Foreword ................................................................. 1
How to Use this Guide ............................................. 2
PIN Security Program Overview ............................... 3
PIN Security: From the Attacker's Point of View .......... 5
What to Look for (and Where to Look) .................... 6
Preparing for the Audit ............................................ 6
Control Objective 1-Secure Equipment and Methodologies .... 6
  Question 1-Compliant Hardware .............................. 7
  Question 2a-Cardholder PINs Processed Online - TDES Algorithm .... 11
  Question 2b-Cardholder PINs Processed Offline Protection Requirements 13
  Question 3-PIN Blocks ........................................... 15
  Question 4-No PIN Store and Forward or Logging ........... 18
Control Objective 2-Secure Key Creation ................... 20
  Question 5-Random Keys ...................................... 20
  Question 6-Key Compromise During Key Generation .......... 23
  Question 7-Key Generation Procedures ..................... 25
Control Objective 3-Secure Key Conveyance/Transmission .... 27
  Question 8-Send/Receive Keys ................................ 27
  Question 9-Key Component Access .......................... 30
  Question 10-Key Exchange/Transport Keys Strength .......... 32
  Question 11-Key Transmission Procedures .................. 34
Control Objective 4-Secure Key Loading ..................... 35
  Question 12-Key Loading to TRSM .......................... 35
  Question 13-Key Loading Protection ........................ 38
  Question 14-Key Loading Hardware Dual Control ............ 41
  Question 15-Key Validation ................................. 43
Question 16-Key-Loading Procedures ........................................ 44

**Control Objective 5-Prevent Unauthorized Usage** .................. 45
Question 17-Unique Network Node Keys ................................. 45
Question 18-Key Substitution Prevention .............................. 47
Question 19-Single Purpose Keys ......................................... 49
Question 20-Unique PED Keys ............................................. 51

**Control Objective 6-Secure Key Administration** ................. 54
Question 21-Permissible Key Forms ..................................... 54
Question 22-Key Compromise Procedures ............................ 57
Question 23-Key Variants ................................................... 59
Question 24-Secure Destruction of Obsolete Keys .................. 60
Question 25-Limit Key Access ............................................. 62
Question 26-Log Key Access .............................................. 63
Question 27-Backup Keys ................................................... 64
Question 28-Key Administration Procedures ......................... 65

**Control Objective 7-Equipment Management** ..................... 66
Question 29-Equipment Inspection ....................................... 66
Question 30-Equipment Decommissioning Procedures ......... 69
Question 31-TRSM Procedures ........................................... 70
Question 32-Equipment Security Procedures .......................... 72
Appendix A-PIN Security Audit Checklist ............................. A-1
Appendix B-PIN Security Field Review Agenda ...................... B-1
Foreword

The security of Personal Identification Numbers (PINs) assigned to Visa-branded products such as Visa, Electron, Plus, and Interlink has always been of great importance to Visa and its Members. Technical staff from Visa and many Member banks have helped to formulate the standards under which PINs and cryptographic keys are managed and processed by the entities that make up the worldwide payment system.

However, Visa's efforts have extended well beyond the development of standards and regulations. Since the mid-1990s, Visa has had a comprehensive PIN Security Compliance program in place. The program includes publication of documents such as the PIN Security Requirements, a compliance-reporting requirement for entities involved in the acceptance or processing of interchange PINs, and the conducting of on-site Field Reviews to verify compliance.

This document is designed to explain to internal and external auditors and information security specialists what Visa means by compliance in each area and to help them understand how a Visa Field Reviewer determines compliance in a particular area. By extension, entities can employ these same techniques to assess the adequacy of their implementation for the protection of PINs.

While we have attempted to make this document easy to read and use, we wish to reiterate the tremendous importance that Visa places in PIN Security. We consider PIN Security to be a matter of collective security, rather than an area for competition, and we encourage everyone involved to share information and knowledge freely and openly.
How to Use this Guide

As you go through the Self-Audit Questionnaire, refer to the appropriate individual sections of this Auditor's Guide. Each of these sections describes what we mean by "compliance" in a particular area, and the things to look for during a review to determine whether an acceptable level of compliance exists.

Use the Auditor's Guide as a reference tool, not as hard-and-fast rules for the only acceptable way to do things. In many areas, there are a variety of ways to establish compliance, some cleverer than others. Remember that this analysis is important to your company, to staff involved in cryptography, to the other participants in the Visa payment system, and to the integrity of the Visa brand.
PIN Security Program Overview

Visa requires a PIN Security Self-Audit before commencing operations and in subsequent years. While filling out this document, an auditor usually identifies some areas of non-compliance. For each of these areas, an Exception Report must be completed and filed with Visa. All entities that accept or process PIN-based transactions for Visa-branded products are subject to these requirements.

Following receipt of the Member's documents, Visa may call to schedule a site inspection. This is one of the most valuable and educational services that Visa provides to its Members and their agents.

Field Review Logistics

The PIN Security Field Review usually requires two days to complete. During the review (note that we use the term "review" rather than "audit"), the information submitted on the Self-Audit Questionnaire and Exception Forms is verified and a determination is made as to whether the Member is in compliance with each of the seven control objectives examined. The Review generally begins with introductions followed by a restatement of the goals and objectives of the PIN Security Program. Then a network diagram is developed which describes how messages containing interchange PINs flow through the Member operation being reviewed. The types and quantities of ATMs, POS equipment, Host computers, and Hardware Security Modules are listed and the operating system and application software are identified.

Once the network components and topology have been identified, the details of the cryptographic structure are discussed. This begins with the method(s) used to initialize or re-initialize ATMs or POS equipment. This is followed by the "life history" of all of the other cryptographic keys, including the Master File Key, device-level keys and any keys shared with other networks. The information gathered on each cryptographic key includes the date and method of creation, storage methods and location (if managed in hard copy, on EPROMs, and so forth) and the usage of the key. At this point, a substantial portion of the data gathering process has been completed.

At some point during the review, we will:

- Want to see inside the key-entry area of a production ATM (if applicable).
- Need to see that portion of the data center housing the Hardware Security Modules.
- Carry out a physical inventory of all key components and key-loading equipment.
- Need to see demonstrations of key loading for all cryptographic device types used to process PINs (HSMs, ATMs, POS devices).

These "field trips" can be scheduled so as to minimize disruption to your operations.
We will also need to interview staff involved with receiving and installing ATMs and POS devices, and staff knowledgeable about network operations. Detailed conversations with cryptographic key custodians should reveal all of the details relevant to the receipt, dispatch and storage of cryptographic keys, and how keys are actually loaded (e.g., for HSMs, ATMs, POS devices). At various points during the review, we will need to look at all available written documentation, including policies, procedures, audit trails and logs.

**After the Field Review**

After the review is complete, an exit interview is held, during which the compliance status of each area is presented. A question and answer session then brings the on-site portion of the review to an end.

Shortly thereafter, a management report of findings labeled "Tentative and Preliminary" is submitted and any errors of fact, omission or oversight that are agreed upon between the reviewer and the Member are corrected. Once this is done, the report is reissued in final form and the Member (or their agent) is asked to submit a compliance plan within 30 days. This plan must address each of the areas of non-compliance identified during the review, along with a timeline for completion. Visa will review the plan and agree to establish an action plan with the Member. After an action plan has been agreed upon, periodic status updates must be submitted by the Member (or their agent) in order to track the remedial plan until full compliance is established.
Increasingly sophisticated adversaries with increasingly powerful tools are attacking the Visa payment system every day. No matter how complex and robust our defenses are, given enough time, money and (most importantly) incentive, they can be defeated by a determined attacker. By its very nature, defense consists of the processes of forecasting what the enemy will do and setting barriers and/or traps to frustrate his efforts.

*What constitutes an attractive target?* Ideally, the attacker is looking for the maximum score with the minimum degree of effort and risk. The perfect target would have some or all of the following attributes:

- Production keys would be used in the test environment, allowing the technical support staff to attack the key structure;
- PINs would not be protected by a secure PIN block, allowing "dictionary" attacks;
- Failure to use approved (see www.visa.com/PIN) cryptographic devices for PIN processing;
- Cryptographic keys would be non-random, non-unique and never change;
- Hard copy keys would be in the clear or in cleartext halves;
- Few, if any, procedures would be documented; and,
- No audit trails or logs would be maintained.

Every one of these weaknesses that is corrected reduces the size of the window of opportunity for an attacker. Correct all of them and a rational attacker will likely decide that the potential reward is far too small for the effort and risk involved.
**What to Look for (and Where to Look)**

**Preparing for the Audit**

It is important to diagram the path(s) that interchange messages with encrypted PIN blocks can follow as the PIN blocks pass through the network of the organization under review. Among the questions to address:

- How many ATMs, cash dispensers, and POS terminals with PIN pads are deployed or in inventory?
- How many of these PIN acceptance devices accept Visa-branded transactions from cardholders for whom the organization under review is not the card issuer?
- How many of these devices are compliant with Visa's cryptographic device security requirements (www.visa.com/PIN)?
- Where do these messages go when they leave the ATM or POS PIN pad? to the organization's computer? to a third party processor? somewhere else?
- Where do messages from cardholders who are not the customers of the organization under review get sent?

Once you understand how interchange messages originate and where they go, then you can move on to other questions.

- Does the organization under review operate a backup site that includes the ability to process messages that contain interchange PINs?
- What steps are required to bring a new ATM and/or POS PIN pad into operation? (Make certain that you identify every cryptographic key involved in this process and how each key is used.)
- Does the organization under review use in-house (proprietary) developed processing software or does the organization use a commercial package?

With this information in hand, you can proceed to investigate the 32 individual questions that make up the PIN Security Self-Audit.

**Control Objective 1—Secure Equipment and Methodologies**

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

This Control Objective covers Questions 1-4 of the Self-Audit Questionnaire. These questions ask whether PINs are being encrypted and decrypted inside suitable cryptographic hardware, whether the DES algorithm (TDES with at least double length keys) is being used, whether the PIN is protected within a suitable PIN block and whether PINs are inappropriately stored.

Note: *Equipment TDES capability dates exist globally as defined below, however TDES implementation dates vary by Visa Region. The applicable Visa Regional Risk Management group should be contacted for specifics.*
Question 1–Compliant Hardware

Is the Hardware Compliant?

All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. The following two instances of TRSMs are considered:

- Tamper responsive or physically secure devices: penetration of the device will cause immediate erasure of all PINs, cryptographic keys and all useful residues of PINs and keys contained within it.
- Tamper-evident or minimum acceptable PIN Entry Devices: any attempt to penetrate the device will be obvious. Such a device can only be used for PIN encryption and key management schemes where penetration of the device will offer no information on previously entered PINs or secret keys.

A Tamper-Resistant Security Module (TRSM) must meet the requirements of a Physically Secure Device as defined in ISO 9564 1. Such a device must have a negligible probability of being successfully penetrated to disclose all or part of any cryptographic key or PIN. A TRSM can be so certified only after it has been determined that the device’s internal operation has not been modified to allow penetration (e.g., the insertion within the device of an active or passive “tapping” mechanism). A TRSM (e.g., a PIN Entry Device (PED) that complies with this definition may use a Fixed Key or a Master Key/Session Key key management technique, that is, a unique (at least) double-length PIN encryption key for each PED, or may use double-length key DUKPT as specified in ANSI X9.24.2002 Part 1.

A TRSM relying upon compromise prevention controls requires that penetration of the device when operated in its intended manner and environment shall cause the automatic and immediate erasure of all PINs, cryptographic keys and other secret values, and any useful residuals of those contained within the device. These devices must employ physical barriers so that there is a negligible probability of tampering that could successfully disclose such a key.

In the cases where a PIN is required to travel outside the tamper-resistant enclosure of the PED, the PED must encrypt the PIN directly at the point of entry within the secure cryptographic boundary of the PED to meet the requirements for compromise prevention. PEDs in which the cleartext (unenciphered) PIN travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.

Tamper-evidence is sufficient for PEDs that do not retain any PIN data or key that has been used to encrypt or decrypt secret data, including other keys (e.g., DUKPT schemes or EMV off-line PIN validation where the PED and the IC card reader are integrated in the same tamper-evident enclosure).

Applicability–Question Scope

This question applies to equipment, specifically to all PIN entry devices and Host/Hardware Security Modules (HSMs). See www.visa.com/PIN.
**Intent of Question**

- To ensure PINs and keys are processed only in equipment (ATMs, POS devices, cash dispenser, and other PIN entry devices—PEDs, and Host Security Modules—HSMs) that meet the requirements for physical security as defined in ISO 9564 and ISO 13491.

**NOTE:** The characteristics of the actual device can vary, depending on the cryptographic scheme being employed. If a unique master key/unique session key hierarchy is being used, the PIN entry device must qualify as a Tamper-Resistant Security Module (TSRM) using compromise prevention techniques. If a unique fixed key hierarchy is being used, the PIN entry device must also qualify as a TRSM using compromise prevention techniques. If the device does not retain any key that has been used to encrypt or decrypt secret data, including other keys (e.g., Derived Unique Key per Transaction–DUKPT), the PIN entry device may use compromise detection techniques. TRSMs relying on compromise detection must use DUKPT.

- Ultimately, to prevent disclosure of PINs and keys.

The processing of PINs outside a TRSM represents a serious violation because it exposes cryptographic keys and the PINs that they protect in unprotected computer memory.

**Audit Technique**

**Identify all PIN entry devices (ATMs, POS) and Host Security Modules and compile a list of all such equipment that accepts PINs and processes PINs (e.g., translates PINs from encryption under one key to encryption under another key).**

For each such device, obtain and examine one or more of the following:

- NIST certification that the equipment used for PIN translation (hardware or host security modules) complies with a minimum of level 3 of FIPS 140-2-Security Requirements for Cryptographic Modules. This may be obtained from the NIST website (csrc.nist.gov). Hardware Security Modules must be compliant with **FIPS 140-2** Level 3 or Level 4 (formal certification is not required, however, such certification is evidence of a device’s compliance to this requirement).

- Vendor Certification letters or technical documentation to indicate that the equipment has been designed to meet (**ANSI X9.24** and **ANSI X9.8/ISO 9564** are the minimum criteria):
  - **FIPS 140-2**—Security requirements for Cryptographic Modules-Level 3 or 4.
  - **ANSI X9.24**—Financial Services Retail Key Management.
  - **ANSI X9.8**—Personal Identification Number Management and Security (all parts).
  - **ISO 9564**—Banking-Personal Identification Number Management and Security (all parts).
  - **ISO 13491-1**—Banking-Secure Cryptographic Devices (Retail), Part 1 Concepts, Requirements and Evaluation methods.
c. Purchase orders and vendor invoices to identify where crypto- graphic hardware is specified for PEDs. Note that for certain vendors this is “optional” equipment.

d. Purchase orders and vendor invoices should be used to identify the point of PIN encryption (PIN Pad, motherboard, etc.) for a PED. Physical inspection of the device may also be used where feasible.

Note that vendor documentation previously reviewed may be referenced where the documentation exists in workpapers pertaining to another specific review (this review and the workpaper references must be cited) using the same make and model of equipment. Also note that PEDs that meet the definition in ANSI X9.24 of “compromise detection” may be employed if they utilize a DUKPT technique.

For POS PIN acceptance devices and for ATM and Cash Dispensing PIN acceptance devices, refer to www.visa.com/PIN to ensure that devices have been evaluated at a Visa recognized laboratory and that the evaluation has been completed in compliance with the Visa PED Security Program. Obtain documented verification of the evaluation. Specifically:

a. Ensure the PIN entry device security evaluation has been completed:
   - Effective January 1, 2004, all newly deployed POS PIN acceptance device models (including replacement devices) must have passed testing by a Visa-recognized laboratory and been approved by Visa.
   - Effective July 1, 2010, all POS PIN acceptance device models must have passed testing by a Visa-recognized laboratory and been approved by Visa.
   - Effective October 1, 2005, all newly deployed EPPs, including replacements or those in newly deployed ATMs must have passed testing by a Visa-recognized laboratory and have been approved by Visa.

b. Ensure such equipment complies with TDES requirements:
   - Effective January 1, 2003, all newly deployed ATMs (including replacement devices) must support TDES.
   - Effective January 1, 2004, all newly deployed POS PIN acceptance devices (including replacement devices) must support TDES.

c. Ensure display options used by such equipment are in compliance. These options are specified at www.visa.com/PIN as either class A (the device is either totally locked by the PED vendor from alteration of display or the display can only be altered by the PED vendor) or class B (the PED display can be altered by a third party subject to constraints noted below):
   - If the PIN entry keyboard may be used to enter non-PIN data, then all prompts for non-PIN data are under the control of the cryptographic unit of the PED. If the User Prompts are stored inside the cryptographic unit, they cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the User Prompts are stored outside the cryptographic unit, mechanisms must exist to ensure authenticity and proper use of the prompts and modification of prompts or improper use of prompts is prevented (class A), or
If the PIN-entry keyboard may be used to enter non-PIN data, then the unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without the expenditure of at least US $10,000 per PED (class A), or

Cryptographically based controls are utilized to control the device display and PED usage such that it is infeasible for an entity not possessing the unlocking mechanism to alter the display and to allow the output of unencrypted PIN data from the PED. The controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Key management techniques and other control mechanisms are defined and include appropriate application of the principles of dual control and split knowledge (class B).

d. **Examine the device and its characteristics:** (A TRSM has a number of features that are designed to protect the secrecy of the cryptographic key(s) contained in its memory. These features may include temperature, pressure and motion sensors, an enclosing wire grid, and an armored case and components. All of these features are designed to detect, resist and react to any attempt by an adversary to learn the value of cryptographic keys. The primary method used by a TRSM to defeat such an attempt is to "dump" or erase the keys whenever unauthorized intrusion is detected.)

- Ensure indicator lights (if any) signify that the device is powered up and armed.
- Ensure locks (if any) are turned to the locked position and the keys are removed.
- Determine if the device has mechanisms that will cause it to "dump" or erase the keys in the event of intrusion.
- Determine if the same make and model were previously reviewed and determined to be compliant or non-compliant then.
- If it is not clear that the device is a TRSM, request an affidavit of compliance from the manufacturer. This affidavit should stipulate that the device satisfies ANSI and ISO requirements for a TRSM, should identify the independent testing lab that supports this claim, and should bear the signature of a corporate officer.  

*Note: A clause should be in all of the organization's purchase contracts for ATMs, cash dispensers, POS PIN pads, and Hardware Security Modules requiring the manufacturer to stipulate that all PIN-processing equipment supplied under the contract is compliant.*

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make sure that the Hardware Security Modules physically present in the data center are powered up, connected to the Host computer, armed and in a state to resist attempts at tampering. One large installation was very proud of its investment in state of the art HSMs until it was pointed out that they were not connected to the Host computer.</td>
</tr>
</tbody>
</table>

---

^4For POS PIN Entry Devices (PEDs) purchased after January 1, 2004 and for ATMs purchased after 1 July 2004, validate that the devices are listed as approved at www.visa.com/PIN for the specific purpose (e.g., online or offline PIN)
Question 2a–Cardholder PINs Processed Online–TDES Algorithm

Is the TDES algorithm being used to encrypt/decrypt online PINs?

All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards.

Online PIN translation must only occur using one of the allowed key management methods: DUKPT, Fixed Key, Master Key/Session Key.

Online PINs must be encrypted using the TDEA Electronic Code Book (TECB) mode of operation as described in ANSI X9.52. For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in ANSI X9.52.

As of the publication date of this document, Visa has not set global dates for enforcement of the requirement for TDES. However for specific Visa Regional implementation dates contact your Visa Regional Risk Group.

Applicability – Question Scope

This applies to all interchange PINs entered at all ATMs, POS PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing. This also applies to any internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”). Examine the algorithm type parameter (to ensure it denotes DES, specifically TDES) 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. Examine cryptograms' key length (32 hexadecimal characters for TDES) on every terminal link, network link, and if applicable, internal path.

Intent of Question

- To ensure that a valid approved algorithm is used to encrypt online cardholder PIN (i.e., to ensure that PINs are encrypted using TDES).
- To ensure that only one of the allowed key management methods is used in encrypting PINs and/or in encrypting keys that are used in encrypting PINs.
- Ultimately to ensure that clear PINs are not exposed across network links or on databases, computer memory, electronic media, or on system logs, backup tapes etc.
Audit Technique

Interview responsible personnel to determine encryption algorithms utilized in connection with “not-on-us” acquisitions of PIN blocks.

Examine vendor certification letters or technical documentation to indicate that the PIN processing equipment has been designed to meet approval standards and specifically:

- ANSI X3.106—Modes of DEA Operation.
- ANSI X3.92—Data Encryption Algorithm.
- ANSI X9.24—Financial Services Retail Key Management.
- ANSI X9.52—Triple Data Encryption Algorithm Modes of Operation.

Examine system documentation to verify information provided during 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.

Examine PIN translation transactions in a trace log and ensure that the “from” key cryptogram does not equal the “to” key cryptogram. (Note-this is only valid after establishing the keys are encrypted under the same key and variant). The command(s) to the HSM must be verified (command exists and instructs the HSM to perform PIN translation). Examine the HSM manual to ensure that the PIN translation command utilizes DES/TDES.

As noted in the question's scope above, examine the algorithm type parameter (to ensure it denotes DES — specifically TDES) 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.

As noted in the question's scope above, examine the encrypted values of the keys to determine the length (32 hexadecimal characters for TDES) on every terminal link, network link, and if applicable, internal path.

Examine encrypted PIN blocks to validate they are 8 bytes (16 hexadecimal characters) long and that the individual position values are in the range 0-9, A-F. (Note-TDES encrypted PINs will be 16 hexadecimal characters in length with values in the range of 0-9, A-F. TDES keys themselves, and cryptograms of TDES keys will be 32 hexadecimal characters in length).
Question 2b–Cardholder PINs Processed Offline Protection Requirements

*Is the offline PIN protected during transit whether using an integrated reader and PIN pad or not?*

All cardholder PINs processed offline using IC Card technology must be protected in accordance with the requirements in Book 2 of the EMV2000 IC Card Specifications for Payment Systems.


**Applicability–Question Scope**

This applies to all interchange PINs entered at PIN acceptance devices that process the PINs offline using IC Card technology.

**Intent of Question**

- When performing offline PIN verification using IC Cards, to ensure the secure transfer of a PIN from entry point to the ICC regardless of whether using an integrated reader and PIN pad or not.
- Ultimately to ensure that clear PINs are not exposed across links from point of PIN entry to the point of PIN verification in the ICC.

**Audit Technique**

**Interview the responsible personnel to determine types and design of offline IC Card technology devices.**

**When the terminal supports offline PIN verification, ensure that proper devices are in place.** Specifically:

- If the reader (Interfacing Device–IFD) and PIN pad are integrated, the device is a TRSM, or
- If separate, the reader (IFD) is a TRSM and the PIN pad is a TRSM.
- Refer to www.visa.com/PIN to ensure that devices have been evaluated at a Visa recognized laboratory and that the evaluation has been completed in compliance with the Visa PED Security Program as explained in question 1. Obtain documented verification of the evaluation.

**Examine vendor documentation to determine the flow of the PIN from entry point to ICC PIN validation point.** Ensure the PIN is protected as described in Section 11.1.2 of *Book 2 of the EMV2000 IC Card Specifications for Payment Systems*. Specifically:

- “If the IFD and PIN pad are integrated and the offline PIN is to be transmitted to the card in plaintext format, then the PIN pad does not encipher the offline PIN when the plaintext PIN is sent directly from the PIN pad to the IFD.”
• If the IFD and PIN pad are integrated and the offline PIN is to be transmitted to the card in plaintext format, but the offline plaintext PIN is not sent directly from the integrated PIN pad to the IFD, then the PIN pad shall encipher the offline PIN according to ISO 9564-1 (or an equivalent payment system approved method) for transmission to the IFD. The IFD will then decipher the offline PIN for transmission in plaintext to the card.

• If the IFD and the PIN pad are not integrated and the offline PIN is to be transmitted to the card in plaintext format, then the PIN pad shall encipher the offline PIN according to ISO 9564-1 (or an equivalent payment system approved method) for transmission to the IFD. The IFD will then decipher the offline PIN for transmission in plaintext to the card.

• If the offline PIN is to be transmitted to the card in enciphered format, then the PIN must be enciphered as described in section 7.2. The PIN encipherment process shall take place in either
  - The tamper evident PIN pad itself.
  - A secure component in the terminal. In this case the PIN pad shall encipher the PIN according to ISO 9564-1 (or an equivalent payment system approved method) for secure transport of the PIN between the PIN pad and the secure component.

If encipherment for offline PIN verification is supported using an asymmetric based encipherment mechanism, review documentation and interview personnel to determine proper management and verification.

Check to see that:

• Keys and certificates are managed in accordance with Section 7 of Book 2 of the EMV2000 IC Card Specifications for Payment Systems.

• PIN encipherment and verification occur as specified in Section 7 of Book 2 of the EMV2000 IC Card Specifications for Payment Systems.

Note: Acquirer keys used for the transport of PINs during an offline PIN verification transaction must be either TDES using at least double length keys, RSA with a key modulus of at least 1024 bits, or an algorithm and key size of equivalent or greater strength approved by Visa.
Question 3–PIN Blocks

Are you enclosing PINs within secure PIN blocks?

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

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 9564–1 format 0, ISO 9564–1 format 1, or ISO 9564–1 format 3.

For ISO format 0 and 3, the cleartext PIN block and the Primary Account Number block must be XOR'ed together and then Triple-DES encrypted in Electronic Code Book (ECB) mode to form the 64-bit output cipherblock (the reversibly encrypted PIN block). ISO format 3 should be used for encryption zones where the PIN encryption key is static for the productive life of the device in which it resides.

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

PINs enciphered only for transmission between the PIN entry device and the IC reader must use ISO format 0, 1 or 3.

Applicability–Question Scope

This applies to all interchange PINs entered at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing. This also applies to any internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”). Examine PIN block formats on every link into and out of the host system, and on internal paths within the application itself (i.e., if the site operates multiple physical and/or logical instantiations of the application). Examine the PIN block format parameter on every terminal link, network link, and if applicable, internal path (i.e., if using an Intermediate Key) for the host application.

Intent of Question

• To protect against a dictionary attack that can occur if PINs with the same values have encrypted PIN blocks that are the same.

The encrypted PIN is not inserted into a message in the clear. It is formatted into a PIN block. PINs can be any length—from 4 to 6 characters—and the field in the message that holds the encrypted PIN is a fixed 16 characters in length. Therefore, the encrypted PIN is combined with other data to completely fill this field. This combination of the PIN and other data is called a PIN Block.
Early ATMs, such as the IBM 3624 just filled or "padded" the PIN with hexadecimal Fs. This is called the 3624 or "PIN Pad" PIN block format. The problem with this system is that a given PIN value, such as 1234, will always produce the same encrypted result under a specific key value, which allows an attacker to carry out something called a "dictionary" attack. He doesn't crack the key, but rather just recognizes specific encrypted PIN blocks as the result of entering a particular PIN value.

Dictionary attacks are prevented by using ISO PIN Block Format 0 (also known as ANSI PIN Block Format 0), which XORs (exclusive ORs) the right-most 12 digits of the account number (less the check digit) with the PIN, then encrypts the resulting string using TDES in Electronic Code Book (ECB) mode. ISO PIN Block Format 3 does the same. Even if two cardholders enter the same PIN value, the resulting PIN blocks will be different, since the account numbers are different. As mentioned in question 2, a scheme approved alternative encryption method may be used.

**NOTE:** The old Visa PIN Block Formats 02, 03, and 04 are not acceptable for interchange traffic.

### TIPS, TRICKS, AND STRANGE OBSERVATIONS

Some superceded Visa publications (incorrectly) allow use of Visa Format 3 PIN blocks. These PIN blocks are identical to the old "PIN Pad" or IBM 3624 format. They are not acceptable and represent a serious security exposure. Visa systems will be modified to reject any incoming messages with insecure PIN blocks in the near future.

The Visa Payment Technology Standards Manual (or ISO 9564–1 or ANSI X9.8–1) contains details on how to construct the required PIN block.

### Audit Technique

Using the network schematic from the preliminary step, interview responsible personnel to determine the PIN block format(s) utilized for Visa branded product "not-on-us" traffic from point of acquisition through routing of the transaction to another entity.

- **Examine vendor certification letters or technical documentation to ensure proper design.** The equipment must meet one or more of the following:
  - ANSI X9.8–1 - *Personal Identification Number Management and Security.*
• 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 used.
  – Application packages, examine parameter files where the PIN block format is specified (e.g., the KEYF file for Base 24). Verify the format is ANSI or ISO Format 0, ISO format 1 or ISO format 3 as the online PIN block type for compliance. An entry of PIN Pad, 3624, Diebold or anything else is out of compliance.

• **Examine PIN translation transactions in a trace log and ensure that the “from” PIN block and the “to” PIN block are using either ISO format 0, 1 or 3.** The command(s) to the HSM must be verified (command exists and instructs the HSM to perform PIN translation).

As noted in the question's scope on page 15, examine PIN block formats on every link into and out of the host system, and on internal paths within the application itself (i.e., if the site operates multiple physical and/or logical instances of the application). Examine the PIN block format parameter on every terminal link, network link, and if applicable, internal path (i.e., if using an Intermediate Key) for the host application.
Question 4–No PIN Store and Forward or Logging

No insecure "store and forward" or logging is taking place.

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

Transactions may be stored and forwarded under certain conditions as noted in ISO 9564–1. When such conditions are present, any store-and-forward transaction PIN must be stored in encrypted form using a unique key not used for any other purpose.

PIN blocks, even encrypted, must not be retained in transaction journals or logs. PIN blocks are required in messages sent for authorization, but are not required to be retained for any subsequent verification of the transaction.

Applicability–Question Scope

This question applies to all interchange PINs.

Intent of Question

• To prevent the potential harvesting and subsequent attacking of any large repository of logged encrypted PINs.

• To compartmentalize the risk of a successful key exhaustion attack against static encrypted PIN data. If the key that protects the repository of static encrypted PIN data is successfully attacked and discovered, then using a unique key for such store-and-forward transaction PINs limits the risk to only those PINs and not to every PIN in every transaction. Using a unique key for store-and-forward transaction PINs also limits the risk to discovery of just that key and not to the discovery of any key that is used normally to protect PINs entered at PIN entry devices.

Normally, PIN-based transactions take place in real time. The PIN is entered by the cardholder, encrypted, enclosed in a message, and transmitted to the authorizing entity that makes the approval decision. The message containing the PIN encrypted under the PEK is not normally stored or logged in any way. However, some exceptions to this situation may exist in certain point-of-sale environments, such as large supermarkets. In the event that the PIN is stored, it must be stored under an encryption key different from the one used to encrypt it at the point of transaction in order to protect the PIN Encryption Key (PEK) from attack. However, it is important to restate that the PIN block should never be logged except as part of a store-and-forward transaction.
Audit Technique

Interview appropriate personnel to determine if PINs are stored or retained for some period of time as part of a Store and Forward environment. Where PINs are stored, determine the encryption key used. Verify that a different encryption key is used and that the translation from the PEK to this other working key is performed within a TRSM using the DES algorithm. (Note that store and forward is sometimes used in a supermarket or hypermarket environment.)

Examine transaction journals/logs to determine the presence of PIN blocks.

For environments using online transaction monitors such as CICS or IMS-DC, specifically note how management has identified that no PINs are 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.

### TIPS, TRICKS, AND STRANGE OBSERVATIONS

Be alert to transactions passing through store controllers or concentrators. Ask what happens to the transaction if the Issuer or the Acquirer host is unavailable. If the message is held at the store controller, get the details of the key used to protect the PIN during the period when it is being stored, and get the make and model of the HSM attached to the controller. If there is no HSM, note it as a finding the resolution of which requires installation of a HSM.

*Note: We have never seen this happen in an ATM environment.*
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.

This Control Objective covers Questions 5-7 of the Self-Audit Questionnaire. It seeks to ensure that all cryptographic keys are created randomly and whether the key-generation process can be compromised. In addition, key components must only exist as two or more full-length components that are then XOR’ed together to form the active key.

Question 5–Random Keys

Are all cryptographic keys created randomly?

All keys and key components are generated using an approved random or pseudo-random process.

Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys.

Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values. An independent laboratory must certify self-developed implementations of a cryptographic pseudo-random number generator, which includes testing in accordance to the statistical tests defined in FIPS 140-2 (Level 3).

Applicability–Question Scope

This question applies to:

- All cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing.
- Master Keys and hierarchy keys (e.g., Atalla equipment's “Super Keys”).
- Any keys used for internal PIN translations that may occur in the system, or keys used internally.

Intent of Question

- To maximize the range of possible values for any one key thereby increasing the difficulty of guessing or brute-force attacking keys (making key exhaustion more difficult).
- To eliminate the use of known keys.
- To avoid the use of default, test, predictable, easily guessed or “simple” keys (e.g., 0123456789ABCDEF, alternating 0s and 1s, etc.).
The DES algorithm itself is no secret. In fact, anyone can acquire a copy of it. The only protection offered by DES rests in the strength and secrecy of the cryptographic key used to encrypt the data. One of the ways to defeat DES is to mount a "brute force" attack; in other words, to try all possible combinations until the correct key is guessed. One of the most powerful defenses against a successful "brute force" attack is to ensure that all possible keys have an equal chance of occurrence. The only way to guarantee that this happens is to ensure that a truly random process is used to generate keys. The definition of a random process, whether manual or mechanical, is one that can neither be predicted nor reproduced. The outcome from a true random process is neither predictable nor predictably reproducible.

Audit Technique

Using the network schematic from the preliminary step, interview responsible personnel to determine the origin of the cryptographic keys used for interchange.

Examine the operation's documentation that describes the key generation processes. This should include manual logs for Master File Keys and Key Exchange Keys.

Examine cryptogram files (or samples of check values) to validate unique keys (random/pseudo-random generation).

Have the technical staff sort on the cryptograms field (or the check digit field) to make it easier to spot duplicates.

Examine vendor certification letters or technical documentation to indicate that the equipment has been designed to meet appropriate standards and specifications.

The equipment must meet one or more of the following:

- **FIPS 140–2**—Security requirements for Cryptographic Modules-Level 3 or Level 4.
- **ISO 11568–1**—Banking-Key Management (Retail)-Part 1: Introduction to Key Management.
- **ISO 11568–2**—Banking-Key Management (Retail)-Part 2: Key Management Techniques for Symmetric Ciphers.
- **ISO 11568–3**—Banking-Key Management (Retail)-Part 3: Key Life Cycle for Symmetric Ciphers.
- **ANSI X9.17**—Financial Institution Key Management (Wholesale).
- **ANSI X9.24**—Financial Services Retail Key Management.
- Observe a demonstration of the key generation process.

Ensure keys are generated by using the key generation function of a **Hardware Security Module (HSM) or similar device**. Other acceptable ways are a series of coin flips or any similar process where the outcomes can be reduced to binary values (0-1, true-false, on-off, red-white, and so forth).
Ensure keys are NOT generated as follows:

- **By staff “thinking up” values.** Statistical analysis has shown that some values occur more often than others, resulting in an uneven distribution of key values.
- **In computer memory.** These could be compromised during the process.
- **By a method that gives the same output value every time a specific starting or “seed” value is used.**

**Compare key check values against those for known, default, test, predictable, easily guessed or “simple” keys.** Such check values are often printed in vendor manuals.

**Ask key custodians to examine key components in order to identify any obviously non-random components.**

**TIPS, TRICKS, AND STRANGE OBSERVATIONS**

No matter what your colleagues tell you, "thinking up" a key or key components is not acceptable. Use the HSM to generate keys. This can also weed out "weak" keys.

Refer to the vendor documentation for a list of known factory default and test key check values. If you spot one of these values, ensure the key is replaced and ensure they generate a new random key. Also see question #15.
Question 6–Key Compromise During Key Generation

Collusion is needed to compromise a key during its creation.
Compromise of the key generation process is not possible without collusion between at least two trusted individuals.

The output of the key generation process must be monitored by at least two authorized individuals who can ensure there is no unauthorized tap or other mechanism that might disclose a cleartext key or key component as it is transferred between the key generation TRSM and the device or medium receiving the key or key component.

Printed key components must be printed within blind mailers or sealed immediately after printing so that only the party entrusted with it can observe each component and so that tampering can be detected.

Any residue from the printing or recording process that might disclose a component must be destroyed before an unauthorized person can obtain it.

Applicability–Question Scope

This question applies to the generation of:

- All cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing.
- Master Keys and hierarchy keys.
- Any keys used for internal PIN translations that may occur in the system, or keys used internally.

Intent of Question

To ensure:

- The secrecy and integrity of keys during the key generation process, including during the transfer to the target device or medium.
- No visual or electronic surveillance or monitoring occurs during the key generation and transfer of the key to the target device or medium.
- Any secure device (such as a Tamper-Resistant Security Module) used for generating keys is free from any electronic tapping devices, that the component values cannot be observed by any unauthorized person, and that only secure printed output such as a PIN mailer is created.

Audit Technique

For keys identified in the network schematic, interview appropriate personnel to determine the processes used for the key generation.

For keys generated as components and/or manually loaded, examine the documentation of how the processes should occur.

Examine key generation logs to verify that multiple personnel participate in the key generation processes.
Witness a structured walk through/demonstration of the key generation processes for all key types (MKs, AWKs, TMKs, etc.). This should be done to verify information provided through verbal discussion and written documentation:

**Observe if there is any way that an adversary could obtain the values of the key components.** Inspect the devices used in the process for evidence of tampering. Observe whether the devices are "cold started" and powered off after use (except when an HSM is being used to generate key components). Observe whether any live network connections exist. Determine whether any compromise of paper outputs can take place, including waste, printer ribbons, and so forth.

**Examine the physical area to verify that the key component generation process can be done in complete seclusion.** Verify that any mechanical or electronic devices being used do not have any extra "dangly bits", such as wiretaps, or mysterious wires or cables sprouting from them. If the component value is printed out, ensure that it is either printed inside a blind envelope, such as a PIN mailer, or that no one but the authorized custodian ever has physical access to the output.
Question 7—Key Generation Procedures

Documented procedures exist and are demonstrably in use for all key generation processing.

Written key creation procedures must exist and be known by all affected parties (key custodians, supervisory staff, technical management, etc.). All key creation events must be documented.

Applicability—Question Scope

This question applies to written procedures that describe how all cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing are generated. This includes Master Keys and hierarchy keys, and any keys used for internal PIN translations that may occur in the system, or keys used internally.

Intent of Question

To ensure:

- Adequate and appropriate documented written procedures exist for the generation of all cryptographic keys.
- Documented procedures are followed, and that keys are not generated in any other (especially non-compliant) manner.

Audit Technique

Review existing documentation for completeness. Documentation detailing procedures and personnel (by organizational placement or name) may include references to vendor documentation.

Overview of Documented Procedures for All Questions:

Questions 7, 11, 16, 28 and 32—Procedure Documentation. Documented procedures are in place for all aspects of cryptographic key management.

Question 7—Key-Generation Procedures. Documented procedures exist and are demonstrably in use for all key-generations processing.

Question 11—Key-Transmission Procedures. Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.

Question 16—Key-Loading Procedures. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.

Question 28—Key Administration Procedures. Documented procedures exist and are demonstrably in use for all key administration operations.

Question 32—Equipment Security Procedures. Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.
The operations of all PIN-acceptance processes must be governed by comprehensive written procedures that ensure that both Visa's rules and the institution's policies are strictly observed at all times.

**Ensure written procedures cover key creation, formation, transmittal, storage, loading, and destruction, as well as govern equipment receipt, inspection, storage, deployment, and decommissioning.** Examine the policies that stipulate the use of these procedures and assess, through the distribution list, whether the procedures have been placed in the hands of the appropriate staff. Finally, ensure the existence of the set of logs and audit trails that prove that the procedures have been carried out on an ongoing basis.
Control Objective 3—Secure Key Conveyance/Transmission

Keys are conveyed or transmitted in a secure manner.

This Control Objective covers Questions 8-11 of the Self-Audit Questionnaire. These questions seek to ensure that keys are not subject to compromise during conveyance both within the organization and to other entities.

Question 8—Send/Receive Keys

How are keys sent and received?

Secret or private keys are transferred by:

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

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

Specific techniques exist in how keys must be transferred in order to maintain their integrity. An encryption key, typically Key Encryption Keys (KEKs), must be transferred by physically forwarding the separate components of the key using different communication channels or transmitted in ciphertext form. Key components must be transferred in either tamper-evident packaging or within a TRSM. No person shall have access to any cleartext key during the transport process.

A person with access to one component of a key, or to the media conveying this component, must not have access to any other component of this key or to any other medium conveying any other component of this key.

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.

Public keys must use a mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received.

Applicability—Question Scope

This question applies to:

• All symmetric and to the public key of asymmetric cryptographic keys that are transferred from a location where the key was generated to a location for loading and/or storing of the key.
• All cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site’s host system for all directions of PIN flow—incoming and outgoing.
• Master Keys and hierarchy keys.
• Any keys used for internal PIN translations that may occur in the system, or keys used internally.
**Intent of Question**

To ensure:
- Secrecy and integrity of keys when key components are transferred from the location of generation to the location of loading and/or storing.
- Integrity and authenticity of public keys that are conveyed from one location to another. This is to protect against a “man-in-the-middle” attack, or substitution of a public key by an adversary.

**Secret or private keys:**
When a secret or private cryptographic key is sent from one place to another, it must be sent in such a way that it remains totally secret. The governing principles of a secret or private key transmitted as two or more components are split knowledge and dual control. This means that no one person has sufficient knowledge to compromise the key and the key cannot be formed without the direct participation of more than one person. To ensure that these principles are observed, a secret or private key must be sent as two or more full-length components to separate designated recipients through separate delivery methods, such as different courier service firms, or it can be sent encrypted. **Note that an encrypted secret or private key may be sent without any special precautions.**

**Public keys:**
When a public cryptographic key is sent from one place to another, some mechanism independent of the actual conveyance method that provides the ability to validate that the correct key was received must be used.

**Audit Technique**

**Interview appropriate personnel and examine transmittal and receipt logs for key components that are manually conveyed or received.** **Note that electronically transmitted keys or components should only be transmitted as cryptograms.**

**Review procedural documentation for key receipt and transfer of key components.**

**Follow the route taken by each key component that the organization sends.** Typically, these consist of Key Exchange Key (KEK) components that the organization creates and sends to a network with which it exchanges message traffic containing PINs and ATM or PIN pad initialization keys, often referred to as the A and B keys. Note that these rules apply to initialization keys also. Verify that each key component is sent in an opaque, tamper-evident package to a specific, named recipient. Ensure that the components are sent through different methods (for example, FedEx for one and UPS for the other). Components sent on chip cards or other non-paper media must follow the same rules.

**If sending the cryptogram of a key rather than its components, no special precautions need be taken.** However, it is still a good practice to give a transmittal notice and receive a notice of receipt.

**When the organization receives key components, verify that the components are received by staff designated as key custodians and that they are logged before being placed into secure storage.**
Trace how all keys are sent and received under normal conditions to ensure that the rules have been followed. Review the written documentation and the key logs to crosscheck that everything has been accounted for. Determine how keys, especially ATM initialization keys, are sent in an emergency. (It seems to be common practice to violate every security procedure in the name of customer service, and it is often the case that the key values are dictated over the telephone or faxed to a service technician. This has the possibility of compromising that key and all of the keys and/or PINs that it ever protected.)

TIPS, TRICKS, AND STRANGE OBSERVATIONS

A standard courier envelope is tamper-evident, but the original envelope could have been replaced by another. Use pre-numbered tamper-evident envelopes, with the number of the envelope that was used being communicated to the recipient by phone, fax, email, and so forth. The best transmittal methods include notification to the recipient that a component is coming and with it, a receipt to be returned to the sender.

Things not to do:

• Dictate keys over the telephone
• Fax cleartext keys or components
• Write key values into startup instructions
• Tape key values inside ATMs
• Write key values in procedure manuals
Question 9–Key Component Access

Are key components accessible only to designated key custodians while conducting cryptographic operations?

Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:

a. Under the continuous supervision of a person with authorized access to this component, or

b. Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it, or

c. In a physically secure TRSM.

Key components are the separate parts of a cleartext key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, key components exist for KEKs, such as keys used to encrypt Working Keys for transport across some communication channel. Until such keys can be protected by encryption, or by inclusion in a TRSM, the separate parts must be managed under the strict principles of dual control and split knowledge. Dual control involves a process of using two or more separate entities (usually persons), which are operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of the materials involved. No single person shall be able to access or use all components of a single cryptographic key. Split knowledge is a condition under which two or more entities separately have key components that, individually, convey no knowledge of the resultant cryptographic key.

Procedures must require that plaintext key components stored in tamper-evident envelopes that show signs of tampering must result in the destruction and replacement of the set of components, as well as any keys encrypted under this key.

No one but the authorized key custodian (and designated backup) shall have physical access to a key component prior to transmittal or upon receipt of a component. Mechanisms must exist to ensure that only authorized custodians place key components into tamper-evident packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components upon receipt.

Applicability–Question Scope

This question applies to: all symmetric cryptographic key components when they are transmitted, conveyed or moved between two organizational entities. This applies to all symmetric cryptographic key components for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing. This question also applies to components of Master Keys and hierarchy keys. This question also applies to components of any keys used for internal PIN translations that may occur in the system, or keys used internally.
Intent of Question

- To ensure the secrecy and integrity of key components and keys when key components are transferred, conveyed or moved between two organizational entities.
- Unlike the previous question, which examines the methods used to transport keys (as either cryptograms or key components), this question addresses the transfer of key components between business entities such as a Member bank and a processing network. This question refers to the methods in place to transport key components within a specific enterprise. (For example, this question is intended to ensure that key components are not compromised while they are being transported from secure storage to the data center where they will be entered into a TRSM.)

Audit Technique

Interview appropriate personnel and examine documented procedures for the custody (and storage or destruction if applicable) of key components from the time of generation to the time of transmittal/loading, or for the time from receipt until the time of loading.

Examine logs of access to the security containers to validate that only the authorized individual(s) accesses each component.

Ensure that the principles of dual control and split knowledge are being strictly enforced. Diagram the process, as detailed in the written procedures and during conversations with the participants. Identify any points in the process when someone other than a designated key custodian holds a key component or when one person has physical control of all of the components of a key.

Examine the key component storage arrangements. Ensure the container is secure and the custodian is the only person who has access to the contents. (For example, if the components are stored in a safe, they should be in different locked areas with the brass keys or combinations held by the designated custodians.)

| Dual Control—No single person can gain control of a protected item or process. |
| Split Knowledge—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. |

Ensure key components are NOT stored in unsecured desk drawers. (This is not robust enough for the purpose, and master brass keys are often held by facilities or maintenance staff.) Ensure multiple components are NOT stored in the same physical area within a safe or lockbox. Verify that the key custodian must participate in the process of retrieving the component and that no single person, whether designated as a custodian or not, can access all components of a key.
**Question 10—Key Exchange/Transport Keys Strength**

*All DES Key Exchange or Transport keys are double length. RSA keys used to transmit or convey other keys use a key modulus of at least 1024 bits.*

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

All DES keys used for encrypting keys for transmittal must be at least double-length keys and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key encipherment. A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.

RSA keys used to transmit or convey other keys must use a key modulus of at least 1024 bits.

**Applicability—Question Scope**

This question applies only to keys that are used to transmit other keys. It does not apply to keys that encrypt PINs. Applicable keys include symmetric cryptographic keys used in the Master Key Transaction Key management technique for ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing. Applicable keys also include asymmetric keys used to convey other keys.

**Intent of Question**

- To ensure that encrypted keys are protected by encryption with keys that are as least as strong as they are.
- Ultimately to protect against a key exhaustion attack to protect the key that ultimately protects PINs.

NOTE: All DES cryptographic keys fall into one of three categories:

- A specific key is a Master key, used to encrypt other keys for storage as cryptograms in a device or host environment.
- A Key Encryption (Key Exchange, Key Transport, Key Encipherment) key is used to encipher a DES key during transport. This question involves these DES keys. These DES keys must be at least double length keys and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key encipherment. A double or triple length DES key must not be encrypted with a DES key of a shorter length.
- A Working key is used to encipher the actual data, such as a PIN. Visa requires that all DES Key Exchange keys must be at least double length (32 hexadecimal characters).

Note: As of the publication date of this document, Visa has not set global dates for enforcement of the requirement for TDES. However for specific Visa Regional implementation dates contact your Visa Regional Risk Group.
The industry is developing techniques for using asymmetric keys to distribute symmetric keys to remote devices. Such schemes may involve RSA keys to encrypt a TDES symmetric key. If implemented, the RSA key must use a key modulus of at least 1024 bits to be in compliance with this question.

**Audit Technique**

Based upon the network schematic, identify all key encipherment keys. This should include the master file key(s) used for interchange transactions.

Interview appropriate personnel and examine documented procedures for the creation of these keys. This must be done to ensure that they are at least double length keys and use TECB or TCBC mode of operation for encryption if a DES key, and if a RSA key, it uses a key modulus size of at least 1024 bits.

For all terminal link, network link, and if applicable, internal path (i.e., if using an Intermediate Key) for the host system that uses the Master Key Transaction (Session) Key key management method, examine the cryptograms of their key exchange keys and validate that all DES symmetric keys are 32 or 48 hexadecimal characters. If there are RSA asymmetric transport keys, validate that the RSA public key modulus is at least 1024 bits on all applicable terminal links and all applicable network links.

Verify that no Key Exchange Key is shorter than the cryptographic keys that it protects and it is at least double length for a DES key; and if RSA, that it uses a key modulus of at least 1024 bits. Examine the DES key cryptogram and ask the custodians to count the number of characters in each DES key component in order to verify compliance with this requirement. Examine the RSA public key modulus and count the number of characters to verify it is at least 1024 bits.
Question 11—Key Transmission Procedures

_Key transmission procedures are in place._

Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.

Written procedures must exist and be known to all affected parties. Conveyance or receipt of keys managed as components or otherwise outside a TRSM must be documented.

_Applicability—Question Scope_

This question applies to written procedures that describe how all cryptographic keys and/or symmetric key components are transmitted, conveyed or moved between two entities. This applies to all keys and symmetric key components transmitted/conveyed for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system. This question also includes conveyance of any Master Key and hierarchy key components (e.g., if operating multiple production data centers and/or host hardware security modules and/or hardware platforms, etc.). This question also includes any keys used for internal PIN translations that may occur in the system, or keys used internally.

_Intent of Question_

To ensure that:

- Adequate and appropriate documented written procedures exist for the conveyance of all cryptographic keys.
- Documented procedures are followed and that keys are not conveyed in any other (especially non-compliant) manner.

_Audit Technique_

Review existing documentation for completeness. See Question 7.
Key loading to hosts and to PIN entry devices is handled in a secure manner.

This Control Objective covers Questions 12-16 of the Self-Audit Questionnaire. The processes and equipment utilized to load keys and their components must not allow for the compromise of these keys; they must also include a validation mechanism to ensure the authenticity of the keys.

Question 12–Key Loading to TRSM

How are keys loaded to TRSMs?

Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.

The Master File Key and any Key Encryption Key, when loaded from the individual key components, must be loaded using the principles of dual control and split knowledge. Procedures must be established that will prohibit any one person from having access to all components of a single encryption key.

Host Security Module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA.

For manual key loading, dual control requires split knowledge of the key among the entities. Manual key loading may involve the use of media such as paper or specially designed key-loading hardware devices.

Any other TRSM loaded with the same key components must combine all entered key components using the identical process.

Key establishment protocols using public key cryptography may also be used to distribute PED symmetric keys. These key establishment protocols may use either key transport or key agreement. In a key transport protocol, the key is created by one entity and securely transmitted to the receiving entity. For a key agreement protocol, both entities contribute information, which is then used by the parties to derive a shared secret key.

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

- Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA).
- Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question.
- Provide for mutual device authentication for both the host and the PED, including assurance to the host that the PED actually has (or actually can) compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key.
**Applicability–Question Scope**

This question applies to:

- Key loading to HSMs and PEDs.
- All keys (symmetric and asymmetric) and symmetric key components loaded to all ATMs, PIN pads, and PIN entry devices.
- The loading of any Master Key and hierarchy key components to a site's HSMs.

**Intent of Question**

- To ensure that no one knows the final key during key loading (knowledge of any one key component gives no knowledge of the final key). (For DES, the method to implement this is to enter the cryptographic key values as two or more components, each of which is equal in size to the actual key.)

**Audit Technique–Loading into HSMs**

Interview appropriate personnel and review documentation to determine the procedures for key loading to the HSM.

Demonstration/walk through of the usage of any equipment (terminals, PIN pads, etc) used as part of the key loading process.

Examine logs of access to security containers that passwords, PROMs, smartcards, brass keys, etc. are stored in to ensure dual control.

Ensure key loading devices can only be accessed and used under dual control.

Examine vendor documentation describing options for how the HSM MF is created. Corroborate this with information gathered during the interview process and procedural documentation provided by the entity under review.

**Audit Technique–Loading to PEDs**

Interview appropriate personnel and review documentation to determine the procedures for key loading to PEDs.

Demonstration/walk through of the usage of any equipment (terminals, external PIN pads, key guns, etc) used as part of the key loading process.

Examine logs of access to security containers for key components.

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 PED.
Audit Technique—Loading to Both HSMs and PEDs

Interview appropriate personnel to determine the number of key components, the length of the key components, and the methodology used to form the key for each interchange related key identified in the network schematic. If other mechanisms do not exist to verify key component length, a custodian may be requested to examine a component stored on paper.

Examine HSM and PED vendor documentation to determine the methodologies (XOR, DEA, Concatenation) supported for the combination of key components.

Witness a structured walk through/demonstration of various key generation processes for all key types (MKs, AWKs, TMKs, etc.). Verify the number and length of the key components generated to information provided through verbal discussion and written documentation. Also verify that the process includes the entry of individual key components by the designated key custodians.

Ensure check values from the HSM and verify that PED are the same during the key loading demonstration.

- Custodians do NOT hand their components to a third party to enter.
- Components are full-length (two or more components, each of which is equal in size to the actual key) and are NOT 8 character halves that are concatenated together.
- HSM brass keys are held under dual control.

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>While the requirement implies that keys can only be loaded from paper components with values entered by designated key custodians, other compliant methods exist. The most common non-paper method is the entry of key components by means of &quot;chip&quot; cards or similar secure tokens, with each card holding one component. In all cases the principles of split knowledge and dual control must be followed.</td>
</tr>
</tbody>
</table>
Question 13–Key Loading Protection

Is the key-loading process free from monitoring from an unauthorized third party?

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

TRSM equipment must be inspected to detect evidence of monitoring and to ensure that the key loading occurs under dual control.

A TRSM must transfer a plaintext key only when at least two authorized individuals are identified by the device (e.g., by means of passwords or other unique means of identification).

Plaintext keys and key components must be transferred into a TRSM only when it can be ensured that there is no tap at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys, and that the device has not been subject to any prior tampering which could lead to the disclosure of keys or sensitive data.

The injection of key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) results in either of the following:

- The medium is placed into secure storage, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device, or
- All traces of the component are erased or otherwise destroyed from the electronic medium.

For keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:

- The key-loading device is a physically secure TRSM, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; and
- The key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it; and
- The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another TRSM. Such personnel must ensure that a key-recording device is not inserted between the TRSMs; and
- The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.

The media upon which a component resides must be physically safeguarded at all times.
Any tokens, EPROMs, or other key component holders used in loading encryption keys must be maintained using the same controls used in maintaining the security of hard copy key components. These devices must be in the physical possession of only the designated component holder and only for the minimum practical time.

If the component is not in human comprehensible form (e.g., in a PROM module, in a smart card, on a magnetic stripe card, and so forth), it is in the physical possession of only one entity for the minimum practical time until the component in entered into a TRSM.

If the component is in human readable form (e.g., printed within a PIN-mailer type document), it is only visible at one point in time to only one person (the designated component custodian) and only for the duration of time required for this person to privately enter the key component into a TRSM.

Printed key component documents are not opened until just prior to entry. The component is never in the physical possession of an entity when any one such entity is or ever has been similarly entrusted with any other component of this same key.

**Applicability–Question Scope**

This question applies to:

- Key loading mechanisms and the process of loading all cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing.
- Key loading process of Master Keys and hierarchy keys.
- Key loading process of any keys used for internal PIN translations that may occur in the system, or keys used internally.

**Intent of Question**

To ensure:

- Security and integrity of keys during the key loading process into a TRSM—specifically to ensure no visual or electronic surveillance or monitoring occurs during the key transfer process.
- Secrecy and the integrity of keys transported from the location of generation to the location of loading in an electronic key loading device (KLD).
- Security of the KLD.
- That the KLD is a TRSM.
- The KLD is designed or controlled so it cannot output a key into another TRSM except under dual control.

**Audit Technique**

Interview appropriate personnel and review documentation to determine the procedures for key loading to HSMs and PEDs. Review any logs of key loading. Ensure all documentation supports the key loading process is in accordance with this question's requirements.
Observe/demonstration/walk through of the usage of any equipment (terminals, PIN pads, key guns, etc.) that is part of the key loading process.

Inspect the environment(s) where key loading occurs.

Ensure cameras cannot monitor the entering of key components.

Ensure dual control mechanisms and dual control custody of the key loading devices and of the key loading process.

Ensure the TRSM equipment is inspected for evidence of monitoring.
Electronic monitoring would normally be accomplished by attaching taps on the cable between the PIN pad and the encryptor board or by tapping the line between the ATM and the host. Physical inspection of the device should be performed to identify and remove any such devices.

Ensure there are no default dual control mechanisms (e.g., default passwords –usually printed in the vendor’s manual–in a key loading device).

Validate that key loading procedures include instructions to delete the keys from the key loading device after successful transfer.
Question 14–Key Loading Hardware Dual Control

Is key-loading hardware under dual control?

All hardware and passwords used for key loading are managed under dual control. Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. Use of the equipment must be monitored and a log of all key-loading activities maintained for audit purposes. All cable attachments must be examined before each application to ensure they have not been tampered with or compromised.

Any physical (e.g., brass) key(s) used to enable key loading must not be in the control or possession of any one individual who could use those keys to load cryptographic keys under single control.

Applicability–Question Scope

This question applies to:

• Key loading equipment, specifically to ensuring dual control over the equipment and/or any enabling passwords used with the key loading devices.
• It also applies to key loading equipment used to load: all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing.
• Master Keys and hierarchy keys.
• Any keys used for internal PIN translations that may occur in the system, or keys used internally.

Intent of Question

• To ensure the secrecy and integrity of keys during the key loading process, specifically to contribute to this by ensuring dual control over the use of key loading devices.

Audit Technique

Interview appropriate personnel and review documentation to determine the procedures for the use of any key loading equipment or device enablers that are used for either HSMs or PEDs. Examine emergency procedures in order to determine whether dual control rules are violated under those circumstances.

Inspect storage locations of key loading equipment (including physical brass keys used to enable loading, passwords, key guns, etc.) to ensure enforcement of dual control (procedural controls are not adequate).

Review logs of equipment usage to determine documentation of dual custody and that only authorized individuals have access.

Ensure dual control mechanisms and dual control custody of the key loading devices and of the key loading process.
Ensure the TRSM equipment is inspected for evidence of monitoring.

Ensure there are no default dual control mechanisms (e.g., default passwords—usually printed in the vendor's manual—in a key loading device).

Verify that if passwords are used for key loading, they are under dual control.

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>There was a bank with many HSMs, each of which had both copies of both brass keys dangling from the locks. Anyone with access to the data center, including guards, vendors, cleaners, and technical staff, could have turned the keys, hit the Reset button, lifted a tile, tossed the keys under the raised floor, and walked away, having put this major bank out of the ATM business for a considerable period of time. These keys usually come with a little aluminum tag containing a key number. Note this number because you will need it to get extra keys.</td>
</tr>
</tbody>
</table>
Question 15–Key Validation

Is the key validated after loading?

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

A cryptographic-based validation mechanism helps to ensure the authenticity and integrity of keys and components (e.g., testing key check values, hashes or other similar unique values that are based upon the keys or key components being loaded).

Applicability–Question Scope

This question applies to:

- Mechanisms (e.g., key check values, hashes, etc.) that validate the keys and key components that are loaded.
- Key loading validation mechanisms used to load all cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing.
- Key loading validation mechanisms used to load Master Keys and hierarchy keys.
- Key loading validation mechanisms used to load any keys used for internal PIN translations that may occur in the system, or keys used internally.

Intent of Question

- To ensure the integrity and authenticity of keys after loading. To be able to validate that the key on the system is in fact the key that is desired to be on the system, (i.e., to ensure that the key was not tampered with, substituted, or compromised during the loading process).

Audit Technique

Interview appropriate personnel and review documentation (including both logs and procedural) to determine the mechanisms used to validate the authenticity of the keys loaded to HSMs and PEDs.

Review vendor documentation to determine which methods of verification for key loading are supported.

Observe a demonstration of the key loading process.

If check values are used, compare key check values against those for known, default, test, predictable, easily guessed or “simple” keys. Such check values are often printed in vendor manuals.
Question 16–Key-Loading Procedures

**Is key-loading documentation in place?**

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

Written procedures must exist and be known to all parties involved in cryptographic key loading. All key loading events must be documented.

**Applicability–Question Scope**

This question applies to written procedures that describe how all cryptographic keys are loaded. This applies to all keys loaded into all ATMs, PIN pads, PIN entry devices, host security modules and key loading devices.

**Intent of Question**

To ensure that:

- Adequate and appropriate documented written procedures exist for the loading of all cryptographic keys.
- Documented procedures are followed and keys are not loaded in any other (especially non-compliant) manner.

**Audit Technique**

Review existing documentation for completeness. See Question 7 for details.
Control Objective 5- Prevent Unauthorized Usage

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

This Control Objective covers Questions 17-20 of the Self-Audit Questionnaire. It includes questions on whether all keys are unique to either an endpoint device and its host or to a network (peer-to-peer) connection. It also seeks to ensure that keys are used for their sole, intended purpose.

Question 17—Unique Network Node Keys

All keys that link network nodes are unique.

Unique cryptographic keys must be in use for each identifiable link between host computer systems.

Where two organizations share a key to encrypt PINs (including key encipherment keys used to encrypt the PIN encryption key) communicated between them, that key must be unique to those two organizations and must not be given to any other organization.

This technique of using unique keys for communication between two organizations is referred to as “zone encryption” and is required. Keys may exist at more than one pair of locations for disaster recovery or load balancing (e.g., dual processing sites).

Applicability—Question Scope

This question applies to all cryptographic keys for all network processor links to the site’s host system for all directions of PIN flow—incoming and outgoing. This question applies to keys that encrypt PINs and to keys that encrypt other keys on every such network link. Note that this question does not apply to any of the PED terminal links or to any internal paths. Examine all cryptograms on every network link to ensure there are no duplicates. (Note that a PIN key may be the same as a key encrypting key but the cryptograms will be different if variants of the MFK are used to encipher different key types, although the check digit will be the same. Also, it is still possible to compare all PIN encrypting keys’ cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other, and then to separately compare all key encrypting keys’ cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other.)

Intent of Question

To:

- Compartmentalize the risk associated with disclosure of a host link (interfacing processor) key, so that the risk is limited to just that one processor, and so that the discovery of that one key does not provide information to determine the key used on any of the site’s other links.
- Eliminate the use of known keys.
- Avoid the use of default, test, predictable, easily guessed or “simple” keys (e.g., 0123456789abcdef, alternating 0s and 1s, etc.).
Audit Technique

Using the network schematic from the preliminary step, interview responsible personnel to determine which keys are shared between this and other entities (or possibly other organizational units of this entity).

Examine system documentation to verify information provided during interviews. This is mandatory if personnel have indicated the use of unique keys with other organizations:

- Obtain check values for any master file keys and interchange based zone keys, including other interchange networks to verify key uniqueness.
- For internally developed systems, review system design documentation or source code for uniqueness of cryptograms.
- For application packages, examine parameter files where the cryptograms of keys shared with other network nodes are specified (e.g., the KEYF file for Base 24. Ensure the correct number of cryptograms exist (account for each network link) and that there are unique values for each link.
- Examine PIN translation transactions in a trace log and ensure that the “from” cryptographic key does not equal the “to” cryptographic key (this assumes the keys are encrypted under the same variant of the same KEK).

Corroborate this information to what is determined during the review of key generation, storage and destruction.

Compare all PIN encrypting key cryptograms on every network link to ensure there are no duplicates. Then compare all key encrypting key cryptograms on every network link to ensure there are no duplicates. (Note that a PIN key may be the same as a key encrypting key but the cryptograms will be different if variants of the MFK are used to encipher different key types, although the check digit will be the same. Also, it is still possible to compare all PIN encrypting keys' cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other, and then to separately compare all key encrypting keys' cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other.)

Compare key check values against those for known, default, test, predictable, easily guessed or “simple” keys. Such check values are often printed in vendor manuals.
Question 18–Key Substitution Prevention

Are key substitution procedures in place?

Procedures exist to prevent or detect the unauthorized substitution of one key for another or the operation of any cryptographic device without legitimate keys.

The unauthorized substitution of one stored key for another, whether encrypted or unencrypted, must be prevented. This will reduce the risk of an adversary substituting a key known only to them. These procedures must include investigating multiple synchronization errors.

To prevent substitution of a compromised key for a legitimate key, key component documents that show signs of tampering must result in the discarding and invalidation of the component and the associated key at all locations where they exist.

Applicability–Question Scope

This question applies to the procedures that need to exist to protect against unauthorized key substitution for all cryptographic keys for all ATMs PIN pads, PIN entry devices and network processor links to the site’s host system for all directions of PIN flow—incoming and outgoing. This question also refers to protections against substitution of Master Keys and hierarchy keys, and any keys used for internal PIN translations that may occur in the system or keys used internally. This question applies to protections on all TRSMs that can experience cryptographic synchronization errors.

Intent of Question

To:

- Prevent and detect the unauthorized substitution of keys.
- Prevent misuse of a TRSM to determine keys and PINs by exhaustive trial and error.
- Ensure procedures are executed when multiple synchronization errors occur.

Audit Technique

Interview appropriate personnel and review techniques and procedural documentation pertaining to preventing key substitution.

Ensure procedures/policy does not allow HSMs to remain in the “authorized” state when connected to online production systems.

Ensure that keys no longer needed are destroyed, especially those keys used to encipher other keys for distribution.
Ensure there is some “velocity checking” on multiple cryptographic synchronization errors (PIN synchronization errors) and ensure procedures exist to investigate such occurrences. Those procedures need to include specific actions that determine whether the legitimate value of the cryptographic key has changed, such as encryption of a known value to determine whether the resulting cryptogram matches the expected result. The procedures need to ensure that proactive safeguards are in place that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.

Ensure controls exist over the access to and use of devices (e.g., KKTs and SCTs) used to create cryptograms.

In the case of paper components, review procedures and discuss with key custodians the steps that are taken whenever a key component appears to have been tampered with. These procedures must include a requirement to immediately replace any key whose components may have been tampered with as well as any key ever stored or transported under the suspect key.

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why would anybody do this, given that the transaction will not go through successfully? One scenario has an attacker tapping into outbound messages from an ATM, which is not difficult to do from dial-up devices. By substituting a key, he can decrypt PIN blocks until the device is reset. With the PIN (that he decrypted) and the account data (from the stripe), a counterfeit card is just a hotel key and an encoder away. By the way, one common reaction is for new keys to be downloaded from the Host. If an attacker has tapped into the line and knows the encryption key used to protect the new PIN Encryption key, the downloaded new key is also ascertainable. This is another strong argument for the implementation of unique keys in all devices.</td>
</tr>
</tbody>
</table>
Question 19–Single Purpose Keys

Are keys used for a single purpose?

Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.

Encryption keys must only be used for the purpose they were intended (e.g., Key Encryption Keys must not to be used as PIN Encryption Keys). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended to be used also significantly strengthens the security of the underlying system. Keys must never be shared or substituted in a processor's production and test systems.

Applicability–Question Scope

This question applies to:

- All cryptographic keys used at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing.
- Any keys used for internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”).
- All Master Keys or hierarchy keys used in the system. This question applies to all keys in both the test and production environments.

Intent of Question

To:

- Minimize damage that can result from a key compromise.
- Ensure that test keys are not used in a production environment and to ensure that production keys are not used in a test environment.
- Ensure there is a separation of keys to minimize misuse (for example so that HSMs cannot be “tricked” into decrypting PINs with a “Decrypt Data” command through the use of a mechanism that ensures that the commands recognize the purpose of the keys and force the use of separate types of keys).

Audit Technique

Using the network schematic from the preliminary step, interview responsible personnel to determine which keys exist at various points in the interchange process, whether any keys are used to encipher other keys and to encipher any data (including PIN blocks) and whether keys are shared between production and test.

Obtain check values for master file keys for both production and test environments and ensure they are different values.

Examine the cryptograms and key check values in both the production and test systems to ensure that all keys are different.
Examine system documentation to verify information provided during interviews—this is mandatory if personnel have indicated the use of unique keys. Coordinate this with steps in questions 17 and 20.

Ensure that if new PIN Encryption Keys are periodically downloaded to an ATM, the new PEK must not be encrypted under the old PEK.
Question 20–Unique PED Keys

Are unique keys used?

All cryptographic keys ever present and used for any function (e.g., key encipherment or PIN encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device.

Any key used to encrypt a PIN in a PED must be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations. Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.

In a master/session key approach, the master key(s) and all session keys must be unique to each cryptographic device.

If a transaction-originating terminal interfaces with more than one Acquirer, the transaction-originating terminal TRSM must have a completely different and unique key or set of keys for each Acquirer. These different keys, or set of keys, must be totally independent and not variants of one another.

Keys that are generated by a derivation process and derived from the same Base Key must use unique data for the derivation process so that all such cryptographic devices receive unique initial keys.

Applicability–Question Scope

This question applies to:

- All cryptographic keys for all ATMs, PIN pads, and PIN entry devices to the site's host system for all incoming PINs.
- Keys that encrypt PINs and to keys that encrypt other keys on every such terminal link. (Note that this question does not apply to any of the network links or to any internal paths. Examine all cryptograms on every terminal link to ensure there are no duplicates.) (Note that a PIN key may be the same as an enciphering key, but the cryptograms will be different if variants of the MFK are used to encipher different key types, although the check digit will be the same. Also, it is still possible to compare all PIN encrypting keys' cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other, and then to separately compare all key encrypting keys' cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other.)

Intent of Question

To:

- Compartmentalize the risk associated with disclosure of a device key, so that the risk is limited to just that one device, and so that the discovery of that one key does not provide information to determine the key in any other device.
- Eliminate the use of known keys.
• To avoid the use of default, test, predictable, easily guessed or “simple” keys (e.g., 0123456789ABCDEF, alternating 0s and 1s, etc.).

Audit Technique

Interview responsible personnel to determine which keys are shared between multiple PEDs.

Examine system documentation to verify information provided during interviews. This is mandatory if personnel have indicated the use of unique keys per PED:

• Obtain check values for a sample of PEDs keys (both TMKs and PEKs) to verify key uniqueness.
• For internally developed systems, review system design documentation or source code (or any program/compiled files) for uniqueness of cryptograms.
• For application packages, examine parameter files where the cryptograms of keys used for PEDs are specified (e.g., the TDF file for Base 24).
• Examine PIN translation transactions in a trace log and ensure that the “from” cryptographic key does not equal the “to” cryptographic key (this assumes the keys are encrypted under the same variant of the same KEK).

Corroborate this information to what is determined during review of key generation, storage and destruction.

Have the technical staff sort all of the key encrypting key cryptograms for every terminal link, and sort all of the PIN encrypting key cryptograms for every terminal link. Ask for a printout of the sorted information including the terminal ID numbers and check digits if available. Compare all PIN encrypting key cryptograms on every terminal link to ensure there are no duplicates. Then compare all key encrypting key cryptograms on every terminal link to ensure there are no duplicates. (Note that a PIN key may be the same as a key encrypting key but the cryptograms will be different if variants of the MFK are used to encipher different key types, although the check digit will be the same. Also, it is still possible to compare all PIN encrypting keys’ cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other, and then to separately compare all key encrypting keys’ cryptograms encrypted by the same value (i.e., MFK variant) to see if they are duplicates of each other). Compare key check values for all keys on all terminal links to ensure there are no duplicates.

Compare key check values against those for known, default, test, predictable, easily guessed or “simple” keys. Such check values are often printed in vendor manuals.

Perform a comparison check between the number of devices being operated and the number of cryptographic keys in use. If there are fewer keys than devices, it is clear that the same key is being used in several places.

Examine "emergency" procedures in an attempt to identify situations where otherwise compliant procedures are violated. Such emergency procedures are sometimes invoked when an ATM goes out of service after normal business hours or when certain staff members are not available. Ensure these procedures support this question’s requirements for unique PED keys.
TIPS, TRICKS, AND STRANGE OBSERVATIONS

Although the use of unique keys in each PIN entry device has been required by ANSI since 1982, by Visa since the early 1990s, and by Plus since 1998, it still elicits both surprise and resistance from many entities. Some arguments stated against compliance are:

"We have too many ATMs." Several banks with more than 8,000 ATMs are in full compliance.

"Our ATMs are spread too far." A Canadian bank with ATMs spread 4,000 miles East to West, with a number North of the Arctic Circle is in full compliance.

"I can't afford to send two people to start an ATM." The typical ATM only needs to have a key reloaded less frequently than once a year because of battery-backed RAM. The institution promised to follow all the rules when it signed up.

"Our software won't handle different keys." Your software is totally unsuitable for the current environment. If you wrote it, fix it; if you bought it, tell the supplier to fix it. Work through a User Group, if one exists.

"Where can I store the components?" Maybe put one in the money vault and the other in a little strongbox glued or welded to the ATM. (Be clever, you'll come up with something appropriate.) (Note that this is only necessary if you are intending to reuse the same keys in the event the ATM loses its key(s) because of an extended power outage).

"How can I generate all those keys?" Make it a weekend project with pizzas and sodas provided as lunch.

TIPS, TRICKS, AND STRANGE OBSERVATIONS

Visa has been working with ATM manufacturers, software and hardware suppliers, and a representative sample of members to develop a methodology that uses asymmetric cryptography to download unique DES keys to ATMs, eliminating the need for human interaction. Certain forward-looking members are already implementing methods like this. As you decide upon a unique key strategy, keep these developments in mind and feel free to contact Visa for the most current information.
Control
Objective 6-
Secure Key
Administration

Keys are administered in a secure manner.

This Control Objective covers Questions 21-28 of the Self-Audit Questionnaire. It includes requirements for key storage, compromise, and destruction.

Question 21–Permissible Key Forms

Are keys and key components managed securely?

Keys used for enciphering PIN Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.

Effective implementation of these principles requires the existence of barriers beyond procedural controls to prevent any custodian (or non-custodian for any individual component) from gaining access to all key components. An effective implementation would have physically secure and separate locking containers that only the appropriate key custodian (and their designated backup) could physically access.

Components for a specific key that are stored in separate envelopes, but within the same secure container place reliance upon procedural controls and do not meet the requirement for physical barriers. Furniture-based locks, or containers with a limited set of unique keys are not sufficient to meet the requirement for physical barriers.

Key components may be stored on tokens (e.g., PC cards, smart cards, and so forth). These tokens must be stored in a special manner to prevent unauthorized individuals from accessing the key components. For example, if key components are stored on tokens that are secured in safes, more than one person might have access to these tokens. Therefore, additional protection is needed for each token (possibly by using tamper-evident envelopes) to enable the token's owner to determine if a token was used by another person. In particular, key components for each specific custodian must be stored in separate secure containers.

If a key is stored on a token and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup) must have possession of both the token and its corresponding PIN.

Printed or magnetically recorded key components must reside only within tamper-evident sealed envelopes so that the component cannot be ascertained without opening the envelope.

DES keys that are used to encipher other keys or to encipher PINs, and which exist outside of a TRSM, must be enciphered using either:

- The TDEA using at least double length keys, or
- RSA using a key modulus of at least 1024 bits.
A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.

Symmetric secret keys may be enciphered using public key cryptography for distribution to PEDs as part of a key-establishment protocol as defined in Requirement 12.

**Applicability–Question Scope**

This question applies to all keys used to encrypt PINs and to all keys used to encrypt those keys.

**Intent of Question**

- To ensure clear keys are not exposed across network links or on databases, software programs, computer memory, electronic media, or system logs, backup tapes, etc.

**Audit Technique**

Using the network schematic from the preliminary step, interview responsible personnel to determine which keys are stored as components and on which type of media they are stored (paper, PROM, smartcard, etc.). Keys that will probably be managed as components include ATM initialization keys, Base derivation keys, Master keys and Key Exchange Key components shared with other networks.

Examine documented procedures to determine the algorithms and key sizes used for storing encrypted keys.

Examine vendor documentation describing options for usage of key encipherment keys. Corroborate this with information gathered during the interview process and procedural documentation provided by the entity under review.

Physically verify the location of all interchange based key components, including the inspection of any containers for those components. For each of the keys identified in the first paragraph above under “Audit Technique,” identify the key custodians and perform a physical inventory to verify that each key is managed as two or more full-length components. Be alert for instances where both components of a key are stored together or where the non-random test value is not stored at all, but rather known to a number of current and former employees and third party staff.

Identify all individuals with access to components and trace that access to key custodian authorization forms.

Examine logs of access to the key components to ensure only authorized custodians access components, PROMs, smartcards, etc., including verification of tamper evident serial numbers.

Ensure there are no clear keys stored in containers, in databases, on floppy disks, and in software programs (as is done when performing software PIN translates).
Ensure key components are not XOR'ed or otherwise combined in software programs.

Ask to see inside the key entry area of one or more production ATMs. Often, start-up instructions and other notes used by service technicians are kept here. In a number of cases, a review of these startup instructions reveals that the initialization key values are written in the clear at the point in the checklist where the DES keys are entered. This is obviously a major breach of security as the initialization keys as well as all the keys that they protect are now compromised. Also review operations manuals to ensure that no confidential information has been written "in the margins."

Inspect key-loading procedures for HSMs to ensure that no key component values have been recorded in inappropriate places.

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Here is where we find the greatest disparity between theory and practice. While many institutions have staff members who understand that the only security offered by DES lies in maintaining the confidentiality of the key, we often find keys managed as cleartext strings, written in the clear in documents or dictated over the telephone, sometimes to people claiming to be third-party personnel.</td>
</tr>
<tr>
<td>Promote the use of pre-numbered, tamper-evident envelopes for key component storage. These envelopes, plus a log, can completely document whether an unauthorized access has been made. Remember, having a break-in is bad enough, but having a break-in and not being aware of it is infinitely worse.</td>
</tr>
</tbody>
</table>
Question 22–Key Compromise Procedures

Do key compromise procedures exist?

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

Key components are never reloaded when there is any suspicion that either the originally loaded key or the device has been compromised. If suspicious alteration is detected, new keys must not be installed until the TRSM has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.

A cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. In addition, all keys encrypted under or derived using that key must be replaced with a new key within the minimum feasible time. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.

Procedures must include a documented escalation process and notification to organizations that currently share or have previously shared the key(s). The procedures should include a damage assessment and specific actions to be taken with system software and hardware, encryption keys, encrypted data, and so forth.

The compromise of a key requires the replacement and destruction of that key and all variants and non-reversible transformations of that key, as well as all keys encrypted under or derived from that key. Known or suspected substitution of a secret key requires replacement of that key and any associated key encipherment keys.

Specific events must be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:

- Missing cryptographic devices.
- Tamper-evident seals or envelope numbers or dates and times not agreeing with log entries.
- Tamper-evident seals or envelopes that have been opened without authorization or show signs of attempts to open or penetrate.
- Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.

If attempts to load a key or key component into a cryptographic device fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased or otherwise destroyed in the original device.
Applicability—Question Scope

This question applies to the key compromise procedures that need to exist for all cryptographic keys for all ATMs, PIN pads, PIN entry devices and network processor links to the site's host system for all directions of PIN flow—incoming and outgoing. This question also refers to Master Keys and hierarchy keys, and any keys used for internal PIN translations that may occur in the system or keys used internally. This question also applies to all subsidiary keys of compromised keys.

Intent of Question

• To ensure a proactive, well-conceived, (not reactive) plan is established for expedient and efficient execution should a key compromise occur, in order to minimize the fraudulent activities and also the potential adverse effects to other organizations that may result due to key compromise, and to effectively communicate such to all interested parties.

Audit Technique

Interview appropriate personnel and examine documented procedures to determine the adequacy of key compromise procedures.

If written procedures do not exist for replacing compromised keys, the institution is out of compliance. If written procedures do exist, review them to verify that all of the steps needed to generate and deploy a random key are in place. Also verify that for each key in the institution's key suite, the keys protected or transported under each key are listed. This allows the recovery team to assess the scope of the recovery process. Ensure that the procedures include the names and/or functions of each staff Member assigned to the recovery effort, as well as phone numbers and the place where the team is to assemble.
Question 23–Key Variants

Are key variants used correctly?

Key variants are only used in those devices that possess the original key.

A key used to encrypt a PIN must never be used for any other cryptographic purpose. A key used to protect the PIN Encrypting Key must never be used for any other cryptographic purpose. However, variants of the same key may be used for different purposes.

Variants of an MFK must not be used external to the (logical) configuration that houses the MFK itself.

Applicability–Question Scope

This applies to all cryptographic keys used at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site’s host system and for all directions of PIN flow—incoming and outgoing. This also applies to any keys used for internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”). This question also applies to all Master Keys or hierarchy keys used in the system.

Intent of Question

- To ensure there is a separation of keys to minimize misuse (for example so that HSMs cannot be “tricked” into decrypting PINs with a “Decrypt Data” command through the use of a mechanism that ensures that the commands recognize the purpose of the keys and force the use of separate types of keys).

For example, some types of Hardware Security Modules (Atalla, Racal) do not encrypt other keys under the actual MFK, but under a variant. A variant of a key is the result of combining the key with a known value (typically done by the XOR process) to derive another key. Variants in HSMs are used to segregate cryptograms into groups based on the type of key being encrypted (Key Exchange Key, Working Key). It is a requirement that no variant of a key exist in any device that does not also contain the original key.

Audit Technique

Interview responsible personnel to determine which 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.

Review vendor documentation to determine support for key variants.

Examine the key creation and injection process to ensure that a unique key is generated and loaded into each PIN entry device and that it is not just a variant of an existing key.
Question 24—Secure Destruction of Obsolete Keys

Are obsolete keys securely destroyed?

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

Instances of keys that are no longer used or that have been replaced by a new key must be destroyed. Keys maintained on paper must be burned, pulped or shredded in a cross-cut shredder. If the key is stored in EEPROM, the key should be overwritten with binary 0s (zeros) a minimum of three times. If the key is stored on EPROM or PROM, the chip should be smashed into many small pieces and scattered. Other permissible forms of a key instance (physically secured, enciphered or components) must be destroyed following the procedures outlined in ISO-9564-1 or ISO-11568-3. In all cases, a third party—other than the custodian—must observe the destruction and sign an affidavit of destruction.

The procedures for destroying keys that are no longer used or that have been replaced by a new key must be documented.

Key encipherment key components used for the conveyance of working keys must be destroyed after successful loading and validation as operational.

Applicability—Question Scope

This question applies to:

- All cryptographic keys used at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing.
- Any keys used for internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”).
- All Master Keys or hierarchy keys used in the system.

Intent of Question

- To prevent the misuse or mismanagement of the inactive key that could potentially lead to compromise of data and loss of integrity to the active system, and to minimize the damage to the active key hierarchy should the inactive key be compromised.

Audit Technique

Interview responsible personnel and identify all keys that have been destroyed.

Examine all logs of destruction. Note that all key encipherment keys should be traceable to either storage or destruction.

Examine key history logs and key destruction logs to determine compliance.
During the physical inventory of key components, be alert for any envelopes that cannot be accounted for on the list of keys expected to be stored in the container. It is not uncommon to find keys that were in use by entities that have been absorbed by merger or keys linking the institution to networks that no longer exist. Be particularly alert for Master File keys that have been replaced.

Search for Visa-supplied key components, referred to as a Zone Control Master Key (ZCMK). There is a Visa requirement that these components must be destroyed shortly after the key has been successfully loaded to the system.

### TIPS, TRICKS, AND STRANGE OBSERVATIONS

You may run into someone who is reluctant to allow key components to be destroyed. "What if we need to reload it in the future?" is the usual refrain. Remind anyone who says this that as long as you have copies of the Master key and cryptograms of the other keys encrypted under the Master, you can reload the Master key and copy the cryptograms back to the database, thus restoring all of the keys.

One good trick is to have the affidavit of destruction as a part of the same piece of paper that contains the key component value itself. To destroy the key, tear off the section of the sheet that contains the value, destroy it, sign and witness the affidavit and log it.
Question 25—Limit Key Access

Is cryptographic key access limited?

Access to cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.

Limiting the number of key custodians to a minimum helps reduce the opportunity for key compromise. In general, the designation of a primary and a backup key custodian for each component is sufficient. This designation must be documented by having each custodian sign a Key Custodian Form. The forms must specifically authorize the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them.

Applicability—Question Scope

This question applies to:

- All cryptographic keys used at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing.
- Any keys used for internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”).
- All Master Keys or hierarchy keys used in the system.

Intent of Question

- To reduce the possibility of key compromise. This is ultimately to protect against PIN compromise.

Audit Technique

Interview responsible personnel and identify all individuals with access to components and trace to key custodian authorization forms. Compare information to the individuals who open secure containers.

Examine logs of access to keys and key materials to ensure only authorized custodians access components, PROMs, smartcards, etc., including verification of tamper evident serial numbers.

TIPS, TRICKS, AND STRANGE OBSERVATIONS

On more than one occasion, we have discovered that the people that had access to safes containing key components had not been designated as key custodians. This meant that the designated key custodians had responsibility without authority. Remember, designated or not, the people that can gain access to the components are de facto key custodians and assignments should be made accordingly.
Question 26—Log Key Access

Is key access logged?

Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.

At a minimum, the logs must include the date and time in/out, purpose of access, signature of custodian accessing the component, envelope number (if applicable).

Applicability—Question Scope

This question applies to:

- All containers that secure cryptographic materials. Each such container must have a log. Contents of the containers may include cryptographic keys (components) used at all ATMs, PIN pads, PIN entry devices, and network processor links connected to the site's host system and for all directions of PIN flow—incoming and outgoing.
- Any keys used for internal PIN translations that may occur within the host system (e.g., if the application uses a “Switch Working Key” or SWK, or “Intermediate Key”).
- All Master Keys or hierarchy keys used in the system.

Intent of Question

- To maintain an audit trail of access to stored cryptographic materials.

Audit Technique

Review logs for completeness. Inspect logs for any discrepancies.

Attempt to identify anomalies, such as a key that remained out of storage for an excessive time or an access that did not have a corresponding key load event.
Question 27—Backup Keys

Are backup keys stored securely?
Backups of secret keys must exist only for the purpose of reinstating keys that are accidentally destroyed. The backups must exist only in one of the allowed storage forms for that key.

The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as keys in current use (see Requirement 21).

Backups (including cloning) must require a minimum of two authorized individuals to enable the process.

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

Applicability—Question Scope
This applies only to backup copies of keys and key components.

Intent of Question
• To ensure the secrecy and integrity of keys, minimize the potential for their exposure, minimize the number of potential “attack points” and minimize the number of places where controls need to be established for the management of keys.

Audit Technique
Interview responsible personnel and determine whether any copies of keys or their components exist for backup/recovery or disaster recovery purposes.

Inspect location of key components stored for backup/recovery or disaster recovery purposes. Determine that no obsolete key materials are being retained and that the storage arrangements are satisfactory. Inspect any key logs in order to identify any unusual access events.

Review disaster recovery plans and discuss them with the responsible staff. The intent here is to identify any circumstance that could cause normal security procedures to be breached.

<table>
<thead>
<tr>
<th>TIPS, TRICKS, AND STRANGE OBSERVATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be alert for branches that are being closed or renovated. Try to get a section of safe deposit boxes to be used for the storage of key components, HSM brass keys and key-loading equipment. Also, ensure that the backups are stored where they will not be lost in the event of a catastrophe at the primary site.</td>
</tr>
</tbody>
</table>
Question 28–Key Administration Procedures

*Is key administration documented?*

Documented procedures exist and are demonstrably in use for all key administration operations.

Written procedures must exist and be known to all affected parties. All activities related to key administration must be documented.

**Applicability–Question Scope**

This question applies to written procedures that describe how all cryptographic keys are administered.

**Intent of Question**

To ensure that:

- Adequate and appropriate documented written procedures exist for the administration of all cryptographic keys.
- Documented procedures are followed, and that keys are not administered in any other (especially non-compliant) manner.

**Audit Technique**

Review existing documentation for completeness. See Question 7 for details.
Control
Objective 7-
Equipment
Management

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

This Control Objective covers Questions 29-32 in the Self-Audit Questionnaire. It includes requirements for both the placing into service as well as the decommissioning of cryptographic equipment. It also includes requirements for preventing the unauthorized use of specific types of cryptographic equipment.

Question 29—Equipment Inspection

Is PIN processing equipment inspected before use?

PIN processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.

HSMs and PEDs must only be placed into service if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering. This requires physical protection of the device up to the point of key insertion or inspection, and possibly testing of the device immediately prior to key insertion. Techniques include the following:

a. Cryptographic devices are transported from the manufacturer's facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.

b. Cryptographic devices are shipped from the manufacturer's facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident packaging. The devices are then stored in such packaging, or in secure storage, until key-insertion occurs.

c. The manufacturer's facility loads into each cryptographic device a secret, device-unique “transport-protection token.” The TRSM used for key-insertion has the capability to verify the presence of the correct “transport-protection token” before overwriting this value with the initial key that will be used.

d. Each cryptographic device is carefully inspected and perhaps tested immediately prior to key-insertion using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that is has not been subject to any unauthorized modifications.

- Devices incorporate self-tests to ensure their correct operation. Devices must not be re-installed unless there is assurance they have not been tampered with or compromised.

- Controls must exist and be in use to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.

Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to:

- protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it, and

- detect lost or stolen equipment.
Procedures must include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.

Notwithstanding how the device is inspected and tested, it is mandatory to verify the device serial number against the purchase order, invoice, waybill or similar document to ensure that device substitution has not occurred.

**Applicability—Question Scope**

This applies to all cryptographic equipment from the time of manufacture or removal of service to the time of initial key loading.

**Intent of Question**

To:

- Determine that only legitimate equipment is used and is operating properly and that equipment has not been subject to unauthorized modifications/tampering prior to loading keys.
- Prevent the ability to monitor and gain knowledge of keys and components during loading and use.

**Audit Technique**

Examine documentation and interview appropriate personnel.

To ensure that:

- Physical inspection and testing of the equipment occur immediately prior to key loading.
- Procedures ensure that inventory practices accurately track cryptographic equipment, including devices used for key loading.
- The equipment is physically protected to prevent or detect access by unauthorized personnel from the time of manufacture or removal from service to the time of initial key loading. For example:
  - Bonded carrier.
  - Device Authentication code injected by terminal vendor and verified by the terminal deployer.
  - Tamper evident packaging.

**Review all written purchasing, receipt and deployment procedures.** It is crucial that these procedures include a step that verifies the actual machine serial number against the serial number from the shipping waybill or manufacturer's invoice. Then discuss what pre-installation inspections take place. These should include both physical and functional tests as well as a thorough visual inspection.
Review how equipment is received and where it is "staged." It should remain in the original packaging until it is installed, unless it is received and staged at a secure facility. Be alert to gaps in the process that would allow an adversary to tamper with a device before it is placed into service.

Ascertain how serial numbers are loaded to the institution's asset register in order to determine if the identity of the installed device is known at the time of installation, or only later.

**TIPS, TRICKS, AND STRANGE OBSERVATIONS**

One clever method for bringing equipment into service is to use a well-designed script. Have the installation technician initial each step of the process and store the completed (and initialed) script in a log.
Question 30–Equipment Decommissioning Procedures

**Do equipment-decommissioning procedures exist?**

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

If a TRSM has been removed from service, all keys stored within the device that have been used (or potentially could be) for any cryptographic purpose must be destroyed.

- All critical initialization, deployment, usage, and decommissioning processes must impose the principles of dual control and split knowledge (e.g., key or component-loading, firmware or software-loading, and verification and activation of anti-tamper mechanisms).
- Key and data storage must be zeroized when a device is decommissioned.

If necessary to comply with the above, the device must be physically destroyed so that it cannot be placed into service again, or allow the disclosure of any secret data or keys.

**Applicability–Question Scope**

This question applies to all TRSMs that are removed from service.

**Intent of Question**

- To protect against the unauthorized use of a “production-cryptographically-capable” device.
- To protect against the disclosure of cryptographic keys and ultimately the disclosure of PINs.

**Audit Technique**

Interview appropriate personnel and review documentation of procedures to ensure that a proactive practice exists to ensure that cryptographic devices removed from service have all keys and keying materials destroyed.

Ensure that this process is also performed on all equipment being returned for repair.

ATMs and PIN pads removed from service can retain cryptographic keys (including PIN Encryption keys) in battery-backed RAM for days or weeks. Proactive key removal procedures must be in place to delete all such keys from equipment being removed from the network.

Host/Hardware Security Modules can also retain keys and of course, the Master File key is resident within these devices. Therefore, proactive key removal procedures must also be in place for HSMs.
Question 31–TRSM Procedures

**Do adequate TRSM security procedures exist?**

Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following:

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

Cryptographic equipment must be managed in a secure manner in order to minimize the opportunity for key compromise or key substitution. Physical keys, authorization codes, passwords, or other enablers must be managed so that no one person can use both the enabler(s) and the device which can create cryptograms of known keys or key components under a key encipherment key used in production.

**Applicability–Question Scope**

This question applies to all TRSMs at all sites. This question includes test, production, and spare, and old and new devices. This question also includes key loading devices that can encrypt keys and produce cryptograms of those keys.

**Intent of Question**

- To protect against the ability to misuse a TRSM in a manner that would allow the discovery of known plaintext and the corresponding ciphertext, which could allow the discovery of keys and ultimately the discovery of PINs.
- To protect against key compromise and key substitution.

**Audit Technique**

Interview appropriate personnel and review documentation of procedures to ensure the adequacy of procedures over equipment that could be used to produce cryptograms of keys under valid production keys.

Ensure procedures/policy does not allow HSMs to remain in the “authorized” state when connected to online production systems.

Ensure KLDs are not under single control, and that they do not use default passwords.

Examine the storage arrangements for all HSM brass keys, passwords, and any devices that are used to enter the component values into the HSM. Verify that no single person has the ability to place the device in a state that would allow key values to be entered.
If multiple brass keys are needed to activate the HSM, ensure that these keys are not in the locks and that they have been assigned to separate designated custodians.

Inspect the HSMs to ensure that they are in an armed state, that the anti-tamper sensors have been enabled and that the brass keys are not in the locks. Advise that the copies of an individual brass key be separated and stored securely in two different sites.
Question 32–Equipment Security Procedures

**Do written equipment security procedures exist?**

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

Written procedures must exist and be known to all affected parties. Records must be maintained of the tests and inspections given to PIN-processing devices before they are placed into service, as well as devices being decommissioned.

Procedures that govern access to Host TRSMs must be in place and known to data center staff and any others involved with the physical security of such devices.

**Applicability–Question Scope**

This question applies to written procedures that describe how all PIN processing equipment is managed.

**Intent of Question**

- To ensure that adequate and appropriate documented written procedures exist for the management of all cryptographic PIN processing equipment.
- To ensure that the documented procedures are followed, and that PIN processing equipment is not mismanaged.

**Audit Technique**

Review existing documentation for completeness. See Question 7 for details.
Appendix A: PIN Security Audit Checklist

(Use this checklist as an aid in taking notes during the audit. Make sure that you have an entry in each area.)

<table>
<thead>
<tr>
<th>Question 1.</th>
<th>All PINs are processed in compliant TRSM devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 2a.</th>
<th>PINs processed online are always processed using Triple DES and double- or triple-length keys.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 2b.</th>
<th>PINs processed offline using IC Card technology are protected in accordance with the requirements in Book 2 of the EMV2000 IC Card Specifications for Payment Systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 3.</th>
<th>ISO PIN Block Format 0, 1, or 3 is being used for online interchange transactions. Format 2 must be used for PINs that are submitted from the IC reader to the IC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 4.</th>
<th>PINs are only stored (store and forward) in a compliant manner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
<tr>
<td>Question 5.</td>
<td>All keys are generated randomly using a process that is capable of satisfying the statistical tests of FIPS 140–2 level 3.</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 6.</th>
<th>Any compromise of a key during generation would require collusion.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 7.</th>
<th>Written key creation procedures exist and are in use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 8.</th>
<th>Secret or private keys are conveyed as components using different communication channels, or as cryptograms. A mechanism independent of the actual conveyance method that provides the ability to validate the correct key was received is used when conveying public keys.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 9.</th>
<th>During key loading or other internal movements, unencrypted key components are in the custody of custodians, in a secure container, or in a TRSM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 10.</th>
<th>All key exchange keys are at least as strong as any key transmitted or conveyed. All DES keys are at least double length keys and RSA keys use a key modulus of at least 1024 bits.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes  No  N/A</td>
</tr>
<tr>
<td>Question 11.</td>
<td>Written key transfer procedures exist and are in use.</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 12.</th>
<th>Unencrypted keys are loaded into TRSMs (HSMs and PEDs) under dual control/split knowledge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 13.</th>
<th>Key loading at HSMs or PIN entry devices is protected against external surveillance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 14.</th>
<th>Key-loading hardware is managed under dual control.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 15.</th>
<th>The key-loading process includes procedures to guard against tampering or modification (e.g., testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 16.</th>
<th>Written key-loading procedures exist and are in use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 17.</th>
<th>Keys used between pairs of network nodes are unique, except by chance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
<tr>
<td>Question 18.</td>
<td>Procedures to prevent or detect key substitution are in place.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 19.</th>
<th>Cryptographic keys are only used for a single purpose.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 20.</th>
<th>All keys in PIN entry devices are unique, except by chance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 21.</th>
<th>Keys exist only as components, as cryptograms, or within TRSMs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 22.</th>
<th>Written key compromise procedures exist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 23.</th>
<th>Key variants are not used outside the device that holds the original key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 24.</th>
<th>Obsolete keys are destroyed securely.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 25.</th>
<th>Access to key components is limited to a &quot;need-to-know&quot; basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
<tr>
<td>Question 26.</td>
<td>Key access logs are maintained.</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 27.</th>
<th>Backup copies of keys are stored in a compliant manner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 28.</th>
<th>Written key administration procedures exist and are in use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 29.</th>
<th>PIN-processing equipment (PEDs and HSMs) is inspected before being placed into service and substitution protection exists.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 30.</th>
<th>Keys, PINs and other PIN-related information are removed from devices taken out of service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 31.</th>
<th>All TRSMs are managed under dual control and have adequate physical protection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 32.</th>
<th>Written equipment security procedures exist and are used in equipment commissioning and decommissioning.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant?</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Appendix B: PIN Security Field Review Agenda

Should your institution be selected for a PIN Security Field Review, the following agenda will be used.

Note that the first four steps take place in the order shown, but that the remaining steps (up to the Exit Interview) can take place in the order that causes the least disruption to your normal routine.

1. **Introduction**—A brief history of Visa's PIN Security program and its impact on the Member being reviewed. The Field Review process is described, including the management report. Questions about the process are addressed.

2. **Network Topology**—A diagram of how messages with encrypted interchange PINs flow through your system is developed. This diagram identifies the number and types of ATMs and POS devices with PIN pads that are deployed, the type and number of Host computer systems with attached Hardware Security Modules that process the traffic, the operating and applications software that is being used and the upstream network hosts to which messages with interchange PINs can be routed.

3. **ATM/POS PIN Pad Initialization Process**—The steps involved in initializing or reinitializing an ATM and/or a POS PIN Pad are developed in detail, including the identification of cryptographic keys loaded at the endpoint device, identification of keys downloaded from the Host and the sequence of encryptions and translations experienced by an interchange PIN as it passes from the ATM or POS PIN Pad to the upstream network node.

4. **Key Matrix**—For each cryptographic key in the ATM and the Host, the following information will be tabulated:
   a. Key creation date
   b. Key creation method
   c. Key form (cleartext, halves, components, and so forth)
   d. Key storage locations (if components on paper, Smartcard, and so forth)
   e. Key Usage (Master, KEK, Working Key)
The following steps can take place in any order.

- **Visit to Data Center**—The area of the data center housing the Hardware Security Modules will be visited in order to perform a physical examination of the devices.

- **Physical Inventory of Key Components**—The hard copy key components and/or secure tokens being held will be inventoried. The components on hand will be crosschecked against the key matrix and the key access logs will be reviewed. Any obsolete key materials will be noted.

- **Examine Production ATM**—The key entry area (Not the money vault) of an ATM will be examined and any documents stored therein will be reviewed.

- **Examine Key-loading Equipment**—Any special equipment (Brass keys, special cables, passwords, key input devices, and so forth) will be inventoried.

- **Discuss Key-loading procedures**—Procedures for ATMs, POS devices, and HSMs will be discussed, including documentation and load logs.

- **Discuss Key Component Transmittal/Receipt Procedures**—Descriptions of how key component values are conveyed to and received from other networks will be discussed, as will the processes used to convey key component values to ATM or POS endpoints.

- **Describe PIN Block**—The PIN Block format used to protect interchange PINs will be described in order to verify that it is compliant.

- **Key Component Destruction Procedures**—The methods and documentation involved in the destruction of obsolete key components will be discussed and all logs and affidavits of destruction will be examined.

- **ATM/POS PIN Pad/HSM Install and Decommissioning Procedures**—The steps used to bring endpoint devices and Hardware Security Modules into and out of service are discussed.

- **Documentation**—In addition to documentation for the key life cycle and equipment management procedures described above, written—as distinct from verbal—procedures in the following areas will be reviewed:
  a. Equipment commissioning/decommissioning
  b. Equipment substitution
  c. Equipment theft
  d. Key substitution
  e. Periodic equipment inspections
  f. Key compromise procedures

- **Exit Interview**—A discussion of the findings from the Field Review will take place in order to advise management of the variances (if any) that will be documented in the management letter.