PIN Security Program: Auditor's Guide

Effective: 1 January 2002

Contents

Foreword

The security of PINs (Personal Identification Numbers) assigned to Visa-branded products such as Visa, Electron, Plus, and Interlink has always been of great importance to the Association and its members. Technical staff members 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 *PIN Security Requirements*, an annual 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 auditors and data 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.

While we have attempted to make this document enjoyable 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.

This page is intentionally left blank.

How to Use the 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 we look for during a review to determine whether an acceptable level of compliance exists.

Use the Auditor's Guide as a guide, 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.

This page is intentionally left blank.

PIN Security Program Overview

Air Force pilots often say, "When the weight of the paper equals the weight of the plane, then they let you take off." Although this saying illustrates the impatience hotshot pilots have with paperwork, they all understand the importance of pre-flight inspections in managing the risks of flight. While Visa does not require the weight of an ATM in documentation before interchange PINs are processed, we do require 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, 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. While this may seem be about as much fun as being reminded of an upcoming root canal procedure by your dentist, we believe that it is one of the most valuable and educational services that Visa provides to its members and their agents.

The PIN Security Field Review usually requires about 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 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. We will also need to see that portion of the data center housing the Hardware Security Modules and we will carry out a physical inventory of all key components and key-loading equipment. 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 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. At various points during the review, we will need to review all available written documentation, including policies, procedures, audit trails and logs.

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 is asked to submit a compliance plan within 45 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 in order to track the remedial plan until full compliance is established.

PIN Security: From the Attacker's Point of View

Sun-Tzu, the 6th century Chinese strategist, stated "The art of war teaches us not to rely on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable." (*The Art of War*)

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;
- 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 and will go into some other line of work, maybe even legitimate!

This page is intentionally left blank.

What to Look for (and Where to Look)

Preparing for the Audit

Before setting out on your quest, build yourself a map of the territory that you plan to traverse. It is important to diagram the path(s) that interchange messages containing encrypted PIN blocks can follow as they pass through your organization's network. Among the questions you should ask are:

- How many ATMs, cash dispensers, and POS terminals with PIN pads do we have?
- How many of them accept Visa-branded transactions from cardholders for whom we are not the card issuer?
- Where do these messages go when they leave the ATM or PIN pad? to our computer? to a third party processor? somewhere else?
- Where do we send messages from cardholders who are not our customers?

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

- Does your organization 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 PIN pad into operation? (Make certain that you identify every cryptographic key involved in this process and how each key is used.)
- Does your organization use in-house-developed processing software or do you use a commercial package?

With this information in hand, you can proceed to investigate the 35 individual questions that make up the PIN Security Self-Audit.

Control Objective 1—Secure Equipment and Methodologies

PINs used in interchange transactions are processed using equipment and methodologies that ensure that 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 is being used, whether the PIN is protected within a suitable PIN block and whether PINs are inappropriately stored.

Question 1—Compliant Hardware

Is the Hardware Compliant?

All cardholder-entered PINs are processed in equipment that conforms to the requirements for a Tamper-Resistant Security Module. (TRSM)

- What do we mean? We want to ensure that every PIN pad, ATM, Cash Dispenser and Hardware Security Module (HSM) in use meets the requirements of American National Standards Institute (ANSI) Standards X9.24, ANSI X9.8 and International Organisation for Standardisation (ISO) 9564-1. 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 different PIN encryption key is used for every transaction, the PIN entry device may use compromise detection techniques.

  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 (a polite term for a crook) 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.

  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.

Tips, Tricks, and Strange Observations

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.

- What should I look for? First, examine the sales literature and technical documentation that describe the device in question. Do they contain assertions that the device is a TRSM or a Physically Secure Device? Do they refer to any ISO or ANSI or Federal Information Processing Standards (FIPS) standards? (Hardware Security Modules must comply with FIPS 140-2/ANSI X9.66 Level 3 or Level 4.) Next, examine the device and discuss its characteristics. Does it have mechanisms that will cause it to "dump" or erase the keys in the event of intrusion? Does the device have indicator lights that signify that it is powered up and armed? If the device has locks, are they turned to the locked position with the keys removed? 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 your purchase contracts for ATMs, cash dispensers, PIN pads, and Hardware Security Modules requiring the manufacturer to stipulate that all PIN-processing equipment supplied under the contract is compliant.*

- What do we look at? Do we know the equipment? Have we seen the same make and model elsewhere and did we determine at that time that it was compliant? Is the equipment known to be non-compliant? Are the locks and indicators set to ensure secure operation? Does the vendor documentation cite ISO or ANSI specifications concerning Secure Cryptographic Modules?

Question 2—DES Algorithm

Is the DES algorithm being used to encrypt/decrypt PINs?

All cardholder PINs processed online are encrypted and decrypted using Triple DES with at least a double-length key.

As of the publication date of this document, Visa has not set a date for enforcement of the requirement for TDES. Once the Board of Directors has agreed to the date, an update will be published.

- What do we mean? We want to make sure that only the Data Encryption Standard (DES) algorithm is used to encrypt cardholder PINs, since this is the only algorithm approved for this purpose by Visa.
- What should I look for? It is very probable that DES is being used to encrypt interchange PINs at your organization. However, you should view the encrypted output to see if it is 8 bytes (16 hexadecimal characters) long and that the individual position values are in the range 0-9, A-F. Ask the technical staff to show you the application software code or parameter settings where the calls are made to the HSM to determine which algorithm is being invoked.
- What do we look for? We view a parameter report, such as the Base24 KEYF report, if available. Otherwise, we review the code structures with technical staff in order to ensure that DES encryption is taking place. Specific attention is given to those points in the code where calls are made to the Hardware Security Module.

  We also view an output cryptogram in order to ensure that it has the appropriate length and form as that produced by DES. We may also review a trapped transaction to verify what calls are being made to the HSM

Question 3—PIN Blocks

Are you enclosing PINs within secure PIN blocks?

For interchange transactions, PINs are only encrypted using ISO 9564-1 PIN Block Formats 0 or 3.

- What do we mean? The encrypted PIN is not inserted into a message "naked." One reason for this requirement is that PINs can be any length–from 4 to 12 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. We require the use of ISO PIN Block Format 0 (also known as ANSI PIN Block Format 0), which XORs (exclusive ORs) the rightmost 12 digits of the account number (less the check digit) with the PIN, then encrypts the resulting string using DES. Even if two cardholders enter the same PIN value, the resulting PIN blocks will be different, since the account numbers are different.

  (We will also allow the use of ISO 9564-1 Format 3 when it becomes finalized, but the old Visa Formats 02, 03, and 04 are not acceptable for interchange traffic.)

Tips, Tricks, and Strange Observations

Some 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.

- What should I look for? Check the *Visa Card Technology Standards Manual* (or ISO 9564-1 or ANSI X9.8-1) for details on how to construct the required PIN block. Verify with your technical staff that this is the method being used at your organization.

- What do we look for? We check any application software parameter report, such as the KEYF report from Base24. If we see ANSI or ISO Format 0 as the PIN block type, you are in compliance; an entry of PIN Pad, 3624, Diebold or anything else means that you are out of compliance in one of the most serious areas of PIN security. We may also review a trapped transaction to verify what calls are being made to the HSM. We also look for the same things that you should be looking for in this area.

Question 4—No 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.

- What do we mean? Normally, PIN-based transactions take place in real time. In other words, 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.

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 said HSM does not exist and all you get is red faces and sheepish looks, waggle your finger at the culprits and offer forgiveness upon installation of the missing security module. Then pat yourself on the back for spotting an uncommon variance.

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

- What should I look for? Ask your technical staff to describe the entire "life history" of a PIN-bearing message with specific attention to the disposition of the message in the event the Issuer or Agent is unavailable or after the approve/decline decision has been made. If the PIN block is not stored at any point in its journey, this question does not apply to your organization.

  However, if the message is stored or logged, verify that it is translated from the PEK to a different key, which is used only for the purpose of storage. You must also verify that any such translation is performed by a compliant TRSM as described in Question 1 and that the DES algorithm is used. (Note that store

and forward is sometimes used in a supermarket or hypermarket environment.)

- What do we look for? We trace the message flow, looking for points at which message logs are created. As long as the PIN block is not stored, there is no question of compliance. If the PIN block is stored, we 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.

Control Objective 2—Secure Key Creation

Keys 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 5–8 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 a random or pseudo-random process that is capable of satisfying the statistical tests of FIPS 140-2 level 3. Random number generation processing is designed, implemented and used in compliance with Visa requirements.

- What do we mean? As you know, 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.
- What do I look for? Keep in mind the two principles that the outcome from a true random process is neither predictable nor predictably reproducible. For example, check whether a method being used or contemplated gives the same output value every time a specific starting or "seed" value is used. Most computer-based "random" functions are of this type. Having staff members "think up" keys is also not suitable, since statistical analysis has shown that some values occur more often than others, resulting in an uneven distribution of key values. Be alert for keys that are generated in regular computer memory, since they can be compromised during the process. Rather, you should find keys being 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).

Tips, Tricks, and Strange Observations

No matter what your colleagues tell you, "thinking up" a key or key components is not acceptable. However, while the vast majority of software routines are not random, we have seen a few which comply. All of these have an element of unpredictability to them, such as the press of a key or the time needed to access a specific disk sector. This adds that element of non-reproducibility that is required. Whenever possible, make them use the HSM to generate keys, since this can also weed out "weak" keys.

- What do we look for? We ask detailed questions about the methods used to generate keys, with specific attention to any computer-based methods. Our concern is raised when no one can remember how a key was created. We always assume that any such key was generated by a non-random method and therefore is non-compliant. We ask key custodians to examine key components in order to identify any obviously non-random components. We also ask to see written procedures that detail how keys are to be generated.

Question 6—Key Compromise

Collusion is needed to compromise a key during its creation.

Compromise of the key generation process is not possible without collusion between two trusted individuals.

What do we mean? We want to make sure that if you have gone to the trouble of generating proper random key components that the values remain confidential. This means that 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.

- What should I look for? 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.

  Some recent software systems running on PCs can pass the ANSI definition of a random process. While we strongly recommend that secure devices should be used for key generation, we recognize that compliant PC-based systems might exist. If a PC is used for key generation at your organization, you must ensure that it is not used for any other purpose, that access controls limit its use to authorized key custodians, and that it is powered off after the key generation process.

- What do we look for? We walk through the entire process, looking for any way that an adversary could obtain the values of the key components. We inspect the devices used in the process for evidence of tampering. We observe whether the devices are "cold started" and powered off after use (except when an HSM is being used to generate key components). We observe whether any live network connections exist. Finally, we determine whether any compromise of paper outputs can take place, including waste, printer ribbons, and so forth.

Question 7—Key Components

All key components must be (at least) double length and the key must be formed such that no one knows any part of the final key value.

Key components must exist as a minimum of two (at least) double-length values that are combined to form the actual key by a process such that no "active" bit of the key could be determined without knowledge of all components.

NOTE: *As of the publication date of this document, Visa has not set a date for enforcement of the requirement for TDES. Once the Board of Directors has agreed to the date, an update will be published.*

- What do we mean? First, we mean that an individual key component must be at least 32 hexadecimal characters long. Once these random components have been created, the actual key must be generated inside a physically secure device through a Boolean XOR or similar reversible transformation, in such a way that complete knowledge of a key component gives no knowledge whatsoever of the final key value.

  This is crucial, not only to protect the institution against the disclosure or compromise of its cryptographic keys, but also to guard the integrity of your trusted key custodians against any future claim of malfeasance.

- What should I look for? Ask the custodians to count the number of characters in the component(s) for which they are responsible. If the number is less than 32, there is a good chance that the key is not double length. If the custodian reports an 8-character key portion, the key is likely to be neither double length nor XOR'ed. Examine the labels on component storage envelopes to ensure that each key managed in hard copy has at least two of these components. Have the key custodians describe in detail how the key is formed and verify that if the component length is less than 32 characters, multiple components are concatenated together to form the double-length component before the double-length components are themselves XOR'ed to form the key.

- What do we look for? First, we look for documented key-creation procedures. If they exist, we compare them with the verbal key formation descriptions given by key custodians. We look for identical left and right 8 or 16-character component portion values that get "glued" together to form the component. Above all, we look for any shortcuts that are taken (often in "emergency" situations) that allow some or all of the final cryptographic key value to become known to any person, trusted or otherwise.

Question 8—Procedures

Questions 8, 12, 19, 31 and 35—Procedure Documentation. Documented procedures are in place for all aspects of cryptographic key management.

Question 8—Key-Generation Procedures. Documented procedures exist and are used for all key-generation processing.

Question 12—Key-Transmission Procedures. Documented procedures exist and are used for all key transmission and conveyance processing.

Question 19—Key-Loading Procedures. Documented procedures exist and are used for all key-loading activities.

Question 31—Key Administration Procedures. Documented procedures exist and are used for all key administration operations.

Question 35—Equipment Security Procedures. Documented procedures exist and are used to ensure that the security and integrity of PIN-processing equipment (e. g., PEDs and HSMs) is placed into service, initialized, deployed, used, and decommissioned.

- What do we mean? As the old plumber once said, "the job ain't over 'till the paperwork is done." While we do not propose to weigh your procedure manuals against your ATMs, we are extremely concerned that the operations of all PIN-acceptance processes are governed by comprehensive written procedures that ensure that both Visa's rules and your institution's policies are strictly observed at all times.

Tips, Tricks, and Strange Observations

When reviewing procedures, try to tie each one to a specific, approved policy. If no governing policies can be found, make it a top priority to put them in place as soon as possible.

- What do we look for? Determining compliance in these areas is pretty straightforward. First, verify that your organization has published policies that call for the correct (as defined by your institution) operational actions to be carried out. For example, your institution needs to have a policy statement that says something like "All cryptographic keys used in processing acquired PINs shall be created in accordance with the applicable Association and International standards." Once this policy is in place, specific detailed procedures or "recipes" for creating cryptographic keys can be prepared. For each of the areas covered by these questions, determine whether governing policies and separate, but consistent, procedures are in place. If you discover that procedure steps (what to do) are interspersed with policy and

philosophy statements (why to do it), we strongly urge you to separate these two types of text. The last thing someone carrying out a process wants to see, especially in an emergency, is background and/or philosophical verbiage. If your procedures do not already consist of a series of imperative sentences, please rewrite them into that form – it will pay off when they are used.

- What do we look for? We look for written procedures covering key creation, formation, transmittal, storage, loading, and destruction. We also look for written procedures governing equipment receipt, inspection, storage, deployment, and decommissioning. We look for the policies that stipulate the use of these procedures and we assess, through the distribution list, whether the procedures have been placed in the hands of the appropriate staff. Finally, we look for 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 9–12 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 9—Send/Receive Keys

How are keys sent and received?

Encryption keys are transferred by:

a. Physically forwarding the separate full-length components (hard-copy, magnetic media, electronic devices) using different communications channels, *or*

b. Transmitting the key in ciphertext form.

- What do we mean? When a 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 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. In order to ensure that these principles are observed, a 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. The encrypted key may also be sent without any special precautions.

Tips, Tricks, and Strange Observations

A standard courier envelope is tamper-evident, but the original envelope could have been replaced by another. We advise using 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

- What do I look for? Follow the route taken by each key component that your organization sends. Typically, these consist of Key Exchange Key (KEK) components that you create and send to a network with which you exchange message traffic containing PINs and ATM or PIN pad initialization keys, often referred to as the A and B keys. Don't let your colleagues tell you that these rules don't apply to initialization keys because they do! 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 you are 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 your organization receives key components, verify that they are received by staff designated as key custodians and that they are logged before being placed into secure storage.

- What do we look for? We trace how all keys are sent and received under normal conditions to ensure that the rules have been followed. We review the written documentation and the key logs to crosscheck that everything has been accounted for. Finally, we ask 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.

Question 10—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.

- What do we mean? Every once in awhile, you actually have to use cryptographic key components to form a key. The previous question examines the methods used to transport keys, and 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, we seek 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.
- What should I look for? In this, as in all key management areas, 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. Try to 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.

  In addition, examine the key component storage arrangements. Is the container secure and is the custodian 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.

- What do we look for? We look for key components stored in unsecured desk drawers. Not only are such arrangements not robust enough for the purpose, but master brass keys are often held by facilities or maintenance staff. We also look for multiple components stored in the same physical area within a safe or lockbox. We 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 11—Key Exchange/Transport Keys

All Key Exchange or Transport keys are double length.

All DES key encryption keys used to transmit or convey other cryptographic keys are (at least) double length.

- What do we mean? All cryptographic keys fall into one of three categories:
  - A specific key is a Master key, used to encrypt other keys in a device or host environment.
  - A Key Encryption (Key Exchange, Key Transport) key is used to encipher a DES key during transport.
  - A Working key is used to encipher the actual data, such as a PIN. Visa requires that all 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 a date for enforcement of the requirement for TDES. Once the Board of Directors has agreed to the date, an update will be published.*

- What do I look for? Identify the use for each of your institution's cryptographic keys. For each key used as a Key Exchange key (normally including at least one of the ATM initialization keys), ensure that it is at least 32 hexadecimal digits in length. You can examine the cryptogram and ask the custodians to count the number of characters in each component in order to verify compliance with this requirement.
- What do we look for? We verify that no Key Exchange Key is shorter than the cryptographic keys that it protects and that it is at least double length.

Question 12—Key Transmission Procedures

Key transmission procedures are in place.

Documented procedures exist and are used for all key transmission and conveyance processing.

See Question 8.

This page is intentionally left blank.

Control Objective 4—Secure Key Loading

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

This Control Objective covers Questions 13–19 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 13—Loading to TRSM

How are keys loaded to TRSMs?

Unencrypted keys are entered into Host Hardware Security Modules only in the form of at least two components using the principles of dual control and split knowledge.

- What do we mean? We require that no person ever knows any portion of the actual value of a cryptographic key. The method used to implement this requirement is to enter cryptographic key values as two (or more) components, each of which is equal in size to the actual key. This includes the actions needed to insert keys into Tamper-resistant Security Modules connected to a host system. Very simply, this is asking whether keys are entered as two or more full-length components.

Tips, Tricks, and Strange Observations

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 "chip" cards or similar secure tokens, with each card holding one component. Some old Atalla HSMs stored the key on an armored circuit called an Atalla Proprietary part. Other Atalla HSMs have their keys loaded by a secure key transfer device such as a Quick Key Transport (QKT) or Secure Configuration Terminal (SCT). Just ensure that the principle of split knowledge is strictly enforced

- What do I look for? Read the procedures and have the key custodians describe in detail how their component values are entered at the host TRSM. If at all possible, watch an actual key loading or a simulated version of the process. Verify that the process includes the entry of individual key components by the designated key custodians.

- What do we look for? We try to identify "shortcuts" such as custodians handing their components to a third party to enter. We also look for instances where the components are not full-length, but may consist of 8 character component halves, concatenated together. This is not uncommon and the result is a key whose effective length is only 28 bits, rather than the 56 bits of a single-length DES key. We are also alert to situations where HSM brass keys are not held securely under dual custody. We may also ask for a demonstration or walk-through of the process.

Question 14—Loading to ATM/PIN Pad

How are keys loaded into ATMs and PIN pads?

Keys are entered into PIN Entry Devices:

a. In the form of at least two components, using the principles of dual control and split knowledge *or*

b. Using a secure key transfer system.

- What do we mean? This is basically the same requirement as in Question 13, except that we are evaluating how cryptographic keys are entered into endpoint devices, such as ATMs and PIN pads, rather than Host Security Modules.

Tips, Tricks, and Strange Observations

- You just kind of have to shake your head about the crazy things that happen in this area, including:
- Use of common, non-random keys such as 0-9, A-F; FFFFF…; 010101…; and so forth.
- Writing or even typing key values in the startup instructions.
- Taping the startup keys to the inside of the ATM.
- Dictating the keys over the telephone during installation.
- Faxing the keys to the installation site or branch.

Be hard-nosed about maintaining the secrecy of the initialization keys. Don't fall for the specious efficiency or cost arguments. Remember, you are responsible without limit for all losses resulting from non-compliance.

We require that key insertion or injection into any endpoint device accepting Visa-branded transactions must be performed by entering two or more full-length components or through a secure insertion device, such as that provided by Hypercom for their PIN pads.

- What do I look for? Manual entry of key component values must proceed as in Question 13; in other words, two separate people must enter full-length component values into the device. Be aware of the arguments that "it's too expensive to have two people" and "our service firm won't do it that way." Neither of these arguments will relieve your institution of its obligations under Visa's Operating Regulations and if you encounter them, you should institute a complete review of the actual risk environment.

If you are injecting PIN pads, inspect the equipment being used. Often, the injection system is based around a PC. Verify that the PC is not used for any other purpose, that it is not connected to an external network, that it is powered up prior to use and powered down after use, and, ideally, that all external input devices except the keyboard have been disabled.

- What do we look for? We look for non-compliant PIN pad injection systems, such as PC-based systems offered by several vendors, which require extensive additional physical and logical security controls to be managed in a compliant manner. At least one such system encrypts the DES keys that are injected under a non-approved proprietary algorithm. We note that any PCs that are used for multiple purposes, that are kept in a room that is not secured under dual access and that have connections to external networks. Any PC used must be a single-purpose device, must be powered up just before use, and must be powered off after use. While password access control can be acceptable, hardware access mechanisms are preferable.

  We are particularly interested in the methods used to initialize ATMs under "emergency" conditions. While many institutions have implemented compliant key-loading procedures for routine situations, they revert to risky and non-compliant practices, such as reciting ATM initialization keys over the telephone in non-routine or after-hours situations.

  We may also ask for a demonstration or walk-through of the process.

Question 15—Loading Protection

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

The transfer mechanisms (terminals, PIN Pads, key guns, and so forth) by which key components are entered into PIN Entry Devices or host Hardware Security Modules are protected so as to prevent any types of monitoring that could result in the unauthorized disclosure of any component.

- What do we mean? Here, the requirement is to ensure that no visual or electronic surveillance or monitoring is used to gain knowledge of keys or key components during the actual loading process.
- What do I look for? If paper components are being used, ensure that any sort of visual surveillance, such as a guard post or closed circuit TV, does not cover the area where component value entry takes place. In some cases, banks have deployed CCTV to cover the backsides of ATMs. Ensure that these cameras are not sensitive enough to read the actual keystrokes being entered. If you discover that cameras could be used in this way, have a screen constructed and erected around the key-loading area during load operations.

  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.
- What do we look for? In this area, we carry out the same type of inspection that we ask you to perform. We look for CCTV cameras, guard posts and electronic monitoring devices that could divulge the value of one or more key components. We also look for and review any logs that document this procedure. The absence of such logs gives us significant concern about whether the process is carried out in accordance with our requirements.

Question 16—Hardware Dual Control

Is key-loading hardware under dual control?

All hardware used for key loading is managed under dual control.

- What do we mean? Normally, both key components and various bits of hardware are required in order to enter keys into a secure device, such as a Hardware Security Module. With the exception of individual components, all other required devices, passwords, and so forth, must be managed under dual control.
- What do I look for? Hardware Security Modules usually are equipped with physical locks that must be disengaged in order to allow key values to be entered. Brass keys control these locks. In addition, there is normally a password (possibly two) that must be entered before the keys can be inserted. Some manufacturers, such as Atalla, provide specialized devices, such as a Quick Key Transport (QKT) or Secure Configuration Terminal (SCT) to carry out the actual key entry procedure. PIN Pad injection usually requires the use of specialized PCs that are connected to injection probes. Some ATMs are initialized with secure entry devices known as "key guns."

  In all cases, the brass keys, passwords, key guns, PCs, and so forth, must be under dual control. This means that no single person can, by him or herself, place a device in a state where a key can be inserted. Verify what devices, brass keys and passwords exist at your institution. Verify that no single person has access to all of the required items. Suitable procedures might include assigning the key to one person and the password to another or storing PIN pad injection gear within a room controlled with two separate locks.

Tips, Tricks, and Strange Observations

There was a bank with a stack of 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. Otherwise, you might find yourself drilling through a tough (and expensive) lock.

- What do we look for? We attempt to identify means by which component holders could also gain physical custody of the keys, passwords and other items actually needed to enter a key. In particular, we examine emergency procedures in order to determine whether dual control rules are violated under those circumstances.

Question 17—Seclusion

Is key loading done in seclusion?

Individuals entrusted with a key component ensure that no other person can observe or otherwise ascertain the component before, during, and after key loading.

- What do we mean? This is perhaps the simplest requirement to comply with. All that is required is for every key custodian to ensure that no one is physically close enough to observe the component value during the entry process, or is able to access the media which contains the key component.
- What do I look for? Review the written procedures and verify that explicit instructions to the custodians stipulate that the component values are entered in seclusion, and that the custodian must physically safeguard the media containing the key component during the key-loading process. Follow this up with a discussion with the key custodians and determine whether they take the appropriate precautions during the key-entry process.
- What do we look for? We pursue the same investigative steps as those laid out for the internal audit staff, including a review of written procedures and discussions with key custodians.

Question 18—Validation

Is the key validated after loading?

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

- What do we mean? This is a rather complicated way of saying that the components and resulting key are verified against a known valid reference value (such as by use of a key check value, hash, digital signature, or Message Authentication code) before the key is placed into production. The key check value is the first six (occasionally 4) characters of the cryptogram that results when a string of binary zeroes is encrypted with the DES key being validated. This key check value is normally stored along with the key components. In fact, most individual key components also have check values. The check value is normally displayed by the HSM and/or ATM following entry of the components and creation of the key.
- What do I look for? Review the key-loading instructions to determine whether instructions to verify key check values or equivalents are in place. Discuss the key-loading process with key custodians and supervisors to determine whether these values are verified before a key is used. Have key-loading staff describe the actions that they take when key check values do not match. Examine the key log or component envelopes to verify that reference key check values have been recorded. If no evidence of key check value verification is found, have the technical staff describe how they can be sure that the key values that are entered are the correct ones.

Tips, Tricks, and Strange Observations

Refer to the vendor documentation for a list of known factory default and test key check values. If you spot one of these values, give the culprits a stern lecture and make them generate a new random key.

- What do we look for? We go through the same procedures as those just described. In addition, we examine the key check values against a list of known default key check values. Should the key check value equal any of these known strings, we can be sure that the factory default key is still being used within the secure device. This is, unfortunately, more common than one would like to believe.

Question 19—Key-Loading Procedures

Is key-loading documentation in place?

Documented procedures exist and are used for all key-loading procedures.

See Question 8 for details.

Control Objective 5—Prevent Unauthorized Usage

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

This Control Objective covers Questions 20–23 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 20—Network Node Keys

All keys that link network nodes are unique.

There is not any discernible relationship between the key in use between any pair of communicating nodes and any key ever known by or used between any other pair of communicating nodes.

- What do we mean? This question refers to host-to-host communications. For example, this question concerns the traffic between a bank's computer and Visa or between two bank hosts. Note that only links carrying interchange messages containing PINs are covered by this question.
- What do I look for? Normally, each host-to-host link consists of at least two cryptographic keys: a Key Exchange Key (KEK) and an Acquirer Working Key (AWK). Count the number of links and multiply by two to compute the number of keys that you should expect to find. If your technical staff can't account for that number, investigate whether one or more links has only a working key. Examine the key check values for each key; these should all be different. (If these keys are no longer managed in hard copy form, count the number of cryptograms on the host database and examine each to ensure that the proper number of keys exist and that the cryptograms are different. (Note that the cryptograms must be created using the same variant of the key that enciphers them for this comparison to be valid.) One of the best ways to ensure uniqueness is when the other end of the link has created part or all of the key.
- What do we look for? First, we identify all host-to-host links. Then, we ensure that each link has a unique key (or probably key pair), either by performing a physical inventory of key components or by examining key check values or cryptograms, both for the correct number and for unique values.

Question 21—Key Substitution

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.

- What do we mean? Very simple – we don't want a cryptographic device (PIN pad, ATM or hardware security module) to be operated with the wrong key (possibly one placed by an attacker). Therefore, procedures and safeguards must be in place to detect such an attempt and to prevent such a key from being used successfully.
- What do I look for? The most common symptom of an attempt to use the wrong key is a PIN synchronization error. Examine software technical specifications in order to determine whether the application code contains a "trigger" which limits the number of PIN synchronization errors that can occur before an alarm sounds. If those safeguards exist, review the procedures that come into effect whenever this alarm occurs. 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.

  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.

Tips, Tricks, and Strange Observations

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, he can really go to town! This is another strong argument for the implementation of unique keys in all devices.

- What de we look for? We review written procedures and discuss alarm processing with the technical staff of the Network Operations Group. What is often found is that new keys are automatically downloaded to any device that has generated a series of PIN synchronization errors. While this may solve the immediate problem, it could also aid an adversary whose true goal was to intercept the PIN encryption key during download. We hope to find proactive safeguards in place that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.

  We also will examine procedures which ensure that HSMs do not remain in "authorized" state, controls over access to and use of devices (e.g., QKTs) used to create cryptograms, and for ensuring the secure destruction of keys used to encipher other keys.

Question 22—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.

- What do we mean? In order to minimize the exposure of confidential information resulting from a successful attack on a cryptographic key, Visa requires that each key be used for one, and only one, purpose. Keys are inexpensive to create, and there are plenty of them (about 72 quadrillion), so that there is no need to make a cryptographic key do "double duty." The important point to remember is that when a cryptographic key is used for more than its sole intended purpose, a successful attack on that key spreads the compromise over multiple areas.
- What do I look for? The most common error in this area of cryptographic key management is the use of live (production) keys in a test environment. The rationale for this is usually that "unless we test with the real keys, we can't be sure that it works". This argument is totally specious! The DES algorithm works and continues to work. As long as both ends of the message link are using the same cryptographic key, the encryption/decryption process will proceed just fine. What this really does is to expose your organization's secret information to potential attack by the technical staff most able to mount such an attack.

  Another common misuse of keys occurs when a working key is also used as a key exchange key. For example, if new PIN Encryption Keys are periodically downloaded to an ATM, the new PEK must not be encrypted under the old PEK. Make sure that each of your cryptographic keys has one, and only one, use.
- What do we look for? We trace message flows, making sure that each link in the process uses a separate and distinct key. We examine the cryptograms and key check values in both the production and test systems to ensure that the keys are different. We verify that new working keys or key exchange keys are transported under KEKs, rather than predecessor working keys and we emphasize the importance of protecting the reputations of the technical staff by separating production keys from the test environment.

Question 23—Unique Keys

Are unique keys used?

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

- What do we mean? Every cryptographic key in an ATM or PIN pad must be unique to that device. This requirement includes all initialization keys, local master keys, and key exchange keys, not just the actual working key used to encrypt the cardholder PIN.
- What do I look for? The most common violation in this area is the use of non-unique ATM initialization keys, often referred to as the "A and B" keys. These keys are often non-random test values that have been used for years. For example, if your institution has 500 ATMs, you need to satisfy yourself that a mechanism is in place to randomly generate 500 ATM startup keys, composed of two or more full-length components. You must also satisfy yourself that a unique, randomly generated working key (PIN Encryption Key) is installed within each production ATM.

  If your institution has deployed PIN pads, each PIN pad must contain, at a minimum, a unique master and session key in Master Key/Session Key architecture or a unique fixed key where a terminal master key is not used. We strongly recommend the use of Derived Unique Key Per Transaction (DUKPT) architecture in the POS environment because it reduces the exposure of a key compromise and makes it easier to implement a unique key per device in a POS environment.

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. Your 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.

- What de we look for? We 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. In addition, here is another instance where we 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.

  If PIN pads are being injected, we ask for complete details of the key generation process. If the institution is using DUKPT and the Base Derivation Key is compliant (double length and with correct key management procedures in place), we are generally satisfied that the uniqueness criterion has been met. If a Master/Session or Fixed key structure is being used, we go into great detail about the creation and injection of these working keys. We verify uniqueness by examining a series of key check values from separate devices. While this is not an absolute guarantee of uniqueness, it is a highly predictive indicator.

This page is intentionally left blank.

Control Objective 6—Secure Key Administration

Keys are administered in a secure manner.

This Control Objective covers Questions 24–31 of the Self-Audit Questionnaire. It includes requirements for key storage, compromise, and destruction.

Question 24—Secure Key Components

Are key components managed securely?

Keys used for enciphering PIN Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except encrypted under TDEA key encipherment keys or securely stored and managed as two or more components using the principles of dual control and split knowledge.

- What do we mean? Any cryptographic key outside a secure device must either exist as a cryptogram protected by DES or as two or more full-length components managed under the principles of split knowledge (held by separate designated key custodians) and dual control (no single individual has access to all key components). Procedural controls, and ineffectual storage containers (such as furniture drawers or devices with a limited set of unique locks) are not sufficient.
- What do I look for? Do an inventory of keys in use at your institution and identify all the key components. 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. For each of these keys, identify the key custodians and perform a physical inventory to verify that each 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. Here is another instance where you need to get the details of how an ATM would be restarted in an emergency or after-hours situation. Even in these circumstances, the principles of dual control and split knowledge must be maintained.

Tips, Tricks, and Strange Observations

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.

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.

- What do we look for? We 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. We also review operations manuals to ensure that no confidential information has been written "in the margins."

  In the same way, we inspect key-loading procedures for HSMs in order to ensure that no key component values have been recorded in inappropriate places. In both cases, we inspect logs of access to the key components to ensure that only the authorized (as evidenced by key custodian agreements) custodians have accessed the keys and that all accesses are logged, including when we examine the storage contents of a safe, and so forth, as part of the field review.

Question 25—Key Compromise Procedures

Do key compromise procedures exist?

Procedures exist to replace any key and its subsidiary keys (those keys enciphered with the compromised key), whose compromise is known or suspected, to a value not feasibly related to the original key.

- What do we mean? Security offered by the DES algorithm is totally dependent on maintaining the secrecy of the encryption key. If it is known or suspected that the value of a key has become known, that key must be replaced promptly, as must every key ever protected by the suspect key. This requirement mandates that the institution have appropriate written procedures that detail the steps necessary to replace suspect keys and to detect a compromise.
- What do I look for? If written procedures do not exist for replacing compromised keys, you are 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 your 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. A highly desirable, but not strictly necessary, aspect of these procedures should be a post-mortem meeting to assess and improve the recovery process. Finally, ensure that the procedures have been distributed to all affected parties and are understood.
- What do we look for? We ask to review the results of any real or simulated key replacement events in order to assess how well the process actually works in practice.

Question 26—Key Variants

Are key variants used correctly?

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

- What do we mean? This somewhat obscure requirement is designed to protect the integrity of other keys in use. 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.
- What do I look for? Noncompliance with this requirement is very rare but not unknown. Examine the topology of the communications network in order to identify any communications concentrators or processors external to the central host. If such devices exist, review the message flow through them with your technical staff. Be alert for any PIN translation that is done within these devices. Any such process must take place within a TRSM attached to the communications controller, not in software. The best verification is to examine the same transaction as it enters and leaves the communications controller; if the encrypted PIN block is the same, you can be confident that no inappropriate translation is taking place.

  Additionally, 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. Because the variant key(s) are created by a known reversible process using known values, the compromise of any such derived key allows the compromise of all related keys
- What do we look for? We carry out the investigation described in the previous paragraph.

Question 27—Obsolete Keys

Are obsolete keys securely destroyed?

Keys and key components that are no longer used or have been replaced are securely destroyed.

- What do we mean? We require that all obsolete keys and their components be securely destroyed. This includes key components for zone or other encipherment keys that have been successfully loaded and enciphered under a Master File Key for local storage. The destruction event must be logged. For example, secure destruction methods for key components on paper consist of cross-shredding (confetti, rather than strip) and/or burning.

  The logging process protects both the institution and the key custodian. The custodian, who logs the details and affixes a signature, must carry out the destruction event. Then, a non-custodial third party signs the log, affirming that the event took place.

- What do I look for? During your physical inventory of key components, be alert for any envelopes that cannot be accounted for on your list of keys. It is not uncommon to find keys that were in use by entities that have been absorbed by merger or keys linking your institution to networks that no longer exist. Be particularly alert for Master File keys that have been replaced.

  Examine the log and review the written destruction procedures. Remember that for paper-based key components, burning or cross-shredding are the only acceptable methods. Ensure that destruction events are witnessed, in order to prevent any future claims of malfeasance against your key custodians.

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.

- What do we look for? In addition to all of the above, we look 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.

Question 28—Limit Key Access

Is cryptographic key access limited?

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

- What do we mean? We just require that the fewest number of people have access to cryptographic key components consistent with efficient operations. These are secrets and the fewer people that have any contact with them, the better. A good rule of thumb is to have one primary and one secondary key custodian assigned to each key component.
- What do I look for? – This is pretty straightforward. Review the written procedures governing the assignment of key custodians and determine whether redundant assignments exist. If you find extra people assigned to active keys or custodians assigned to obsolete keys, remove them from the list of authorized key custodian staff.

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.

- What do we look for? We examine logs of access to keys and key materials to ensure only authorized custodians can access components.

Question 29—Log Key Access

Is key access logged?

Logs are kept for any time that key encipherment keys or their components are removed from storage or loaded to a TRSM.

- What do we mean? We require that a complete key usage history must be maintained. This means that any time components are placed into, or removed from secure storage, the event must be logged. The log should include the date and time out, date and time returned, signature of authorized custodian and the reason for key access.
- What do I look for? Review the written logging procedures and compare the actual key logs in order to verify that the procedures are being followed in practice. Get the chronology of when new network connections came into operation or perhaps when your institution acquired a new Hardware Security Module. Review the dates in the logs in order to establish a relationship between these events and key-loading procedures.
- What do we look for? In addition to the above, we 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 30—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 exist only in one of the allowed storage form for that key.

- What do we mean? You are allowed to retain backup copies of key components only for the purpose of recovering keys that are accidentally destroyed. (This does not include Visa-supplied key components for the ZCMK, which must be destroyed.) If you keep any such backups, they must be stored at least as securely as the primary copies of the key components.
- What do I look for? Ask the key custodians and technical staff if backup copies of key components exist. If they do, perform a physical inventory of the backup site in order to 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.

Tips, Tricks, and Strange Observations

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.

- What do we look for? We 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.

Question 31—Key Administration Procedures

Is key administration documented?

Documented procedures exist and are used for all key administration operations.

See Question 8 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 32–35 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 32—Equipment Inspection

Is PIN processing equipment inspected before use?

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

- What do we mean? We want to make sure that no "doctored" equipment is placed into service. This includes ATMs, PIN pads, Hardware Security Modules and cash dispensers. Therefore, before an item is attached to the network, it must be determined that it is the correct device and that it is operating properly.
- What do I look for? First, 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.

  It is also important to 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.

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.

- What do we look for? We ask the warehouse and installation procedures with responsible staff and compare their description of what happens with the written procedures. We 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.

Question 33—Equipment Decommissioning

Do equipment-decommissioning procedures exist?

Procedures exist to ensure that any cryptographic devices removed from service have all cryptographic keys within the devices destroyed.

- What do we mean? ATMs and PIN pads removed from service can retain cryptographic keys (including PIN Encryption keys) in battery-backed RAM for days or weeks. We require that a set of proactive key removal procedures must be in place to remove 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, key removal procedures must also be in place for HSMs.

- What do I look for? Review the written procedures for taking an ATM, cash dispenser, PIN pad or HSM out of service. These procedures must include a step that results in the removal of all key values. The step could be momentary removal of batteries, removal/replacement of the system board, injection of binary zeroes or any other process that would obliterate the key. Ensure that this process is also performed on all equipment being returned for repair.

- What do we look for? We physically inspect the receiving area and discuss the equipment retirement and repair processes with the responsible staff. It is not uncommon to find a "disjoint" between written procedures and actual operational processes.

Question 34—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 (for example, locked access to it) is under dual control.

- What do we mean? Very simply, all key encryption equipment, including hardware security modules and certain ancillary equipment, such as the Atalla QKT, must be locked under dual control. If the HSM has only one brass key, access to that key must be under dual control. If a key and a password are required, such as in the Jones Futurex Excrypt HSM, one person has the key and another has the password.
- What do I look for? 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 an external device is required, ensure that all such devices are stored under dual control. 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.
- What do we look for? We always 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. We also advise that the copies of an individual brass key be separated and stored securely in two different sites.

Question 35—Equipment Security Procedures

Do written equipment security procedures exist?

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

See Question 8 for details.

This page is intentionally left blank.

Appendix A—Policies Required to Support PIN Security

Administrative Policies

- Key Custodian Selection
- Equipment Selection
- External Service Provider Selection

Key Management Policies

- Key Creation
- Key/Key Component Transmittal
- Key/Key Component Receipt
- Key-loading
- Key Storage
- Key Destruction
- Key Replacement

Equipment-Related Policies

- ATM/HSM/PIN Pad Receipt and Commissioning/ Decommissioning
- Equipment Theft
- Periodic Equipment Inspection

Operating Policies

- Key Substitution
- Key Compromise

For each of the policies listed above, and for any additional policies developed by your organization, one or more specific procedures need to be in place. These procedures should consist of a series of imperative sentences that direct your personnel in the actions to take to deal with a specific situation.

As far as possible, these procedures should be self-documenting. For example, a script that lists the steps necessary to install an ATM could also contain spaces for the person who performed the install to initial after the completion of each step. For those procedures where self-documentation is not practical, external logs or audit trails are required in order to verify that the procedures have been followed.

Appendix B—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.)

Question 1. All PINs are processed in compliant TRSM devices.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____

Question 2. PINs are always processed using Triple DES and double- or triple-length keys.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____

Question 3. ISO PIN Block Format 0 or 3 is being used.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 4. PINs are only stored (store and forward) in a compliant manner.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 5. All keys are generated randomly.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 6. Any compromise of a key during generation would require collusion.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 7. Keys components must only exist as two or more full-length values that are XOR'ed to form the key.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 8. Written key creation procedures exist and are in use.

Compliant? Yes ___No ___N/A ___

_____
_____
_____
_____
_____
_____

Question 9. Keys are conveyed as components or as cryptograms.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 10. During key loading or other internal movements, unencrypted key components are in the custody of custodians, in a secure container, or in a TRSM.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 11. All key exchange keys are at least double length.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 12. Written key transfer procedures exist and are in use.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 13. Unencrypted keys are loaded into TRSMs as two or more components under dual control/split knowledge.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 14. Keys are loaded into PIN entry devices as components or through a secure transfer device.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 15. Key loading at HSMs or PIN entry devices is protected against external surveillance.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 16. Key-loading hardware is managed under dual control.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 17. Key loading is performed in seclusion.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 18. The key-loading process includes procedures to guard against tampering or modification.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 19. Written key-loading procedures exist and are in use.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 20. Keys used between pairs of network nodes are unique, except by chance.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 21. Procedures to prevent or detect key substitution are in place.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 22. Cryptographic keys are only used for a single purpose.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 23. All keys in PIN entry devices are unique, except by chance.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 24. Keys exist only as components, as cryptograms, or within TRSMs.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 25. Written key compromise procedures exist.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 26. Key variants are not used outside the device that holds the original key.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 27. Obsolete keys are destroyed securely.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 28. Access to key components is limited to a "need-to-know" basis.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 29. Key access logs are maintained.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 30. Backup copies of keys are stored in a compliant manner.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 31. Written key administration procedures exist and are in use.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 32. PIN-processing equipment is inspected before being placed into service and substitution protection exists.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 33. Keys are removed from devices taken out of service.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 34. All TRSMs are managed under dual control and have adequate physical protection.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

Question 35. Written equipment security procedures exist and are used in equipment commissioning and decommissioning.

Compliant? Yes ___No ___N/A __

_____
_____
_____
_____
_____
_____

This page is intentionally left blank.

Appendix C—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/PIN Pad Initialization Process—**The steps involved in initializing or reinitializing an ATM and/or a 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 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/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.

This page is intentionally left blank.