint values for production and test/development keys for higher-level keys (e.g., MFKs, KEKs shared with other network nodes and BDKs) to verify that development and test keys have different key values.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.*	**19-5** Interview personnel to determine whether production platforms are ever temporarily used for purposes other than processing of production transactions. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes the HSM is returned to factory state, • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.
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.*	**20-1.a** Examine documented procedures for the loading and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations.
	20-1.b Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POIs to verify that unique keys are generated and used for each POI device.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
	20-1.c Examine check values, hashes, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.
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.	**20-2** Determine whether any transaction-originating terminals interface with multiple acquiring organizations. If so: • Examine documented procedures for generating all types of keys and verify the procedures ensure that unique keys or sets of keys are used for each acquiring organization and are totally independent and not variants of one another. • Interview personnel and observe key-generation processes to verify that unique keys or sets of keys are generated for each acquiring organization.
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.	**20-3.a** Examine documented procedures and observe processes for generating master keys. Verify the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POIs receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.
	20-3.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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 BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model • Different BDKs 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 BDKS of acquiring organizations.	**20-4** Determine whether the entity processing or injecting DUKPT or other key-derivation methodologies does so on behalf of multiple acquiring organizations. If so: • Interview personnel and review documented procedures to determine that unique Base Derivation Keys are used for each acquiring organization. • Observe key-injection processes for devices associated with different acquiring organizations to verify that Base Derivation Key(s) unique to each organization are used.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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	**21-1.a** Examine documented procedures for key storage and usage and observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.
	21-1.b Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.
21-2 Wherever key components are used, they have the following properties:	**21-2** Examine documented procedures and interview responsible personnel to determine all instances where key components are used.
21-2.1 Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.	**21-2.1** Review processes for creating key components to verify that knowledge of any one key component 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.	**21-2.2** Observe processes for constructing cryptographic keys to verify that at least two key components are required for each key construction.
21-2.3 Each key component/share has one or more specified authorized custodians.	**21-2.3.a** Examine documented procedures for the use of key components and interview key custodians and key-management supervisory personnel to verify that each key component is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component.
	21-2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components are designated as key custodians for those particular components.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**21-2.4.a** Examine documented procedures for the use of key components to verify that procedures ensure that any custodian never has access to sufficient key components to reconstruct a cryptographic key. **21-2.4.b** Examine key-component access controls and access logs to verify that authorized custodians cannot access sufficient key components to reconstruct a cryptographic key.
21-3 Key components must be stored as follows:	**21-3** Examine documented procedures, interview responsible personnel, and inspect key-component storage locations to verify that key components are stored as outlined in Requirements 21-3.1 through 21-3.3 below.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**21-3.1.a** Examine key components and storage locations to verify that components are stored in opaque, pre-numbered tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging.
	21-3.1.b Inspect any tamper-evident packaging used to secure key components and ensure that it prevents the determination of the key component without visible damage to the packaging.
	21-3.1.c Ensure clear-text key components do not exist in any other locations, including in non-secure containers, in databases, on floppy disks, or in software programs.
	21-3.1.d Confirm that start-up instructions and other notes used by service technicians do not contain initialization-key values written in the clear (e.g., at the point in the checklist where the keys are entered).
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.*	**21-3.2** Inspect each key component storage container and verify the following: • Key components for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s).
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.	**21-3.3** Interview responsible personnel and observe implemented processes to verify that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its access code.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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** Verify documented procedures exist for replacing known or suspected compromised keys that includes all of 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.	**22-1.1** Interview responsible personnel and observe implemented processes to verify 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.	**22-1.2** Interview responsible personnel and observe implemented processes to verify that 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.*	**22-1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, all the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**22-1.4.a** Interview responsible personnel and review documented procedures to verify key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s).
	22-1.4.b Verify notifications include the following: • A damage assessment including, where necessary, the engagement of outside consultants. • Details of 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	**22-1.5** Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • 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.	**22-2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into a KLD or POI fail, the same key or component is not 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.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**23-1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods. **23-1.b** Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.
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.*	**23-2.a** Interview responsible personnel to determine which host MFKs keys exist as variants. ***Note:*** *Some HSMs may automatically generate variants or control vectors for specific keys, but it is still up to the entity to specify exact usage.* **23-2.b** Review vendor documentation to determine support for key variants. **23-2.c** Via review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used, determine that variants of the MFK are not used external to the logical configuration that houses the MFK.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**23-3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys. • Variants of working keys must only be calculated from other working 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.	**24-1.a** Verify documented procedures are in place for destroying secret or private keys and their components that are no longer used or that have been replaced by a new key.
	24-1.b Identify a sample of keys and key components that are no longer used or have been replaced. For each item in the sample, interview responsible personnel and examine key-history logs and key-destruction logs to verify that all keys have been destroyed.
	24-1.c Review storage locations for the sample of destroyed keys to verify they are no longer kept.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.
	24-2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.
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.*	**24-2.1.a** Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.
	24-2.1.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—are destroyed following the procedures outlined in ISO–9564 or ISO–11568.
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.	**24-2.2.a** Observe the key-destruction process and verify that it is witnessed by a third party other than a key custodian for any component of that key.
	24-2.2.b Inspect key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key destruction process.
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.	**24-2.3.a** Verify documented procedures exist for destroying key components of keys once the keys are successfully loaded and validated as operational.
	24-2.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:
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.	**25-1.1** Review key-custodian assignments for each component to verify that: • A primary and a backup key custodian are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel.
25-1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.	**25-1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form,
	25-1.2.b Examine completed key-custodian forms to verify that backup custodians sign the 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	**25-1.3** Examine all key-custodian forms to verify that they include 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.	
PIN Security Requirements	**Testing Procedures**
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.	**25-1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisor possess the necessary threshold of key components sufficient to form any given key. **25-1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, ensure that documented procedures exist and are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes whistleblower procedures to report any violations.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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)	**26-1.a** Review log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD
	26-1.b Review log files and audit log settings to verify that logs 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.	**27-1** Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following: • Observe backup processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys. • Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: o Securely stored with proper access controls o Under at least dual control o Subject to at least the same level of security control as operational keys as specified in this document

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**27-2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies for top-level keys requires at least 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	**28-1.a** Examine documented procedures for key-administration operations to verify they include: • 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
	28-1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.
	28-1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.
	28-1.d Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws).

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Review documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.
	29-1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.
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** Review documented procedures to verify controls are defined to protect POIs and other SCDs from unauthorized access up to point of deployment.
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.	**29-1.1.1.a** Examine access-control documentation and device configurations to verify that access to all POIs and key-injection/loading devices is defined and documented.
	29-1.1.1.b For a sample of POIs and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POIs and other SCDs is logged.
	29-1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI or other SCD.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**29-1.1.2** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys or passwords are not used.
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.	**29-1.1.3.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POIs and other SCDs are documented in a formal list. • All personnel with access to POIs and other SCDs are authorized by management. • The authorizations are reviewed annually.
	29-1.1.3.b For a sample of POIs and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in the formal list have access to devices.
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.	**29-2.a** Examine documented processes to verify that the chain of custody is required for devices from receipt to placement into service.
	29-2.b For a sample of devices, review documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to placement into service.
	29-2.c Verify that the chain-of-custody records identify responsible personnel for each interaction with the device.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.)* o 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.)* o Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.	**29-3.a** Examine documented procedures to confirm that they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods. **29-3.b** Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion and deployment.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures to confirm that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.
	29-4.b Interview responsible personnel and physically verify the dual-control mechanism used to prevent substitution or tampering of HSMs—both in service and spare or back-up devices—throughout their life cycle.
	29-4.c Determine the adequacy of those controls in enforcing dual control.
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.	**29-4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.
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.*	**29-4.1.b** For a sample of received devices, review sender documentation sent via a different communication channel than the device's shipment (for example, the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.
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.	**29-4.2.a** Obtain and review the defined security policy to be enforced by the HSM.
	29-4.2.b Examine documentation of the HSM configuration settings to determine that the functions and command authorized to be enabled are in accordance with the security policy.
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.	**29-4.2.c** For a sample of HSMs, review the configuration settings to determine that only authorized functions are enabled.
HSMs used for acquiring functions shall not be configured to output clear-text PINs.	**29-4.2.d** Verify that PIN-change functionality, PIN-block format translation functionality, or non-ISO PIN-block formats are not supported without a defined documented and approved business need.
	29-4.2.e Verify that functionality is not enabled to allow the outputting of clear-text PINs.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**29-4.3** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.
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** Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify integrity of device.
29-4.4.1 Running self-tests to ensure the correct operation of the device	**29-4.4.1** Examine records of device inspections and test results to verify that self-tests are run on devices 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	**29-4.4.2** Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, 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	**29-4.4.3** Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify 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	**29-4.4.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	29-4.4.4.b Examine records of inspections to verify records are retained for at least one year.
29-5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	**29-5.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.
	29-5.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**30.1.a** Obtain and review documentation of inventory control and monitoring procedures. Determine that the procedures cover: • Physically securing POI devices when awaiting deployment or otherwise not in use. • The prevention and detection of the unauthorized alteration or replacement of POI devices during deployment. • Ensuring that POI devices are physically secured or otherwise controlled to prevent unauthorized access, modification, or substitution while devices are deployed for use, including both attended and unattended devices (for example, kiosks, "pay-at-the-pump," etc.). • Preventing unauthorized physical access to devices undergoing repair or maintenance while in their possession. **30.1.b** Interview applicable personnel to determine that procedures are known and followed.
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.	**30.2** Obtain and review documentation of POI device-management processes. Determine that procedures cover: • Securely maintaining devices being returned, replaced, or disposed of, along with related instructions to third-party providers performing this service. • Protecting POI devices from known vulnerabilities and implementing procedures for secure updates to devices. • Providing for auditable logs of any changes to critical functions of the POI device(s). • Defined, implemented procedures for merchants on detecting and reporting tampered POI devices, including missing devices. • Implementing 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.	
PIN Security Requirements	**Testing Procedures**
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** Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all keys and key material stored within the device be securely destroyed. • Procedures cover all devices removed from service or for repair.
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.	**31-1.1.a** Review documented procedures for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes.
	31-1.1.b Interview personnel and observe demonstration (if HSM is available) of processes for removing HSMs from service to verify that dual control is implemented 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.	**31-1.2** Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material is rendered irrecoverable (for example, zeroized), or that devices are 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.	**31-1.3** Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.
31-1.4 Affected entities are notified before devices are returned.	**31-1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
31-1.5 Devices are tracked during the return process.	**31-1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
31-1.6 Records of the tests and inspections are maintained for at least one year.	**31-1.6** Interview personnel and observe records to verify that 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:	**32-1** Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices.
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.*	**32-1.1** Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
32-1.2 Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.	**32-1.2** Observe password policies and configuration settings to confirm that passwords used for dual control must be 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).	**32-1.3** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is 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 KLDs.
32-1.4 Devices must not use default passwords.	**32-1.4.a** Examine password policies and documented procedures to confirm default passwords must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys.
	32-1.4.b Observe device configurations and interview device administrators to verify that HSMs, KLDs, and other SCDs used to generate or load cryptographic keys do 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.	**32-1.5.a** Examine documented procedures to confirm that they require devices are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
	32-1.5.b Interview responsible personnel and observe devices and processes to confirm that devices are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**33-1.a** Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for devices placed into service, initialized, deployed, used, and decommissioned.
	33-1.b Verify that written records exist for 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

Control Objective 1:	***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***
PIN Security Requirements	**Testing Procedures**
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.***
PIN Security Requirements	**Testing Procedures**
No additional security requirements added for "Symmetric Key Distribution using Asymmetric Techniques."	

Control Objective 3:	***Keys are conveyed or transmitted in a secure manner.***
PIN Security Requirements	**Testing Procedures**
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.	**10-2** Examine documented procedures to verify that all asymmetric 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.	**10-3** Observe key-generation processes to verify that all asymmetric keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**15-3.a** Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: • POI devices must validate authentication credentials of KDHs prior to any key transport, exchange, or establishment with that device. • KDHs must validate authentication credentials of POIs prior to any key transport, exchange, or establishment with that device. **15-3.b** Interview applicable personnel to verify that mutual authentication of the sending and receiving devices is performed, as follows: • POI devices validate authentication credentials of KDHs immediately prior to any key transport, exchange, or establishment with that device. • KDHs validate authentication credentials of POIs immediately prior to any key transport, exchange, or establishment with that device.
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.	**15-5** Examine system and process documentation to verify that key-establishment and distribution procedures are designed such that: • There are no means available in the implementation design for "man-in-the-middle" attacks. • System implementations are designed to prevent replay attacks.
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.	**15-6** If key pairs are generated external to the device that uses the key pair, perform the following: • Examine documented procedures to verify that controls are defined to ensure the secrecy of private keys and the integrity of public keys during key transfer and loading. • Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured. • Verify the process ensures that key pairs are unique per POI device.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**18-4.a** Examine documented procedures to verify that: • POIs only communicate with CAs for the purpose of certificate signing, or for key injection where the certificate-issuing authority generates the key pair on behalf of the device; • POIs only communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.
	18-4.b Interview responsible personnel and observe POI configurations to verify that: • POIs only communicate with CAs for the purpose of certificate signing, or for key-injection where the certificate issuing authority generates the key pair on behalf of the device; • POIs only communicate 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.	**18-5.a** Examine documented procedures to verify that: • KDHs only communicate with POIs for the purpose of key management and normal transaction processing; • KDHs only to communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.
	18-5.b Interview responsible personnel and observe KDH configurations to verify that: • KDHs only communicate with POIs for the purpose of key management and normal transaction processing; • KDHs only communicate 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.	
PIN Security Requirements	**Testing Procedures**
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.	**19-6.a** Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate
	19-6.b Interview responsible personnel and observe certificate issuing and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Certificates are replaced by generating a new key pair and requesting a new certificate. • Each key pair generated results in only one certificate.
19-7 KDH private keys must not be shared between devices except for load balancing and disaster recovery.	**19-10** Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.
19-8 POI private keys must not be shared between devices.	**19-11.a** Examine documented processes to verify that POI private keys are not permitted to be shared between devices.
	19-11.b Inspect public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**21-4.a** Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.
	21-4.b Observe key-management operations and interview key custodians and key-management supervisory personnel to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.

A2 – Certification and Registration Authority Operations

Control Objective 3:	***Keys are conveyed or transmitted in a secure manner.***
PIN Security Requirements	**Testing Procedures**
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.	**10-2** Examine documented procedures to verify that all asymmetric 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.	**10-3** Observe key-generation processes to verify that all asymmetric keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed.

Control Objective 4:	***Key-loading to hosts and PIN entry devices is handled in a secure manner.***
PIN Security Requirements	**Testing Procedures**
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.	**15-6** If key pairs are generated external to the device that uses the key pair, perform the following: • Examine documented procedures to verify that controls are defined to ensure the secrecy of private keys and the integrity of public keys during key transfer and loading. • Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured. • Verify the process ensures that key pairs are unique per POI device.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**19-5** Interview personnel to determine whether production platforms are ever temporarily used for purposes other than processing of production transactions. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server/computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media. • Prior to reuse for production purposes, the HSM is returned to factory state. • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in 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.	**19-6.a** Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate replacement request • Each key pair generated results in only one certificate
	19-6.b Interview responsible personnel and observe certificate issuing and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Certificates are replaced by generating a new key pair and requesting a new certificate. • Each key pair generated results in only one certificate.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine key-usage documentation and ensure that the usage is in accordance with the certificate policy.
	19-9.b Examine vendor documentation and device configuration settings to verify that the device mechanisms are implemented that preclude the use of a key for other than its designated and intended purpose.
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.*	**19-9.1.a** Examine certificate policy and documented procedures to verify that: • Certificate signature keys, • Certificate status checking (for example, Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs Must not be used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
	19-9.1.b Interview responsible personnel and observe demonstration to verify that: • Certificate signature keys, • Status checking (for example, Certificate Revocation Lists) signature keys, or • Signature keys for updating valid/authorized host lists in POIs Are not used for any purpose other than: • Subordinate entity certificate requests, • Certificate status checking, and/or • Self-signed root certificates.
19-9.2 CAs that issue certificates to other CAs must not be used to issue certificates to POIs.	**19-9.2** If a CA issues certificates to other CAs, examine the CA certificate policy and documented procedures to verify that the CA does not also issue certificates to POI devices.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**19-10** Examine documented procedures to verify that mechanisms are defined for restricting and controlling the use of public and private keys such that they can only be used for their intended purpose.
19-11 CA private keys must not be shared between devices except for load balancing and disaster recovery.	**19-11** Examine CA's documented processes to verify that CA private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**21-4.a** Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.
	21-4.b Observe key-management operations and interview key custodians and key-management supervisory personnel to verify that private keys used to sign certificates, certificate-status lists, messages, or for key protection must exist only in one or more of the approved forms at all times.
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.	**22-6** Through the examination of documented procedures, interviews and observation confirm that Root CAs provide for segmentation of risk to address key compromise.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures to verify that mechanisms are defined to respond to compromise of a CA. Verify the mechanisms include procedures to: • Revoke subordinate certificates, and • Notify affected entities.
	22-7.b Interview responsible personnel to verify that the defined mechanisms to respond to compromise of a CA are in place and include: • Revoking subordinate certificates, and • Notifying 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.	**22-7.1.a** Examine documented procedures to verify that the following are required in the event a compromise is known or suspected: • The CA will cease issuance of certificates. • The CA will perform a damage assessment, including a documented analysis of how and why the event occurred.
	22-7.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: • The CA ceases issuance of certificates. • The CA performs 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.	**22-7.2.a** Examine documented procedures to verify that in the event of a confirmed compromise, procedures are defined for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.
	22-7.2.b Interview responsible personnel to verify procedures are followed for the CA to determine whether to revoke and reissue all signed certificates with a newly generated signing key.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
22-7.3 Mechanisms (for example, time stamping) must exist to prevent the usage of fraudulent certificates, once identified.	**22-7.3.a** Examine documented procedures to verify that mechanisms are defined to prevent the usage of fraudulent certificates.
	22-7.3.b Interview responsible personnel and observe implemented mechanisms to verify the prevention of the use of fraudulent certificates
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.	**22-7.4.a** Examine documented procedures to verify that the following procedures are required in the event of a compromise: • The CA will notify any superior CAs. • The CA will notify any subordinate CAs. • The CA will perform a damage assessment to determine the need to either: o Reissue and distribute certificates to affected parties, or o Notify the affected parties to apply for new certificates.
	22-7.4.b Interview responsible personnel to verify that the following procedures are performed in the event a compromise: • The CA notifies any superior CAs. • The CA notifies any subordinate CAs. • The CA performs a damage assessment to determine the need to either: o Reissues and distributes certificates to affected parties, or o Notifies the affected parties to apply for new certificates.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**22-8.a** Interview appropriate personnel and examine documented procedures for the creation of these keys. **22-8.b** Verify that the following minimum key sizes exist for RSA keys or the equivalent for the algorithm used as defined in Annex C: • 2048 for CAs • 1024 for KDHs and POI devices **22-8.c** Verify that KDH keys expire 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.a** Examine documented procedures to confirm that access to material that can be used to construct secret and private keys is directly attributable to an individual user. **25-2.b** Observe the access-control mechanisms in place to verify that access to material that can be used to construct secret and private keys is directly attributable to an individual user.
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.*	**25-2.1.a** Examine documented procedures to confirm that access to material that can be used to construct secret and private keys must be restricted to actions authorized for that role. **25-2.1.b** Observe user role assignments and access-control mechanisms to verify that access to material that can be used to construct secret and private keys is restricted to actions authorized for that role.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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).	**25-3.1** Examine network diagrams and observe network and system configurations to verify: • CA systems that issue certificates to other CAs and KDHs are operated offline using a dedicated closed network (not a network segment). • The network is only used for certificate issuance, revocation, or both certificate issuance and revocation. • Outside network access shall exist only for the purposes of "pushing" certificate-status information to relying parties (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).	**25-3.2** Examine software update processes to verify that local console access is used for all 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.	**25-3.3** Examine remote-access mechanisms and system configurations to verify that all non-console access, including remote access, requires two-factor authentication.
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.*	**25-3.4.a** Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions. **25-3.4.b** Observe an authorized CA personnel attempt non-console access to the host platform using valid CA credentials without using an authenticated encrypted session to verify that non-console access is not permitted.
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.*	**25-3.5.a** Examine the certificate security policy and certification practice statement to verify that CA certificate-signing keys must only be enabled under at least dual control. **25-3.5.b** Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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).	**25-4.a** Examine documented procedures to verify they include following: • Definition of critical functions of the CA • Separation of duties to prevent one person from maliciously using a CA system without detection • Multi-person control for operational procedures such that no one person can gain control over the CA signing key(s)
	25-4.b Observe CA operations and interview responsible personnel to verify: • Definition of Critical functions of the CA • Separation of duties to prevent one person from maliciously using a CA system without detection • 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.a** Examine system documentation to verify the following is required: • Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, etc., commands in UNIX) must be removed or disabled. • Unnecessary ports must also be disabled. • Documentation must exist to support the enablement of all active services and ports.
	25-5.b For a sample of systems, examine documentation supporting the enablement of active services and ports, and observe system configurations to verify: • Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, etc., commands in UNIX) are removed or disabled. • Unnecessary ports are disabled. • There is documentation to support all active services and ports.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**25-5.1.a** Examine documented procedures to verify that: • Vendor-default IDs are 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 are only be enabled when required and otherwise must be disabled from login.
	25-5.1.b Examine system configurations and interview responsible personnel to verify that: • Vendor-default IDs are 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 are 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.	**25-5.2.a** Examine documented procedures to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.
	25-5.2.b Examine system configurations and interview responsible personnel to verify that vendor defaults, including passwords and SNMP strings, that exist and are not addressed in the prior step are changed, removed, or disabled before installing a system on the network.
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.a** Examine system configurations and audit trails to verify that all key-management operations are logged.
	25-6.b For a sample of key-management operations, examine audit trails to verify they include: • The identity of the person authorizing the operation • The identities of all persons handling any key material • Mechanisms exist to protect logs from alteration and destruction

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
25-6.1 Audit logs must be archived for a minimum of two years.	**25-6.1** Examine audit trail files to verify that they are 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.	**25-6.2.a** For a sample of certificate issuances, examine audit records to verify that the records are retained for at least the life of the associated certificate.
	25-6.2.b For a sample of certificate revocations, examine audit records to verify that the records are retained for at least 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.	**25-6.3.a** Examine audit trails to verify that logical events are divided into operating-system and CA application events.
	25-6.3.b Examine a sample of operating-system logs to verify they contain the following information: • 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.
	25-6.3.c Examine a sample of application logs to verify they contain the following information: • 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.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**25-7.a** Examine log security controls to verify that CA application logs 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.b** Review documentation and interview personnel and observe to verify that signing/MACing key(s) used for this are 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.	**25-7.1.a** Examine network and system configurations to verify that certificate-processing system components operated online are protected from unauthorized access by firewall(s).
	25-7.1.b Examine firewall configurations for verify they are 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.	
PIN Security Requirements	**Testing Procedures**
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.	**25-7.2.a** Observe network-based and/or host-based IDS configurations to verify that on-line certificate-processing systems are protected by IDS to detect inappropriate access.
	25-7.2.b Verify that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.
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).	**25-8.1** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and are pre-expired.
25-8.2 Use of group, shared, or generic accounts and passwords, or other authentication methods is prohibited.	**25-8.2.a** For a sample of system components, examine user ID lists to verify the following: • Generic user IDs and accounts are disabled or removed. • Shared user IDs for system administration activities and other critical functions do not exist. • Shared and generic user IDs are not used.
	25-8.2.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.
	25-8.2.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.
25-8.3 If passwords are used, system-enforced expiration life must not exceed 30 days and a minimum life at least one day.	**25-8.3** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 30 days and have a minimum life of 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.	**25-8.4** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least eight characters long and contain numeric, alphabetic, and special characters.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
25-8.5 Limit repeated access attempts by locking out the user ID after not more than five attempts.	**25-8.5** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon 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.	**25-8.6** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to 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.	**25-8.7** For a sample of system components, obtain and inspect system configuration settings to verify that passwords are not stored unless encrypted as part of a proprietary one-way hash.
25-8.8 The embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.	**25-8.8.a** Review policies and procedures and interview personnel to determine that the embedding of passwords in shell scripts, command files, communication scripts, etc. is strictly prohibited.
	25-8.8.b Inspect a sample of shell scripts, command files, communication scripts, etc. to verify that passwords are not embedded in shell scripts, command files, or communication scripts.
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.*	**25-8.9.a** If log-on security tokens are used, observe devices in use to verify that the security tokens have an associated usage-authentication mechanism, such as a biometric or associated PIN/passphrase to enable their usage.
	25-8.9.b Examine token-configuration settings to verify parameters are set to require PINs/passwords be at least eight decimal digits in length, or equivalent.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
25-9 Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations.	**25-9.a** Examine documented procedures and system configuration standards to verify a method is defined to synchronize all critical system clocks and times for all systems involved in key-management operations.
	25-9.b For a sample of critical systems, review the time-related system parameters to verify that system clocks and times are synchronized for all systems involved in key-management operations.
	25-9.c If a manual process is defined, verify that the documented procedures require that it occur at least quarterly.
	25-9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.
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.	**28-2.a** Examine documented procedures to verify: • CA operations must be dedicated to certificate issuance and management. • All physical and logical CA system components must be separated from key-distribution systems.
	28-2.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.
	28-2.c Observe system and network configurations and physical access controls to verify that all physical and logical CA system components are separated from key-distribution systems.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**28-3.a** Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document. **28-3.b** Examine documented operating procedures to verify they are defined in accordance with the CPS. **28-3.c** Interview personnel and observe CA processes to verify that CA operations are 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.)	**28-4** Examine documented certificate policy to verify that the CA has one in place.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures to verify they include validating the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key. **28-5.b** Observe certificate-issuing processes to verify that the identities of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**28-5.1.a** Examine documented procedures to verify that certificate-signing requests, including certificate or key-validity status changes, require 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.
	28-5.1.b Observe certificate-signing requests, including certificate or key-validity status changes, to verify they 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.	**28-5.2** Examine documentation and audit trails to verify that the identification of entities is retained for the life of the associated certificates: • For all certificates issued • For all certificates whose status had changed

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**32-2.1.a** Examine physical security policies to verify three tiers of physical security are defined as follows: • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices
	32-2.1.b Observe the physical facility to verify three tiers of physical security are implemented as follows: • Level One Barrier – The entrance to the facility • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility • Level Three Barrier – 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.	**32-2.2.1.a** Examine physical-security procedures and policies to verify they require that the facility entrance allows only authorized personnel to enter the facility.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	32-2.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed 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.	**32-2.2.2.a** Examine physical-security procedures and policies to verify they require that the facility have a guarded entrance or a foyer with a receptionist or the entryway prevents access to visitors.
	32-2.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.
32-2.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.	**32-2.2.3.a** Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.
	32-2.2.3.b Observe the facility entrance and observe personnel entering the facility to verify that visitors are authorized and 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.a** Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the Level 2 barrier/entrance.
	32-2.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.
32-2.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.	**32-2.3.1.a** Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.
	32-2.3.1.b Interview personnel and observe visitors entering the environment to verify that visitors are authorized and escorted at all times within the Level 2 environment.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
32-2.3.2 Access logs must record all personnel entering the Level 2 environment. ***Note:*** *The logs may be electronic, manual, or both.*	**32-2.3.2.a** Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.
	32-2.3.2.b Observe personnel entering the Level 2 barrier and review corresponding access logs to verify that all entry through the Level 2 barrier is logged.
32-2.4 The Level 2 entrance must be monitored by a video-recording system.	**32-2.4.a** Observe the Level 2 entrance to verify that a video-recording system is in place.
	32-2.4.b Review a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.
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.	**32-2.5.a** Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.
Note: *All certificate-processing operations must operate in the Level 3 environment.*	**32-2.5.b** Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.
	32-2.5.c Observe operations and interview personnel to confirm that the Level 3 secure room is not used for any business activity other than certificate operations.
32-2.5.1 Doors to the Level 3 area must have locking mechanisms.	**32-2.5.1.a** Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**32-2.5.2.a** Examine physical security documentation for the Level 3 environment to verify that the environment is enclosed on all sides (including the ceiling and flooring areas) using techniques such as have true floor-to-ceiling (slab-to-slab) walls, steel mesh, or bars
	32-2.5.2.b Examine the physical boundaries of the Level 3 environment to verify that the environment is 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 and protection from entry from below floors and above ceilings.
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.a** Examine documented procedures to verify they include the following: • 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.b Interview responsible personnel to verify that the documented procedures are followed 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.*	**32-2.6.1.a** Examine documented policies and procedures to verify they require personnel authorized as having access through the Level 3 barrier to: • Have successfully completed a background security check. • Be assigned resources of the CA operator with defined business needs and duties.
	32-2.6.1.b Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws) on CA personnel prior such personnel being authorized for access through the Level 3 barrier.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	32-2.6.1.c Interview a sample of personnel authorized for access through the Level 3 barrier to verify that they are assigned resources of the CA with defined business needs and duties.
32-2.6.2 Other personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.	**32-2.6.2.a** Examine documented policies and procedures to verify that personnel requiring entry to this level must be accompanied by two (2) authorized and assigned resources at all times.
	32-2.6.2.b Interview a sample of responsible personnel to verify that personnel requiring entry to this level are 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.	**32-2.7.a** Examine documented policies and procedures to verify that the Level 3 environment requires dual-control access and dual-occupancy such that the room is never occupied by one person alone for more than thirty (30) seconds.
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.b** Observe authorized personnel accessing the Level 3 environment to verify that dual-control access and dual-occupancy is enforced such that the room is never occupied by one person alone for more than thirty (30) seconds.
32-2.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated.	**32-2.7.1.a** Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.
	32-2.7.1.b Observe enforcement mechanism configuration to verify it is automated.
32-2.7.2 The system must enforce anti-pass-back.	**32-2.7.2.a** Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.
	32-2.7.2.b Observe mechanisms in use and authorized personnel within the environment to verify that anti-pass-back is enforced by the conduct of a test.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
32-2.7.3 Dual occupancy requirements are managed using electronic (for example, badge and/or biometric) systems.	**32-2.7.3.a** Examine documented policies and procedures to verify that dual occupancy requirements are defined to be managed using electronic (for example, badge and/or biometric) systems.
	32-2.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic 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.	**32-2.7.4.a** Examine documented policies and procedures to verify that any time one person is alone in the room for more than 30 seconds, the system must automatically generate an alarm and an audit event that is followed up by security personnel.
	32-2.7.4.b Observe mechanisms in use to verify that the system automatically generates an alarm event and an audit event when one person is alone in the room for more than 30 seconds.
	32-2.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.
32-2.8 Access to the Level 3 room must create an audit event, which must be logged.	**32-2.8** Observe authorized personnel enter the environment and examine correlating audit logs to verify that access to the Level 3 room creates an audit log event.
32-2.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel	**32-2.8.1** Observe an invalid access attempt and examine correlating audit logs to verify that invalid access attempts to the Level 3 room create an audit log event.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**32-2.9.1.a** Observe the Level 3 physical environment to verify that cameras are in place to monitor the Level 3 environment, including the entry and exit.
	32-2.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.
	32-2.9.1.c If motion-activated systems are used for monitoring, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.
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.	**32-2.9.2** Examine monitoring system configurations to verify; • The system records to time-lapse VCRs or similar mechanisms. • A minimum of five frames are recorded 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).*	**32-2.9.3.a** Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for each camera monitoring the environment.
	32-2.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.
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.	**32-2.9.4.a** Observe each camera locations in the Level 3 environment to verify they are not set to monitor computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.
	32-2.9.4.b Examine a sample of captured footage to verify it does not allow for the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**32-2.9.5.a** Examine documented access policies and procedures to verify that personnel with access to the Level 3 environment are not permitted to have access to the media containing recorded surveillance data for that environment.
	32-2.9.5.b Examine Level 3 access lists as well as access controls to the media containing surveillance data, to verify that personnel with access to the Level 3 environment do not have access to the media containing 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.	**32-2.9.6.a** Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.
	32-2.9.6.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient 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.	**32-2.9.7** Examine backup techniques utilized to ensure that: • Backups are securely stored in a separate location from the primary. • Ensure that segregation is maintained between users and administrators of the system.
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.a** Examine security policies and procedures to verify they require: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment. • Motion detectors must be active when the environment is unoccupied.
	32-3.b Examine intrusion-detection system configurations to verify: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place. • Motion detectors are active when the environment is unoccupied.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
32-3.1 Any windows in the secure area must be locked and protected by alarmed sensors.	**32-3.1.a** Observe all windows in the secure areas to verify they are locked and protected by alarmed sensors.
	32-3.1.b Examine configuration of window sensors to verify that the alarm mechanism is active.
	32-3.1.c Test at least one window (if they can be opened) to verify that the alarms function appropriately.
32-3.2 Any windows or glass walls must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**32-3.2** Observe all windows and glass walls in the secure areas to verify they are 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.	**32-3.3.a** Examine security system configurations to verify: • The intrusion-detection system(s) is connected to the alarm system. • The intrusion-detection system(s) is automatically activated every time all authorized personnel have exited the secure area.
	32-3.3.b Verify the IDS and alarms function correctly via: • Having all authorized personnel who badged or otherwise authenticated into the area exit and one person remain behind even though they have badged out. • Having all but one authorized person who badged or otherwise authenticated into the system badge out and exit.
32-3.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.	**32-3.4** Examine security-system configurations to verify that an alarm event is generated for: • Unauthorized entry attempts • Actions that disable the intrusion-detection system
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.a** Examine security policies and procedures to verify they require all personnel (including CA personnel and visitors) to sign an access logbook when entering the Level 3 environment.
	32-4.b On the escorted entry into the secure area, observe that all personnel appropriately sign the access logbook and that all escorted visitors are required to sign the access logbook.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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	**32-4.1** Examine the access logbook to verify it contains the following information: • 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.	**32-4.2** Observe the location of the access logbook and verify that it is 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).	**32-5** Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems, including intrusion-detection systems, are powered through the UPS.
32-6 All alarm events must be documented.	**32-6.a** Examine security policies and procedures to verify they require that all alarm events are logged.
	32-6.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.
32-6.1 An individual must not sign off on an alarm event in which they were involved.	**32-6.1.a** Examine documented procedures for responding to alarm events to verify that the procedure does not permit a person who was involved in an alarm event to sign-off on that alarm event.
	32-6.1.b Determine who is authorized to sign off on alarm events.
	32-6.1.c For a sample of documented alarm events, review the record to verify that personnel authorized to sign off on alarm events were not also the cause of that event.
32-6.2 The use of any emergency entry or exit mechanism must cause an alarm event.	**32-6.2.a** Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.
	32-6.2.b Conduct a test to verify the mechanisms work appropriately.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedures**
32-6.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.	**32-6.3.a** Review documented procedures to verify they require that all alarms for physical intrusion must be responded to within 30 minutes by personnel assigned security duties.
	32-6.3.b Examine a sample of alarm events and interview personnel assigned with security-response duties to verify that alarms for physical intrusion are responded to within 30 minutes.
	32-6.3.c Conduct a test to verify the appropriate response occurs.
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.a** Examine documented procedures to verify that mechanisms are defined (may be automated or manual) for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs.
	32-7.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.
	32-7.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.
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.	**32-7.1.a** If a manual synchronization process is implemented, interview responsible personnel and examine records of synchronization to verify the mechanism is performed at least quarterly.
	32-7.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.

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.

Note:

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

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

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

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

Control Objective 1:	***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***	
PIN Security Requirements		**Testing Procedures**
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.		**1-2.a** Examine documented procedures and system documentation to verify that key-injection platforms and systems used for managing cryptographic keys are required to conform to the requirements for SCDs.
		1-2.b Examine key-injection platforms and systems used for managing cryptographic keys to verify they 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.		**1-3.a** For all HSM brands/models used, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3, or higher. Refer http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.
		1-3.b Examine documented procedures and interview personnel to verify that all decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified above.

Control Objective 1:	***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***
PIN Security Requirements	**Testing Procedures**
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	**1-4.a** For all PCI-approved HSMs used, examine HSM devices and review the *PCI SSC list of Approved PCI PTS Devices* to verify that all of the following device characteristics match the PCI PTS listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number • Any applications, including application version number, resident within the device which were included in the PTS assessment
	1-4.b For all FIPS-approved HSMs used, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 Level 3 (or higher) approval listing for each HSM: • Vendor name • Model name/number • Hardware version number • Firmware version number

Control Objective 1:	***PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.***
PIN Security Requirements	**Testing Procedures**
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.	**1-5.a** Interview relevant personnel and review documentation to verify that procedures exist for maintaining documentation that describes and/or illustrates the architecture of the KIF.
	1-5.b Interview relevant personnel and review documentation that describes and/or illustrates the architecture of the KIF to verify that all KIF components, key-management flows, and personnel interaction with key-management flows are identified and documented.
	1-5.c Examine the key-management flows and interview personnel to verify: • Documentation shows all key-management flows across functions and networks from the point the key is generated through to the point the key is injected into the POI. • Documentation is kept current and updated as needed upon changes to the KIF architecture

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.***

PIN Security Requirements	Testing Procedures
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.*	**5-1.a** Examine key-management policy document and to verify that it requires that all devices used to generate cryptographic keys meet one of the following • An approved key-generation function of a PCI-approved HSM • 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 qualified laboratory according to *NIST SP 800-22.*
	5-1.b Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following • An approved key-generation function of a PCI–approved HSM • 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 qualified laboratory according to *NIST SP 800-22*
	5-1.c Verify devices used for key generation are those as noted above, including validation of the firmware used.
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** Perform the following:

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.***

PIN Security Requirements	Testing Procedures
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.	**6-1.1.a** Examine documented procedures to verify the following: • Any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key. • There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.
	6-1.1.b Observe key-generation processes and interview responsible personnel to verify: • Any clear-text output of the key-generation process is overseen by only the assigned key custodian(s) for that component/share and is limited to those individual components and not the entire key. • There is no mechanism including connectivity that might disclose a clear-text key or key component between the key-generation device 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.*	**6-1.2.a** Observe the process from end to end to verify there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.
	6-1.2.b Examine key-generation logs to verify that at least two individuals performed the key-generation processes.
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.	**6-1.3** Examine documented procedures for all key-generation methods. Verify procedures require that: • Key-generation devices that generate clear-text key components be powered off when not in use; or • If logically partitioned for concurrent use in other processes, the key-generation capabilities are disabled when not in use and other activities are continuing.

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.***

PIN Security Requirements	Testing Procedures
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).	**6-1.4.a** Review documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering, prior to use.
	6-1.4.b Observe key-generation set-up processes for all key types to verify that key-generation equipment is inspected prior to use, to ensure equipment does not show any signs of tampering.
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.	**6-1.5.a** Examine documentation to verify that physical security controls are defined to ensure the key component/key-generation process cannot be observed or accessed by unauthorized personnel.
	6-1.5.b Observe the physical security controls to verify that key-component/key-generation process cannot be observed or accessed by unauthorized personnel.
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.*	**6-2.a** Examine documented procedures to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.
	6-2.b Observe generation process and review vendor documentation for each type of key to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory. **6-2.c** Where single-purpose computers with an installed SCD are used, verify that either: • Clear keying material is injected directly from a secure port on the SCD to the target (e.g., a POI device) or • Where clear keying material passes through unprotected memory of the PC, the PC requirements of Requirement 13 of Annex B are met.

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.***

PIN Security Requirements	Testing Procedures
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.	**6-3.a** Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed immediately after printing such that: • Only approved key custodians can observe their own key component. • Tampering can be detected. • Printers used for this purpose are not used for other purposes.
	6-3.b Observe processes for printing key components to verify that key components are printed within blind mailers or sealed immediately after printing, such that no one but the authorized custodian ever has physical access to the output.
	6-3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be detected.

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.***

PIN Security Requirements	Testing Procedures
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*	**6-4.a** Examine documented procedures to identify all locations where key residue may exist. Verify procedures are implemented to ensure the following: • Any residue that may contain clear-text keys or components is destroyed or securely deleted immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.
	6-4.b Observe the destruction process of the identified key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, confirm that the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.

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.***

PIN Security Requirements	Testing Procedures
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.	**6-5.a** Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.
	6-5.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (for example, zeroized) immediately after the transfer to the device that will use the key pair.
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	**6-6.a** Examine documented policy and procedures to verify that key components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual

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.***
PIN Security Requirements	**Testing Procedures**
	6-6.b From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating verbally keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual
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.	**7-1.a** Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations.
	7-1.b Interview those responsible for the key-generation processes (including key custodians, supervisory staff, technical management, etc.) to verify that the documented procedures are known and understood by all affected parties.
	7-1.c Observe key-generation ceremonies whether actual or for demonstration purposes, and verify that the documented procedures are demonstrably in use.
7-2 Logs must exist for the generation of higher-level keys such as KEKs exchanged with other organizations and MFKs and BDKs.	**7-2.a** Examine documented key-generation procedures to verify that all key-generation events for higher-level keys (e.g., KEKs shared with other organizations or otherwise manually loaded as components and MFKs and BDKs) must be logged.
	7-2.b Observe demonstrations for all types of key-generation events to verify that all key-generation events are logged.
	7-2.c Examine logs of key generation to verify that exchanges of higher-level keys with other organizations have been recorded.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.

PIN Security Requirements	Testing Procedures
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: o 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. o Ensure that details of the serial number of the package are conveyed transmitted separately from the package itself. o 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.*	**8-1.a** Determine whether keys are transmitted encrypted, as clear-text components or within an SCD. **8-1.b** If key components are ever transmitted in clear text using tamper-evident mailers, perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself. • Examine documented procedures to verify that cryptographic-key components are transferred using different communications channels. • Examine records of key transfers and interview responsible personnel to verify that cryptographic key components are transferred using different communications channels. • Examine documented procedures to verify that serial numbers are verified prior to the usage of the keying material. *(continued on next page)*

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	8-1.c Where SCDs are used to convey components, perform the following: • Examine documented procedures to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels. • Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering. • Examine records of key transfers and interview responsible personnel to verify that the mechanisms to obtain the keying material are conveyed using separate communication channels.
	8-1.d Where SCDs are conveyed with pre-loaded secret and/or private keys, perform the following: • Examine documented procedures to verify that the SCD requires dual-control mechanisms to become operational. • Examine documented procedures to verify that the SCD is inspected to ensure that there are not any signs of tampering. • Examine records of key transfers and interview responsible personnel to verify that the mechanisms make the SCD operational are conveyed using separate communication channels.
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.*	**8-2.a** Examine documented procedures to verify they include controls to ensure that no single person can ever have access to 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. . Verify procedures include: • Any person with access to one component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other components or shares sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a component/share of a key must not have access to other components/shares of this key, or to any other medium conveying any other component of this key that is sufficient to form the necessary threshold to derive the key.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	8-2.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can ever have access to 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. Verify the implemented controls ensure the following: • An individual with access to a key component or key share does not have access to other components/shares of this key or to any other medium conveying other components or shares of this key that are sufficient to form the necessary threshold to derive the key. • Any person with access to the media conveying a key component or key share must not have access to other components/shares of this key or to any other medium conveying any other components or shares of this key that are sufficient to form the necessary threshold to derive the key.
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.	**8-3** Validate through interviews, observation, and logs that email, SMS, fax, or telephone or similar communication is not used as means to convey secret or private keys or key components.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**8-4** For all methods used to convey public keys, perform the following: • Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity such as: o Use of public-key certificates created by a trusted CA that meets the requirements of Annex A o A hash of the public key sent by a separate channel (for example, mail) o Using a MAC (message authentication code) created using the algorithm defined in ISO 16609 o Be within an SCD • Validate that self-signed certificates must not be used as the sole method of authentication. • Observe the process for conveying public keys and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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 BDKs when the BDKs are conveyed between entities (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf), or key components for the BDKs themselves, and terminal master keys used in the master key/session key key-management method.	
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.*	**9-1.a** Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text key component 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 it can be obtained only by a person with authorized access to it, or • Contained within a physically secure SCD.
	9-1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text key component is at all times 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 it can be obtained only by a person with authorized access to it, or • Contained within a physically secure SCD.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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	**9-2.a** Verify documented procedures include requirements for all packaging or mailers containing clear-text key components to be examined for evidence of tampering before being opened.
	9-2.b Interview responsible personnel and observe processes to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being opened.
	9-2.c Verify documented procedures require that any sign of package tampering results in the destruction and replacement of both: • The set of components • Any keys encrypted under this (combined) key
	9-2.d Interview responsible personnel and observe processes to verify that, if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: • 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.	**9-3.a** Verify that a list(s) of key custodians (and designated backup(s)) authorized to have physical access to key components prior to transmittal or upon receipt of a component is defined and documented.
	9-3.b Observe implemented access controls and processes to verify that only those authorized key custodians (and designated backup(s)) have physical access to key components prior to transmittal or upon receipt.
	9-3.c Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each component.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**9-4.a** Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into pre-numbered tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • Check the serial number of the tamper-evident packing upon receipt of a component package.
	9-4.b Observe implemented mechanisms and processes to verify that only the authorized key custodians can perform the following: • Place the key component into tamper-evident packaging for transmittal. • Upon receipt, check the tamper-evident packaging for signs of tamper prior to opening the tamper-evident packaging containing the key component. • 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*	**9-5** Verify that pre-numbered, tamper-evident, authenticable bags are used for the conveyance of clear-text key components and perform the following: • Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself. • Observe the method used to transport clear-text key components using tamper-evident mailers, and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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 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).	
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.*	**10-1.a** Examine documented procedures to verify that all keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed. *(continued on next page)*

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	10-1.b Observe key-generation processes to verify that all keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed. • Interview appropriate personnel and examine documented procedures for the creation of these keys. • Using the table in Annex C, validate the respective key sizes for DEA, RSA, Elliptic Curve, DSA, and Diffie Hellman algorithms where used for key encryption. • Verify that: o 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. o A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength. o TDEA keys are not used to protect AES keys. o TDEA keys shall not be used to encrypt keys greater in strength than 112 bits. o RSA keys used to transmit or convey other keys have bit strength of at least 80 bits. o RSA keys encrypting keys greater in strength than 80 bits have bit strength at least 112 bits. • Verify that any POI device that is version 3 or higher is using RSA with a key size of at least 2048 and SHA-2, where applicable, within 24 months of publication of these requirements. Use as necessary the device inventory used in Requirement 1.
	10-1.c Examine system documentation and configuration files to validate the above, including HSM settings.

Control Objective 3: Keys are conveyed or transmitted in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**11-1.a** Verify documented procedures exist for all key transmission and conveyance processing.
	11-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.
11-2 Methods used for the conveyance or receipt of keys must be documented.	**11-2** Verify documented procedures include all methods used for the conveyance or receipt of keys.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	
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 manufacture's private key and subsequently loaded into the POI for supporting certain key-establishment and distribution applications protocols (if applicable). Dual control is not necessary where other mechanisms exist to validate the authenticity of the key, such as the presence in the device of an authentication key;* • *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.*	**12-1.a** Review documented process to load each key type (MFK, TMK, PEK, etc.) from components to ensure dual control and split knowledge are required.
	12-1.b Interview appropriate personnel to determine the number of key components for each manually loaded key, and the methodology used to form the key.
	12-1.c Witness a structured walk-through/demonstration of various key-loading processes for all key types (MFKs, TMKs, PEKs. etc.). Verify the number and length of the key components to information provided through verbal discussion and written documentation.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	12-1.d Verify that the process includes the entry of individual key components by the designated key custodians.
	12-1.e Ensure key-loading devices can only be accessed and used under dual control.
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.	**12-2** Examine logs of access to security containers for key components to verify that only the authorized custodian(s) have accessed. Compare the number on the current TEA bag for each component to the last log entry for that component.
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.*	**12-3.a** Examine documented procedures for loading of clear-text cryptographic keys, including public keys, to verify they require dual control to authorize any key-loading session.
	12-3.b For all types of production SCDs, observe processes for loading clear-text cryptographic keys, including public keys, to verify that dual control is required to authorize any key-loading session. Verify that any passwords used are a minimum of five characters.
	12-3.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.
	12-3.d Ensure that any default dual-control mechanisms (e.g., default passwords—usually printed in the vendor's manual—in a key-loading device) have been disabled or changed.
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.	**12-4.a** Examine documented procedures for combining symmetric key components and observe processes to verify that key components are combined using a process such that no active bit of the key can be determined without knowledge of the remaining components.
	12-4.b Examine key-component lengths or device configuration settings to verify that key components used to create a key are the same length as the resultant key.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**12-5** Examine vendor documentation describing options for how the HSM MFK is created. Corroborate this via observation of processes, with information gathered during the interview process, and procedural documentation provided by the entity under review.
12-6 Any other SCD loaded with the same key components must combine all entered key components using the identical process.	**12-6** Through examination of documented procedures, interviews, and observation, confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key,
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.	**12-7.a** Examine documented procedures for the loading of TMKs to verify that they require asymmetric key-loading techniques or manual techniques for initial loading. **12-7.b** Examine documented procedures to verify that keys are prohibited from reloading or reuse wherever suspected of being compromised and are 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.	**12-8.a** For techniques involving public key cryptography, examine documentation and develop a schematic to illustrate the process, including the size and sources of the parameters involved, and the mechanisms utilized for mutual device authentication for both the host and the POI. **12-8.b** If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that the remote key distribution requirements detailed in Annex A of this document are met, including: • Use of 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 of key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question. • Providing for mutual device authentication for both the host and the POI device or host-to-host if applicable.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**12-9.a** Examine documented key-injection procedures to verify that the procedures define use of dual control and split knowledge controls for the loading of keys into devices. **12-9.b** Interview responsible personnel and observe key-loading processes and controls to verify that dual control and split-knowledge controls are in place for the loading of keys into devices. **12-9.c** Examine records of key-loading processes and controls to verify that the loading of keys does not occur without dual control and split knowledge.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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., BDKs, TMKs) 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.*

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-1** Observe key-loading environments, processes, and mechanisms (for example, terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following: • Ensure that any cameras that are present are positioned to ensure they cannot monitor the entering of clear-text key components. • Review documented procedures to determine that they require that keys and components are transferred into an SCD only after an inspection of the devices and mechanism; and verify they are followed by observing a demonstration that: o SCDs must be inspected to detect evidence of monitoring and to ensure dual-control procedures are not circumvented during key loading. o An SCD must transfer a plaintext secret or private key only when at least two authorized individuals are identified by the device. o There is not any mechanism (including cabling) at the interface between the conveyance medium and the SCD device that might disclose the transferred keys. o The SCD is inspected to ensure it has not been subject to any prior tampering that could lead to the disclosure of clear-text keying material.
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.	**13-2** Verify that only SCDs are 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 keyboards shall never be used for the loading of clear-text secret or private keys or their components.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-3** Examine documented procedures for the loading of secret or private key components from an electronic medium to a cryptographic device. Verify that procedures define specific instructions to be followed as a result of key loading, including: • Instructions for the medium to be 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 • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.
	13-3 Observe key-loading processes to verify that the loading process results in one of the following: • The medium used for key loading 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.
13-4 For secret or private keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:	**13-4** Review documented procedures and observe processes for the use of key-loading devices. Perform the following:
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.	**13-4.1** Verify the key-loading device is 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.	**13-4.2** Verify the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-4.3.a** Verify the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD.
	13-4.3.b Verify that authorized personnel inspect the key-loading device prior to use to ensure that a key-recording device has not been 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.	**13-4.4** Verify the key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred. For example, attempt to output the same value more than one time from the device or cause the device to display check values for its contents both before and after injection and compare.
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.	**13-5.a** Interview personnel and observe media locations to verify that the media is maintained in a secure storage location accessible only to custodian(s) authorized to access the key components.
	13-5.b Examine documented procedures for removing media or devices containing key components—or that are otherwise used for the injection of cryptographic keys—from the secure storage location. Verify procedures include the following: • Requirement that media/devices are in the physical possession of only the designated component holder(s). • The media/devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.
	13-5.c Interview designated component holder(s) and examine key-management logs to verify that media or devices removed from secure storage are in the physical possession of only the designated component holder.
	13-5.d Interview key-injection personnel and examine logs for the removal of media/devices from secure storage to verify they are removed only for the minimum practical time necessary to complete the key-loading process.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-6** Validate through interview and observation that printed key components are not opened until just prior to entry into the SCD/KLD. Plaintext secret and/or private keys and/or their components are visible only to key custodians for the duration of loading into an SCD/KLD.
13-7 Written or printed key-component documents must not be opened until immediately prior to use.	**13-7.a** Review documented procedures and confirm that printed/written key-component documents are not opened until immediately prior to use.
	13-7.b Observe key-loading processes and verify that printed/written key components are not 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.*	**13-8.a** Examine documented procedures for the use of key components to verify that procedures ensure that any individual custodian only has access to their assigned components and never has access to sufficient key components to reconstruct a cryptographic key.
	13-8.b Examine key-component access controls and access logs to verify that any single authorized custodians can only access their assigned component(s) and cannot access sufficient key components to reconstruct a cryptographic key.
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:	**13-9** Interview appropriate personnel and review documentation to determine the procedures for key loading to POIs, key-loading devices, and HSMs that are part of the key-loading platform. Review any logs of key loading.
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.	**13-9.1** For facilities using PC-based key-loading software platforms or similar devices, verify through interviews and observation that the platform is: • Standalone • Dedicated to only key loading • Located in a physically secure room that is dedicated to key loading activities

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**13-9.2** Verify through interviews and observation that: • All hardware used in key loading (including the PC) is managed under dual control. • Key-injection cannot occur unless there are minimally two individuals in the key-injection room at all times during the process. • Mechanisms exist (See Requirement 32) that do not permit the room to be occupied by fewer than two authorized individuals.
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.	**13-9.3.a** Verify through interviews and observation that logs of key-loading activities are maintained and meet the following: • Retained for a minimum of three years. • Regularly reviewed by an authorized person who does not have access to the room or to the PC. • The reviews are documented.
	13-9.3.b Verify through interviews and observation that logs of key-loading activities are maintained and meet the following: • Retained for a minimum of three years. • Regularly reviewed by an authorized person who does not have access to the room or to the PC. • The reviews are documented. • Logs include a minimum of: o Access to the room from a badge access system, o Access to the room from a manual sign-in sheet, o User sign-on logs on the PC at the operating system level, o User sign-on logs on the PC at the application level, o Logs of the device IDs and serial numbers that are loaded along with the date and time and the individuals performing the key-injection, o Video surveillance logs with a minimum retention period of 45 days.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
13-9.4 Additionally:	**13-9.2** Verify through interviews and observation that:
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.	**13-9.4.1** Cable attachments and the key-loading device are 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.	**13-9.4.2** The key-loading device is 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.	**13-9.4.3** The software application loads 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.	**13-9.4.4** Clear-text keys are not 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.	**13-9.4.5** Personnel responsible for the systems administration of the PC do not have authorized access into the room—i.e., they are escorted by authorized key-injection personnel—and do 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.	**13-9.4.6** Key-injection personnel do 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.	**13-9.4.7** The PC is not able to boot from external media (e.g., USB devices or CDs). It must boot from the hard drive only.
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.	**13-9.4.8** All openings on the PC that are not used for key-injection are covered with security seals that are tamper-evident and serialized. The seals are recorded in a log, and the log is 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.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**13-9.4.9** If the PC application stores keys (e.g., BDKs or TMKs) on portable electronic media (e.g., smart cards), the media is secured as components under dual control when not in use. The key components are manually entered at the start of each key-injection session from components that are maintained under dual control and split knowledge.
13-9.4.10 Manufacturer's default passwords for PC-based applications must be changed.	**13-9.4.10** Manufacturer's default passwords for PC-based applications are 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.	**14-1.a** Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. • Any resources (e.g., passwords and associated hardware) used in the key-loading function must be controlled and managed such that no single individual has the capability to enable key loading.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	14-1.b Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function is controlled and maintained in a secure environment under dual control. • All resources (e.g., passwords and associated hardware) used for key-loading functions are controlled and managed such that no single individual has the capability to enable key loading.
14-2 All cable attachments must be examined before each key-loading operation to ensure they have not been tampered with or compromised.	**14-2.a** Review documented procedures to ensure they require that cable attachments be examined prior to key-loading function.
	14-2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to a key-loading function.
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.	**14-3.a** Observe key-loading activities to verify that key-loading equipment usage is monitored.
	14-3.b Verify logs of all key-loading activities are maintained and contain all required information.
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-	**14-4.a** Examine documented procedures for the use of physical tokens (e.g., brass keys or chip cards) to enable key loading. Verify procedures require that physical tokens 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.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	14-4.b Inspect locations and controls for physical tokens to verify that tokens used to enable key loading are not in the control or possession of any one individual who could use those tokens to load secret or private cryptographic keys under single control.
	14-4.c Review storage locations for physical tokens to determine adequacy to ensure that only the authorized custodian(s) can access their specific tokens.
	14-4.d Verify that access-control logs exist and are in use.
	14-4.e Reconcile storage contents to access-control logs.
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.	**14-5.a** Verify that documented procedures require default passwords or PINs used to enforce dual control are changed.
	14-5.b Verify that documented procedures exist to require that these passwords/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 is 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	**15-1.a** Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and/or components.

Control Objective 4: Key-loading to hosts and PIN entry devices is handled in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	15-1.b Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used and are verified by the applicable key custodians.
	15-1.c Verify that the methods used for key validation are consistent with ISO 11568—for example, if check values are used, they should return a value of no more than six hexadecimal characters.
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.	**15-2.a** Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.
	15-2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.
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.	**16-1.a** Verify documented procedures exist for all key-loading operations.
	16-1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.
	16-1.c Observe key-loading process for keys loaded as components and verify that the documented procedures are demonstrably in use. This may be done as necessary on test equipment—e.g., for HSMs.
16-2 All key-loading events must be documented. Audit trails must be in place for all key-loading events.	**16-2** Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**18-2.a** Verify documented procedures require that key-component packaging/containers showing signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.
	18-2.b Interview personnel and observe processes to verify procedures are implemented to require that key-component packaging/containers showing signs of tampering result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) 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.	**18-3** Examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key blocks using mechanisms that cryptographically bind the key usage to the key at all times via one of the acceptable methods or an equivalent.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.*	**18-4.a** Examine documented key-injection procedures to verify that controls are defined to prevent and detect the loading of keys by any one single person. **18-4.b** Interview responsible personnel and observe key-loading processes and controls to verify that controls—for example, viewing CCTV images—are implemented to prevent and detect the loading of keys by any one single person.
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.	**18-5.a** Examine documented procedures to verify they include: • Controls to protect against unauthorized substitution of keys, and • Controls to prevent the operation of devices without legitimate keys. **18-5.b** Interview responsible personnel and observe key-loading processes and controls to verify that: • Controls are implemented that protect against unauthorized substitution of keys, and • Controls are implemented that prevent the operation of devices without legitimate keys.
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.*	

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**19-1.a** Examine key-management documentation (e.g., the cryptographic key inventory) and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are defined for a specific purpose.
	19-1.b Using a sample of device types, validate via review of check values, terminal definition files, etc. that keys used for key encipherment or PIN encipherment are not used for any other purpose.
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.	**19-2** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that private keys are only used: • To create digital signatures or to perform decryption operations. • For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for POI devices). • Private keys are never 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).	**19-3** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that public keys are only used: • To perform encryption operations or to verify digital signatures. • For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for POI devices).

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**19-4.a** Examine key-management documentation and interview key custodians and key-management supervisory personnel to verify that cryptographic keys are never shared or substituted between production and development systems.
	19-4.b Observe processes for generating and loading keys into in production systems to ensure that they are in no way associated with test or development keys.
	19-4.c Observe processes for generating and loading keys into test systems to ensure that they are in no way associated with production keys.
	19-4.d Compare check, hash, cryptogram, or fingerprint values for production and test/development keys for higher-level keys (e.g., MFKs, KEKs shared with other network nodes, and BDKs) to verify that development and test keys have different key values.
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.*	**19-5** Interview personnel to determine whether production platforms are ever temporarily used for purposes other than processing of production transactions. If they are, verify that documented procedures require that: • All keying material is deleted from the HSM(s) and the server /computer platforms prior to testing. • Subsequent to completion of testing, all keying materials must be deleted and the server/computer platforms must be wiped and rebuilt from read-only media, • Prior to reuse for production purposes the HSM is returned to factory state, • The relevant production keying material is restored using the principles of dual control and split knowledge as stated in these requirements.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**20-1.a** Examine documented procedures for the generation, loading, and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all private and secret keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to HSMs at the minimum number of facilities consistent with effective system operations.
	20-1.b Observe HSM functions and procedures for generating and loading secret and private keys for use in transaction-originating POIs to verify that unique keys are generated and used for each POI device.
	20-1.c Examine check values, hashes, or fingerprint values for a sample of cryptographic keys from different POI devices to verify private and secret keys are unique for each POI device. This can include comparing a sample of POI public keys (multiple devices for each POI vendor used) to determine that the associated private keys stored in the POI devices are unique per device—i.e., the public keys are unique.
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.	**20-2** Determine whether any transaction-originating terminals are intended to interface with multiple acquiring organizations. If so: • Examine documented procedures for generating all types of keys and verify the procedures ensure that unique keys, or sets of keys, are used for each acquiring organization and are totally independent and not variants of one another. • Interview personnel and observe key-generation processes to verify that unique keys or sets of keys are generated for each acquiring organization.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
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.	**20-3.a** Examine documented procedures and observe processes for generating master keys. Verify the following is implemented where master keys are generated by a derivation process and derived from the same Base Derivation Key: • Unique data is used for the derivation process such that all transaction-originating POIs receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.
	20-3.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.
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 BDKs for each financial institution • Different BDKs by injection vendor (e.g., ESO), terminal manufacturer, or terminal model	**20-4.a** Examine documented key-generation and injection procedures to verify that the following is required when injecting keys into a single POI for more than one acquiring organization: • The POI 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.

Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.	
PIN Security Requirements	**Testing Procedures**
	20-4.b Observe processes for generation and injection of keys into a single POI for more than one acquiring organization, to verify: • The POI has a completely different and unique key, or set of keys, for each acquiring organization. • These different keys, or sets of keys, are totally independent and not variants of one another.
20-5 Key-injection facilities that load DUKPT keys for various POI types for the same entity must use separate BDKs per terminal type if the terminal IDs can be duplicated among the multiple types of terminals. In other words, the key-injection facility must ensure that any one given key cannot be derived for multiple devices except by chance.	**20-5.a** If the key-injection facility loads DUKPT keys, examine documented procedures for generation and use of BDKs to verify they require use of separate BDKs per terminal type.
	20-5.b Observe key-loading processes for a sample of terminal types used by a single entity, to verify that separate BDKs are used for each terminal type.
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).	**20-6.a** For techniques involving public key cryptography, examine documentation and develop a schematic to illustrate the process, including: • The size and sources of the parameters involved, and • The mechanisms utilized for mutual device authentication for both the host and the POIPED.
	20-6.b If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that: • Cryptographic mechanisms exist to uniquely identify the keys. • Key pairs used by POI devices are unique per device.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	
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	**21-1.a** Examine documented procedures for key storage and usage and observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored. **21-1.b** Observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.
21-2 Wherever key components are used, they have the following properties:	**21-2** Examine documented procedures and interview responsible personnel to determine all instances where key components are used.
21-2.1 Knowledge of any one key component/share does not convey any knowledge of any part of the actual cryptographic key.	**21-2.1** Review processes for creating key components to verify that knowledge of any one key component 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.	**21-2.2** Observe processes for constructing cryptographic keys to verify that at least two key components are required for each key construction.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
21-2.3 Each key component/share has one or more specified authorized custodians.	**21-2.3.a** Examine documented procedures for the use of key components and interview key custodians and key-management supervisory personnel to verify that each key component is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component.
	21-2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components are designated as key custodians for those particular components.
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.*	**21-2.4.a** Examine documented procedures for the use of key components to verify that procedures ensure that any custodian never has access to sufficient key components to reconstruct a cryptographic key.
	21-2.4.b Examine key-component access controls and access logs to verify that authorized custodians cannot access sufficient key components to reconstruct a cryptographic key.
21-3 Key components must be stored as follows:	**21-3** Examine documented procedures, interview responsible personnel and inspect key-component storage locations to verify that key components are stored as follows:

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**21-3.1.a** Examine key components and storage locations to verify that components are stored in opaque, pre-numbered tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging.
	21-3.1.b Inspect any tamper-evident packaging used to secure key components and ensure that it prevents the determination of the key component without visible damage to the packaging.
	21-3.1.c Interview responsible personnel to determine that clear-text key components do not exist in any other locations, including in non-secure containers, in databases, on floppy disks, or in software programs.
	21-3.1.d Confirm that start-up instructions and other notes used by service technicians do not contain initialization-key values written in the clear (e.g., at the point in the checklist where the keys are entered).
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.*	**21-3.2** Inspect each key component storage container and verify the following: • Key components for different custodians are stored in separate secure containers. • Each secure container is accessible only by the custodian and/or designated backup(s).
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.	**21-3.3** Interview responsible personnel and observe implemented processes to verify that if a key is stored on a token, and an access code (PIN or similar mechanism) is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its access code.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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** Verify documented procedures exist for replacing known or suspected compromised keys that include all of 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.	**22-1.1** Interview responsible personnel and observe implemented processes to verify 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.	**22-1.2** Interview responsible personnel and observe implemented processes to verify that 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.*	**22-1.3** Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, an assessment and analysis is performed. If compromise is confirmed, all the following are performed: • Processing with that key is halted, and the key is replaced with a new unique key. • Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. • The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**22-1.4.a** Interview responsible personnel and review documented procedures to verify key personnel are identified and that the escalation process includes notification to organizations that currently share or have previously shared the key(s).
	22-1.4.b Verify notifications include the following: • A damage assessment including, where necessary, the engagement of outside consultants. • Details of 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	**22-1.5** Interview responsible personnel and review documented procedures to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: • Missing SCDs • 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 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	**22-2** Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into a KLD or POI fail, the same key or component is not 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.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**23-1.a** Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods. **23-1.b** Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.
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.	**23-2.a** Interview responsible personnel to determine which host MFKs keys exist as variants. ***Note:*** *Some HSMs may automatically generate variants or control vectors for specific keys, but it is still up to the entity to specify exact usage.* **23-2.b** Review vendor documentation to determine support for key variants. **23-2.c** Via review of the network schematic detailing transaction flows with the associated key usage and identification of the sources of the keys used, determine that variants of the MFK are not used external to the logical configuration that houses the MFK.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.*	**23-3** Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Variants used as KEKs must only be calculated from other key-encrypting keys. • Variants of working keys must only be calculated from other working 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.	**24-1.a** Verify documented procedures are in place for destroying secret or private keys, and their key components that are no longer used or that have been replaced by a new key.
	24-1.b Identify a sample of keys and key components that are no longer used or have been replaced. For each item in the sample, interview responsible personnel and examine key-history logs and key-destruction logs to verify that all keys have been destroyed.
	24-1.c Review storage locations for the sample of destroyed keys to verify they are no longer kept.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.
	24-2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.
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.*	**24-2.1.a** Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.
	24-2.1.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms—physically secured, enciphered, or components—are destroyed following the procedures outlined in ISO–9564 or ISO–11568.
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.	**24-2.2.a** Observe the key-destruction process and verify that it is witnessed by a third party other than a key custodian for any component of that key.
	24-2.2.b Inspect key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key destruction process.
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.	**24-2.3.a** Verify documented procedures exist for destroying key components of keys, once the keys are successfully loaded and validated as operational.
	24-2.3.b Observe key-conveyance/loading processes to verify that any key components are destroyed once the keys are successfully loaded and validated as operational.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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** Interview key custodians and key-management supervisory personnel and observe implemented processes to verify the following:
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	**25-1.1** Review key-custodian assignments for each component to verify that: • A primary and a backup key custodian are designated for each component. • The fewest number of key custodians is assigned as necessary to enable effective key management. • Assigned key custodians are employees or contracted personnel
25-1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form.	**25-1.2.a** Examine completed key-custodian forms to verify that key custodians sign the form.
	25-1.2.b Examine completed key-custodian forms to verify that backup custodians sign the 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	**25-1.3** Examine all key-custodian forms to verify that they include 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.	
PIN Security Requirements	**Testing Procedures**
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.	**25-1.4.a** Examine key-custodian assignments and organization charts to confirm the following: • Key custodians that form the necessary threshold to create a key do not directly report to the same individual. • Neither direct reports nor the direct reports in combination with their immediate supervisor possess the necessary threshold of key components sufficient to form any given key. **25-1.4.b** For organizations that are such a small, modest size that they cannot support the reporting-structure requirement, ensure that documented procedures exist and are followed to: • Ensure key custodians do not report to each other. • Receive explicit training to instruct them from sharing key components with their direct manager. • Sign key-custodian agreement that includes an attestation to the requirement. • Ensure training includes whistleblower procedures to report any violations.
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. *(continued on next page)*	**26-1.a** Review log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
26-1 *(continued)* 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)	**26-1.b** Review log files and audit log settings to verify that logs 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.	**27-1** Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following: • Observe backup processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the primary keys. • Inspect backup storage locations and access controls or otherwise verify through examination of documented procedures and interviews of personnel that backups are maintained as follows: o Securely stored with proper access controls o Under at least dual control o Subject to at least the same level of security control as operational keys as specified in this document
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.	**27-2** Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies requires at least 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.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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	**28-1.a** Examine documented procedures for key-administration operations to verify they include: • 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
	28-1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.
	28-1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.
	28-1.d Interview responsible HR personnel to verify background checks are conducted (within the constraints of local laws).
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.a** Review documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
	29-1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or code signing have not been substituted or subjected to unauthorized modifications or tampering.
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** Review documented procedures to verify controls are defined to protect POIs and other SCDs from unauthorized access up to point of deployment.
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.	**29-1.1.1.a** Examine access-control documentation and device configurations to verify that access to all POIs and key-injection/loading devices is defined and documented.
	29-1.1.1.b For a sample of POIs and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POIs and other SCDs is logged.
	29-1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI or other SCD.
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.	**29-1.1.2** Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys or passwords are not used.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**29-1.1.3.a** Examine documented authorizations for personnel with access to devices to verify that prior to deployment: • All personnel with access to POIs and other SCDs are documented in a formal list. • All personnel with access to POIs and other SCDs are authorized by management. • The authorizations are reviewed annually.
	29-1.1.3.b For a sample of POIs and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in the formal list have access to devices.
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.	**29-2.a** Examine documented processes to verify that the chain of custody is required for devices from receipt to placement into service.
	29-2.b For a sample of devices, review documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to placement into service.
	29-2.c Verify that the chain-of-custody records identify responsible personnel for each interaction with the device

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.)* o 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.) o Controls exist and are in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.	**29-3.a** Examine documented procedures to confirm that they require physical protection of devices from the manufacturer's facility up to the point of key-insertion and deployment, through one or more of the defined methods. **29-3.b** Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion and deployment.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.a** Examine documented procedures to confirm that dual-control mechanisms exist to prevent substitution or tampering of HSMs—both deployed and spare or back-up devices—throughout their life cycle.
	29-4.b Interview responsible personnel and physically verify the dual-control mechanism used to prevent substitution or tampering of HSMs—both in-service and spare or back-up devices—throughout their life cycle.
	29-4.c Determine the adequacy of those controls in enforcing dual control.
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*	**29-4.1.a** Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.
	29-4.1.b For a sample of received devices, review sender documentation sent via a different communication channel than the devices shipment (for example, the manufacturer's invoice or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial number for the received device was verified to match that documented by the sender.
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.**	**29-4.2.a** Obtain and review the defined security policy to be enforced by the HSM
	29-4.2.b Examine documentation of the HSM configuration settings to determine that the functions and command authorized to be enabled are in accordance with the security policy.
	29-4.2.c For a sample of HSMs, review the configuration settings to determine that only authorized functions are enabled.
	29-4.2.d Verify that PIN-change functionality, PIN-block format translation functionality, or non-ISO PIN-block formats are not supported without a defined documented and approved business need.
	29-4.2.e Verify that functionality is not enabled to allow the outputting of clear text PINs.

Control Objective 6: Keys are administered in a secure manner.	
PIN Security Requirements	**Testing Procedures**
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.	**29-4.3** Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.
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** Examine documented procedures to verify they require inspection and testing of HSMs prior to installation to verify integrity of device.
29-4.4.1 Running self-tests to ensure the correct operation of the device	**29-4.4.1** Examine records of device inspections and test results to verify that self-tests are run on devices 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	**29-4.4.2** Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, 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	**29-4.4.3** Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify 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	**29-4.4.4.a** Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.
	29-4.4.4.b Examine records of inspections to verify records are retained for at least one year.
29-5 Maintain HSMs in tamper-evident packaging or in secure storage until ready for installation.	**29-5.a** Examine documented procedures to verify they require devices be maintained in tamper-evident packaging until ready for installation.
	29-5.b Observe a sample of received devices to verify they are maintained in tamper-evident packaging until ready for installation.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.*	**30.3.a** Obtain and review documentation of inventory control and monitoring procedures. Determine that the procedures cover: • Each production run is associated with a predefined inventory of identified POI devices to be injected or initialized with keys. • Unauthorized personnel are not able to modify this inventory without detection. • All POI devices to be initialized with keys on a production run are identified and accounted for against the inventory. • Unauthorized POI devices submitted for injection or initialized are rejected by the injection platform and investigated. • Once processed by the KIF, whether successfully initialized with keys or not, all submitted POI devices are identified and accounted for against the inventory. **30.3.b** Interview applicable personnel to determine that procedures are known and followed.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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** Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all keys and key material stored within the device be securely destroyed. • Procedures cover all devices removed from service or for repair.
31-1.1 HSMs require dual control (e.g., to invoke the system menu) to implement for all critical decommissioning processes.	**31-1.1.a** Review documented procedures for removing HSM from service to verify that dual control is implemented for all critical decommissioning processes.
	31-1.1.b Interview personnel and observe demonstration (if HSM is available) of processes for removing HSM from service to verify that dual control is implemented 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.	**31-1.2** Interview personnel and observe demonstration of processes for removing SCDs from service to verify that all keying material is rendered irrecoverable (for example, zeroized), or that devices are 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.	
PIN Security Requirements	**Testing Procedure**
31-1.3 SCDs being decommissioned are tested and inspected to ensure keys have been rendered irrecoverable.	**31-1.3** Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.
31-1.4 Affected entities are notified before devices are returned.	**31-1.4** Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.
31-1.5 Devices are tracked during the return process.	**31-1.5** Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.
31-1.6 Records of the tests and inspections maintained for at least one year.	**31-1.6** Interview personnel and observe records to verify that 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*	
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** Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.*	**32-1.1** Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.
32-1.2 Passwords used for dual control must each be of at least five numeric and/or alphabetic characters.	**32-1.2** Observe password policies and configuration settings to confirm that passwords used for dual control must be 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	**32-1.3** Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is 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 KLDs
32-1.4 Devices must not use default passwords.	**32-1.4.a** Examine password policies and documented procedures to confirm default passwords must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys.
	32-1.4.b Observe device configurations and interview device administrators to verify that HSMs, KLDs, and other SCDs used to generate or load cryptographic keys do not use default passwords.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.*	**32-1.5.a** Examine documented procedures to confirm that they require devices are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
	32-1.5.b Interview responsible personnel and observe devices and processes to confirm that devices are either: • Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or • Under the continuous supervision of at least two authorized people at all times.
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.	**32-9.1.a** Examine documented procedures for key conveyance or transmittal to verify that keys used between KIF components are addressed in accordance with applicable criteria in Control Objective 3.
	32-9.1.b Interview responsible personnel and observe conveyance processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.
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.	**32-9.2** Examine documented procedures to confirm they specify the establishment of a channel for mutual authentication of the sending and receiving devices.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.	**32-9.4.a** Examine documented procedures for key loading to hosts and POI devices to verify that they are in accordance with applicable criteria in Control Objective 4.
	32-9.4.a Interview responsible personnel and observe key-loading processes to verify that the documented procedures are followed for key conveyance or transmittal for keys used between KIF components.
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.	**32-9.5** Examine documented procedures to confirm they specify the establishment of a mutually authenticated channel for establishment of enciphered secret or private keys between sending and receiving devices—e.g., POI devices and HSMs.
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.	**32-9.6** Interview responsible personnel and observe processes for establishment of enciphered secret or private keys between sending and receiving devices to verify: • KIFs validate authentication credentials of a POI prior to any key transport, exchange, or establishment with that device. • POI devices validate authentication credentials of KLDs 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 is not 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.	**32-9.7** Examine documented procedures to confirm they define mechanisms to prevent an unauthorized host from performing key transport, key exchange, or key establishment with POIs.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.	**32-10.1** Inspect the secure area designated for key injection to verify that it is constructed with 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.	**32-10.2.a** Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.
	32-10.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.
32-10.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	**32-10.3** Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.
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.	**32-10.4** Inspect the secure area to verify that it is only accessed through a solid-core or a steel door, with door hinges that 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.	**32-10.5** Observe authorized personnel entering the secure area to verify that a badge-control system is in place that enforces the following requirements: • Dual-access for entry to the secure area • Anti-pass-back
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.*	**32-10.6** Examine alarm mechanisms and interview alarm-response personnel to verify that the badge-control system supports generation of an alarm when one person remains alone in the secure area for more than 30 seconds.

Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.	
PIN Security Requirements	**Testing Procedure**
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.	**32-10.7** Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a 24/7 basis.
32-10.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	**32-10.8** Inspect configuration of monitoring systems and interview monitoring personnel to verify that monitoring is supported on a continuous (24/7) basis and 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.	**32-10.9.a** Inspect location of the CCTV server and digital-storage to verify they are located in a secure area that is separate from the key-injection area.
	32-10.9.b Inspect access-control configurations for the CCTV server/storage area and the key-injection area to identify all personnel who have access to each area. Compare access lists to verify that personnel with access to the key-injection area do not have access to the CCTV server/storage 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.	**32-10.10** Inspect CCTV positioning and review a sample of recordings to verify that CCTV cameras are 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.	**32-10.11** Inspect CCTV positioning and review a sample of recordings to verify that CCTV cameras 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.	
PIN Security Requirements	**Testing Procedure**
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.	**33-1.a** Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for devices placed into service, initialized, deployed, used, and decommissioned,
	33-1.b Verify that written records exist for the tests and inspections performed 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:[2]

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 TDEA (§)	1024	160	1024/160
112	Double-length TDEA (§) 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 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.

[2] 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.

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.

Data Encryption Algorithm (DEA) refers to Triple DEA (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
Access controls	Controls to ensure that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
Acquirer	The institution (or its agent) that receives from a card acceptor the data relating to financial transactions with PINs. The acquirer is the entity that forwards the financial transaction into an interchange system.
Advanced Encryption Algorithm (AES)	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
ANSI	American National Standards Institute, a U.S. standards accreditation organization.
Asymmetric cryptography (techniques)	See *Public-key cryptography*.
ATM	Automated teller machine. An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks.
Authentication	The process for establishing unambiguously the identity of an entity, process, organization or person.
Authorization	The right granted to a user to access an object, resource or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource or function.
Authorized key custodian	Having a signed key-custodian agreement and a written authorization for the specific operation.
Base (master) Derivation Key (BDK)	See *Derivation key.*
Cardholder	An individual to whom a card is issued or who is authorized to use the card.
Card issuer	The institution or its agent that issues the payment card to the cardholder.
Certificate	For purposes of these requirements, a certificate is any digitally signed value containing a public key.

Term	Definition
Certificate revocation	The process of revoking an otherwise valid certificate by the entity that issued that certificate. Revoked certificates are placed on a certificate revocation list (CRL) or the information is conveyed using OCSP as specified in the product/service specification.
Certificate Revocation List (CRL)	A list of revoked certificates. Entities that generate, maintain, and distribute CRLs can include, for example, the root or subordinate CAs.
Certification authority (CA)	For purposes of these requirements, a certification authority is any entity signing public keys, whether in X.509 certificate based schemes or other designs for use in connection with the remote distribution of symmetric keys using asymmetric techniques.
Check value	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key must not be feasible.
Cipher text	Data in its enciphered form.
Clear text	See *Plaintext.*
Communicating nodes	Two entities (usually institutions) sending and receiving transactions. This is to include alternate processing sites either owned or contracted by either communicating entity.
Compromise	In cryptography, the breaching of secrecy and/or security—a violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).
Computationally infeasible	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it.
Credentials	Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key.
Critical security parameters (CSP)	Security-related information (e.g., cryptographic keys 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.
Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Term	Definition
Cryptographic key	A parameter used in conjunction with a cryptographic algorithm that determines: • The transformation of plaintext data into ciphertext data, • The transformation of ciphertext data into plaintext data, • A digital signature computed from data, • The verification of a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret.
Cryptographic key component	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.
Customers	Customers are financial institutions that: • Offer payment cards for one or more of the participating payment brands (issuers); • Accept such payment cards for cash disbursement and directly or indirectly enter the resulting transaction receipt into interchange (acquirers); or • 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).
Data Encryption Algorithm (DEA)	A published encryption algorithm used to protect critical information by enciphering data based upon a variable secret key. The Data Encryption Algorithm is defined in ANSI X3.92: Data Encryption Algorithm for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity-checking to ensure that the key is transmitted properly.
Decipher	See *Decrypt*.
Decrypt	A process of transforming cipher text (unreadable) into plain text (readable).

Term	Definition
Derivation key	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the Derived Unique Key Per Transaction key-management method. Derivation keys are normally used in a transaction-receiving (e.g., acquirer) SCD in a one-to-many relationship to derive or decrypt the transaction keys (the derived keys) used by a large number of originating (e.g., terminals) SCDs.
DES	Data Encryption Standard (see *Data Encryption Algorithm*). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the Data Encryption Algorithm.
Digital signature	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.
Double-length key	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDEA cryptographic algorithm.
Dual control	A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. No single person can gain control of a protected item or process. Also see *Split knowledge*.
DUKPT (Derived Unique Key Per Transaction)	A key-management method that uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction-originating TRSM. The unique transaction keys are derived from a Base Derivation Key using only non-secret data transmitted as part of each transaction.
ECB	Electronic codebook.
Electronic code book (ECB) operation	A mode of encryption using the data encryption algorithm, in which each block of data is enciphered or deciphered without using an initial chaining vector or previously (encrypted) data blocks.
EEPROM	Electronically erasable programmable read-only memory.
Electronic key entry	The entry of cryptographic keys into a secure cryptographic device in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.

Term	Definition
Encipher	See *Encrypt*.
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.
Encrypting PIN pad (EPP)	A device for secure PIN entry and encryption in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (e.g., an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell. Encrypting PIN pads require integration into UPTs or ATMs.
EPROM	Erasable programmable read-only memory.
Exclusive-OR	Binary addition without carry, also known as “modulo 2 addition,” symbolized as “XOR” and defined as: • 0 + 0 = 0 • 0 + 1 = 1 • 1 + 0 = 1 • 1 + 1 = 0
FIPS	Federal Information Processing Standard.
Firmware	The programs and data (i.e., software) permanently stored in hardware (e.g., in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.
Hardware (host) security module	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
Hash	A (mathematical) function that is a non-secret algorithm, which takes any arbitrary-length message as input and produces a fixed-length hash result. Approved hash functions satisfy the following properties: 1) One-Way – It is computationally infeasible to find any input that maps to any pre-specified output. 2) Collision Resistant – It is computationally infeasible to find any two distinct inputs (e.g., messages) that map to the same output. It may be used to reduce a potentially long message into a "hash value" or "message digest" 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.
Hexadecimal character	A single character in the range 0–9, A-F (upper case), representing a four-bit string.
Initialization vector	A binary vector used as the input to initialize the algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
Integrity	Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Interchange	The exchange of clearing records between financial institution customers.
Interface	A logical section of a cryptographic device that defines a set of entry or exit points that provide access to the device, including information flow or physical access.
Irreversible transformation	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.
ISO	International Organization for Standardization. An international standards setting organization composed of representatives from various national standards organizations.
Issuer	The institution holding the account identified by the primary account number (PAN).
Key	See *Cryptographic key.*
Key agreement	A key-establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.

Term	Definition
Key backup	Storage of a protected copy of a key during its operational use.
Key bundle	The three cryptographic keys (K1, K2, K3) used with a TDEA mode. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle must never be used separately for any other purpose.
Key component	See *Cryptographic key component*.
Key derivation process	A process, which derives one or more session keys from a shared secret and (possibly) other public information.
Key destruction	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.
Key-distribution host (KDH)	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to the EPP or PED and the financial processing platform communicating with those EPPs/PEDs. A KDH may be an application that operates on the same platform that is used for PIN translation and financial transaction processing. The KDH may be used in conjunction with other processing activities. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys.
Key-encrypting (encipherment or exchange) key	A cryptographic key that is used for the encryption or decryption of other keys.
Key establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generation	Creation of a new key for subsequent use.
Key instance	The occurrence of a key in one of its permissible forms, i.e., plaintext key, key components, enciphered key.
Key-loading	Process by which a key is manually or electronically transferred into a secure cryptographic device.
Key-loading device (KLD)	An SCD that may be used to perform cryptographic injection/loading or code signing.
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving.
Key pair	A key pair comprises the two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is known only to the appropriate entities.

Term	Definition
Key replacement	Substituting one key for another when the original key is known or suspected to be compromised, or the end of its operational life is reached.
Key (secret) share	One of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that less than a quorum does not provide any information about the key.
Key storage	Holding of the key in one of the permissible forms.
Key transport	A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.
Key usage	Employment of a key for the cryptographic purpose for which it was intended.
Key variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Keying material	The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships.
Local Master Key (LMK)	See *Master File Key*.
Manual key-loading	The entry of cryptographic keys into a secure cryptographic device from a printed form, using devices such as buttons, thumb wheels, or a keyboard.
Master derivation key (MDK)	See *Derivation key.*
Master File Key (MFK)	This is a symmetric key used to encrypt other cryptographic keys which are to be stored outside of the Hardware Security Module (HSM).
Master key	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a master key. 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.
Message	A communication containing one or more transactions or related information.
Node	Any point in a network that does some form of data processing, such as a terminal, acquirer, or switch.
Non-reversible transformation	See *Irreversible transformation*.

Term	Definition
Online Certificate Status Protocol (OCSP)	The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
Offline PIN verification	A process used to verify the cardholder's identity by comparing the PIN entered at the chip-reading device to the PIN value contained in the chip.
Online PIN verification	A process used to verify the cardholder's identity by sending an encrypted PIN value to the issuer for validation in an authorization request.
Out-of-band notification	Notification using a communication means independent of the primary communications means.
PAN	Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Password	A string of characters used to authenticate an identity or to verify access authorization.
Personal identification number (PIN)	A numeric personal identification code that authenticates a cardholder in an authorization request originating at a terminal with authorization-only or data-capture-only capability. A PIN consists only of decimal digits.
Physical protection	The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.
Physically secure environment	An environment equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or purpose-built room with continuous access control, physical security protection, and monitoring.
PIN	See *Personal identification number.*
PIN-encipherment key (PEK)	A PEK is a cryptographic key that is used for the encryption or decryption of PINs.
PIN entry device (PED)	A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor, and storage for PIN processing sufficiently secure for the key-management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell and is a complete terminal that can be provided to a merchant “as is” to undertake PIN-related transactions. This may include either attended or unattended POS POI terminals.

Term	Definition
PIN pad	See *PIN entry device*.
Plain text	Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as clear text.
Plaintext key	An unencrypted cryptographic key, which is used in its current form.
Point of interaction (POI)	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.
Private key	A cryptographic key, used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.
PROM	Programmable read-only memory.
Pseudo-random	A value that is statistically random and essentially random and unpredictable although generated by an algorithm.
Public key	A cryptographic key, used with a public-key cryptographic algorithm, uniquely associated with an entity, and that may be made public. In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Term	Definition
Public key (asymmetric) cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key-agreement system. With asymmetric cryptographic techniques, 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.
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware-based “noise” mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
Registration authority (RA)	An entity that performs registration services on behalf of a certification authority (CA). Registration authorities (RAs) work with a particular certification authority (CA) to vet requests for certificates that will then be issued by the certification authority.
ROM	Read-only memory.
Root certification authority (RCA)	The RCA is the top-level certification authority in a public key infrastructure. 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.
Secret key	A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. A secret key (symmetrical) cryptographic algorithm uses a single secret key for both encryption and decryption. The use of the term “secret” in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.
Secure cryptographic device (SCD)	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.

Term	Definition
Sensitive data	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.
Session key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys—e.g., an encryption key and a MAC key.
Shared secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key-derivation function to derive session keys.
Single-length key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DEA cryptographic algorithm.
Software	The programs and associated data that can be dynamically written and modified.
Split knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. 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.
Subordinate CA and Superior CA	If one CA issues a certificate for another CA, the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, EPPs or PEDs. Subordinate CAs may also issue certificates to lower-level CAs and issue certificate status lists regarding certificates the subordinate CA has issued.
Symmetric (secret) key	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
System software	The special software (e.g., operating system, compilers, or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.
Switch	A node that can route data from a node to other nodes.
Tamper detection	The automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.
Tamper-evident	A characteristic that provides evidence that an attack has been attempted.
Tamper-resistant	A characteristic that provides passive physical protection against an attack.

Term	Definition
Tamper-responsive	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
Tampering	The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data.
TDEA	See *Triple Data Encryption Algorithm*.
TECB	TDEA electronic code book.
Terminal	A device/system that initiates a transaction.
Terminal Master Key (TMK)	This is a symmetric key used to encrypt other cryptographic keys at the point of interaction.
Transaction	A series of messages to perform a predefined function.
Triple Data Encryption Algorithm (TDEA)	An algorithm specified in *ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*
Triple Data Encryption Standard (TDES)	See *Triple Data Encryption Algorithm.*
Triple-length key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDEA cryptographic algorithm.
Trustworthy system	A combination of computer hardware and software that: • Are reasonably secure from intrusion and misuse; • Provide a reasonable level of availability, reliability, and correct operation; and • Are reasonably suited to performing their intended functions.
Two-factor authentication	Two-factor authentication (“TFA” or “2FA”) is a system wherein two different factors are used in conjunction for authentication. Two-factor authentication typically is a signing-on process where a person proves his or her identity with two of the three methods: "something you know" (e.g., password or PIN), "something you have" (e.g., smartcard or token), or "something you are" (e.g., fingerprint or iris scan).

Term	Definition
Unattended acceptance terminal (UAT)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment including, but not limited to, the following: • ATM • Automated Fuel Dispenser • Ticketing Machine • Vending Machine
Unattended payment terminal (UPT)	A POS POI device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as: • Automated fuel dispensers • Kiosks • Self-service devices—ticketing/vending or car parking terminals.
Unprotected memory	Data retained within components, devices, and recording media that reside outside the cryptographic boundary of a secure cryptographic device.
Variant of a key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Verification	The process of associating and/or checking a unique characteristic.
Working key	A key used to cryptographically process the transaction. A working key is sometimes referred to as a data key, communications key, session key, or transaction key.
XOR	See *Exclusive-Or.*
Zeroize	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.
Zone master key	See *Key-encrypting key.*