PIN Security Requirements

Effective: 1 January 2002

Contents

Overview 1

Self-Audit Procedures 1

Security Self-Audit 2

Audit Exception Form 2

Auditor Verification 2

Officer Attestation 3

Field Review 3

Fines 3

Appendix A .....

Reference Documents A–1

ANSI and ISO Standards A–1

Appendix B .....

Forms B–1

Appendix C .....

PIN Security Requirements Self-Audit C–1

l. General Security Procedures and Controls C–1

Objective 1 ..... C–1

ll. Key Management and Security C–4

Objective 2 ..... C–4

Objective 3 ..... C–6

Objective 4 ..... C–8

Objective 5 ..... C–12

Objective 6 ..... C–14

lll. Equipment Security and Control C–18

Objective 7 ..... C–18

Glossary

Overview

This document contains the complete PIN Security Requirements, as stated in the *PIN Security Requirements Self-Audit* (in Appendix C) for online PIN processing of Visa transactions in ATM and POS systems, and the procedures and forms used to measure compliance. An acquirer (or its agent) processing PINs for Visa transactions must comply with these requirements. Security considerations not directly related to online PIN processing of Visa transactions are beyond the scope of this document.

NOTE: *This document replaces the* Consolidated PIN Security Standards Requirements*.*

The scope of this document includes:

- Describing minimum security requirements for online PIN-based Visa transactions.
- Outlining the minimum acceptable requirements for securing PINs and encryption keys.
- Assisting all participants in the retail electronic payment system in establishing assurances that cardholder PINs will not be compromised.

The effective date for this document is 1 January 2002. At the time of publication, Visa had not specified mandatory dates for the implementation of Triple Data Encryption Standard (TDES) key management techniques for PIN encryption. After publication of this document, Visa will issue member letters with effective dates for TDES compliance. Until those effective dates, entities that have not implemented TDES do not need to complete exception forms for the TDES portion of applicable questions. All other requirements within those questions must be met (e.g., using single instead of double- length keys and key components).

Self-Audit Procedures

The purpose of this section is to ensure that participants in the electronic interchange system are in compliance with the requirements presented in this manual. To measure compliance, each participant in the transaction processing chain that manages

cardholder PINs and encryption keys must be in compliance with the *PIN Security Requirements*.

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

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

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

Security Self-Audit

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

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

Audit Exception Form

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

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

Auditor Verification

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

Officer Attestation

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

Field Review

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

Fines

FINES MAY BE IMPOSED WHEN THERE IS FAILURE TO COMPLETE A *PIN SECURITY REQUIREMENTS SELF-AUDIT* OR A *SELF-AUDIT COMPLIANCE STATEMENT* OR TO RESPOND TO A NON-COMPLIANCE NOTIFICATION.

An acquirer is subject to fines as specified in the VIOR for the failure to submit the *PIN Security Requirements Self-Audit* or the *Self-Audit Compliance Statement*.

An acquirer who fails to respond to a non-compliance Notification following an onsite inspection is subject to fines or to having its certification suspended, as specified in the VIOR, until the response has been received and acknowledged by the applicable regional office.

An acquirer who submits an action plan but does not fulfill its commitments will be required to post a performance bond or provide an escrow amount as specified in the VIOR.

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

Appendix A

The following standards are provided for reference and information. The versions listed were current as of the publication of this document; however, these documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.

Reference Documents

ANSI and ISO Standards

ANSI X3.92–1981: Data Encryption Algorithm

ANSI X9.24–1998: Financial Services- Key Management Using the DEA

ANSI X9.42–2001: Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

ANSI X9.44–200x (Draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry: Management of Symmetric Keys Using RSA

ANSI X9.52–1998: Triple Data Encryption Algorithm: Modes of Operation

ANSI X9.66–200x (Draft): Security Requirements for Cryptographic Modules

ANSI X9.8–1995: Personal Identification Number (PIN) Management and Security, Part 1: PIN Protection Principles and Techniques

ANSI X9.8–1995: Personal Identification Number (PIN) Management and Security, Part 2: Approved Algorithms for PIN Encipherment

FIPS PUB 140–2: Security Requirements for Cryptographic Modules. 2001

ISO 9564–1: 1991 Personal Identification Number Management and Security, Part 1: PIN Protection Principles and Techniques

ISO 9564–2: 1991 Personal Identification Number Management, Part 2: Approved Algorithms for PIN Encipherment

ISO 11568–1: 1994 Banking Key Management (Retail), Part 1: Introduction to Key Management

ISO 11568–2: 1994 Banking Key Management (Retail), Part 2: Key Management Techniques for Symmetric Ciphers

ISO 11568–3: 1994 Banking Key Management (Retail), Part 3: Key Life Cycle for Symmetric Ciphers

ISO 11568–4: 1998 Banking Key Management (Retail), Part 4: Key Management Techniques for Asymmetric Ciphers

ISO 11568–5: 1998 Banking Key Management (Retail), Part 5: Key Life Cycle for Public Key Cryptosystems

ISO 11568–6: 1998 Banking Key Management (Retail), Part 6: Key Management Schemes

ISO 11770–2: 1996 Information Technology—Security Techniques—Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques

ISO 11770–3: 1999 Information Technology—Security Techniques—Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)

ISO 13491–1: 1998 Banking—Secure Cryptographic Devices (Retail), Part 1: Concepts, Requirements, and Evaluation Methods

Appendix B

Forms

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

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

PIN SECURITY REQUIREMENTS SELF-AUDIT COMPLIANCE STATEMENT

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

ORGANIZATION INFORMATION			
NAME			
ADDRESS			
CITY	STATE/PROVINCE	COUNTRY	POSTAL CODE
VISA BUSINESS ID (IF MEMBER): 10			
NAME OF SPONSORING INSTITUTION(S) (IF APPLICABLE)			
ORGANIZATION CONTACT	TELEPHONE	FAX	
TITLE	EMAIL		
DATE	SUBMITTED FOR YEAR OF	OR START-UP DATE	

COMPLIANCE STATEMENT

I, _____

(print or type name and title)

(check one)

- ❑ am an **internal auditor** for _____ and I have no operational responsibility for matters referenced in the PIN Security Requirements Self-Audit.

- ❑ am an **independent auditor** employed by _____and hired by _____to complete the PIN Security Requirements Self-Audit and the Compliance Statement.

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

(check one)

- ❑ **In full compliance** with the PIN Security Requirements Self-Audit.

- ❑ **Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____Date: _____

Officer Attestation:

I, _____

(print or type name and title)

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

(check one)

- ❑ **In full compliance** with the PIN Security Requirements Self-Audit.

- ❑ **Not in full compliance** as indicated by the attached Audit Exception Form(s).

Signature: _____Date: _____

PIN SECURITY REQUIREMENTS SELF-AUDIT PROCESSING ENVIRONMENT

PROCESSING ENVIRONMENT	
1.	Organization description (check one) ❑ Issuer only ❑ Acquirer only ❑ Both Issuer and Acquirer ❑ Third-Party Processor ❑ Other _____
2.	Do you process PIN-based transactions (drive ATMs or POS devices, or act as a switch to interchange networks)? ❑ yes ❑ no
3.	Does a third-party processor process your interchange PIN-based transactions? ❑ yes ❑ no If yes, by whom? _____ _____
4.	Does your organization perform any of the following Key Management functions? a. Loading keys/Initializing ATM's and/or Point of Sale devices? ❑ yes ❑ no b. Creating keys and/or key components for ATM's, POS or host security modules? ❑ yes ❑ no c. Conveying keys or key components to ATM/POS initialization personnel or to networks with whom you connect? ❑ yes ❑ no d. Storing keys or key components? ❑ yes ❑ no e. Destroying keys or key components? ❑ yes ❑ no
5.	Do you have *written* documentation for the functions in the previous question for which you answered yes? Please check those for which you have documentation. ❑ a. ❑ b. ❑ c. ❑ d. ❑ e

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

ATM	POS	Manufacturer	Model No.	Approx. Quantity
❑	❑			
❑	❑			
❑	❑			
❑	❑			
❑	❑			
❑	❑			

7. If you process your own PIN-based transactions or PIN-based transactions for others (answered "Yes" to question 2), please answer the following:

a. CPU/Operating System (release level) platforms used for PIN processing:

_____

_____

b. Security software: _____

c. Application software:

To drive devices: _____

For switching: _____

d. Host security module(s) used to secure encryption keys:

Make/models: _____

Quantity: _____

e. Do you have access to the source code for the application software?

❑ yes ❑ no

f. Estimated annual number of online PIN-based Interchange transactions for Visa Branded Products (Visa/Plus/Interlink/Visa Electron):

ATM: _____

POS: _____

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

_____

_____

_____

_____

PIN SECURITY REQUIREMENTS SELF-AUDIT EXCEPTION FORM

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

ORGANIZATION INFORMATION		
NAME		
DATE	SUBMITTED FOR YEAR OF	OR START-UP DATE
STATEMENT #		

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

_____

_____

_____

_____

Describe action plan implemented to correct this situation:

_____

_____

_____

_____

Date expected to be in compliance: _____

Auditor's signature: _____

Appendix C

PIN Security Requirements Self-Audit

I. General Security Procedures and Controls

This section covers the general procedures and controls which apply to all portions of the interchange security system.

Objective 1

PINs used in Visa transactions are processed using equipment and methodologies that ensure that they are kept secure.

yes ❑ no ❑ n/a ❑

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

A Tamper-Resistant Security Module (TRSM) must meet the requirements of a Physically Secure Device as defined in ISO 9564–1. Such a device must have a negligible probability of being successfully penetrated to disclose all or part of any cryptographic key or PIN. A TRSM can be so certified only after it has been determined that the device's internal operation has not been modified to allow penetration (for example, the insertion within the device of an active or passive "tapping" mechanism). A TRSM (for example, a PIN Entry Device (PED)) that complies with this definition may use a Fixed Key or a Master Key/Session Key key management technique, that is, a unique (at least) double-length PIN encryption key for each PED, or may use DUKPT as specified in ANSI X9.24.

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

PEDs must use encrypting PIN pads that encrypt the PIN directly at the point of entry to meet the requirements for compromise prevention. PEDs in which the cleartext (unenciphered) PIN travels over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.

Devices that do not retain any key that has been used to encrypt or decrypt secret data, including other keys, require only compromise detection, and may be less tamper resistant. TRSMs relying upon compromise detection controls must use DUKPT.

yes ❑ no ❑ n/a ❑

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

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

PINs must be encrypted using the TDEA Electronic Code Book (TECB) mode of operation as described in ANSI X9.52.

For purposes of these requirements, all references to TECB are using key options 1 or 2, as defined in ANSI X9.52.

yes ❑ no ❑ n/a ❑

3. For interchange transactions, PINs are only encrypted using ISO 9564–1 PIN block formats 0 or 3.

For secure transmission of the PIN from the point of PIN entry to the card issuer, the encrypted PIN block format must comply with ANSI Standard X9.8–1 or ISO 9564–1 format 0 (equivalent to Visa Format 1) or ISO 9564–1 format 3. The cleartext PIN block and the Primary Account Number block must be XOR'ed together to form the contents of the Data Encryption Standard (DES) algorithm input register, which must then be DES encrypted in Electronic Code Book (ECB) mode to form the 64-bit output cipherblock (the reversibly encrypted PIN block).

For encryption zones where the PIN encryption key is static for the productive life of the device in which it resides, ISO format 3 should be used.

yes	no	n/a
❑	❑	❑

4. PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary.

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

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

II. Key Management and Security

The purpose of these statements is to ensure that sufficient controls exist to minimize the risk of keys being compromised during their life cycle of creation, transmission, loading, and administration.

Objective 2

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.

yes ❑ no ❑ n/a ❑

5. 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.

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

Random or pseudo-random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values. An independent laboratory must certify self-developed implementations of a cryptographic pseudo-random number generator.

yes ❑ no ❑ n/a ❑

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

The output of the key generation process must be monitored by at least two authorized individuals, who ensure that there is not any unauthorized tap or other mechanism that might disclose a cleartext key or key component as it is transferred between the key generation TRSM and the device or medium receiving the key or key component.

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

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

yes ❑ no ❑ n/a ❑

7. Key components must exist as a minimum of two (at least) double-length values and 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 of the components.

The encryption key is created by automatically combining within a TRSM all entered key components. The separate 32 (or 48) hexadecimal character components must be XOR'ed together to create a unique key. Note that concatenated values do not satisfy this requirement.

Each thirty-two (forty-eight) hexadecimal character component, as well as the resulting key, must have a check value calculated for verification purposes using the entire 128 (192) bits in an Encrypt, Decrypt, Encrypt operation, whereby the resulting low order five bytes are discarded and the high order three bytes are the check value.

For devices that do not support the entry of full-length components, two (key halves) or more components must still be created.

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

---

yes ❑ no ❑ n/a ❑

8. Documented procedures exist and are used for all key generation processing.

Objective 3

Keys are conveyed or transmitted in a secure manner.

yes ❑ no ❑ n/a ❑

9. Encryption keys are transferred by:

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

b. Transmitting the key in ciphertext form.

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

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

Components of encryption keys must be transferred using different communication channels, such as different courier services. It is not sufficient to send key components for a specific key on different days using the same communication channel.

yes ❑ no ❑ n/a ❑

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

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

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

c. In a physically secure TRSM.

Key components are the separate parts of a cleartext key that have been created for transport to another endpoint in a symmetrical cryptographic system. Typically, key components exist for Key Encryption Keys, such as keys used to encrypt Working Keys for transport across some communication channel. Until such keys can be protected by encryption, or by inclusion in a TRSM, the separate parts must be managed under the strict principles of dual control and

split knowledge. Dual control involves a process of using two or more separate entities (usually persons), which are operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of the materials involved. No single person shall be able to access or to use all components of a single cryptographic key. Split knowledge is a condition under which two or more entities separately have key components that, individually, convey no knowledge of the resultant cryptographic key.

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

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

---

yes ❑ **no** ❑ **n/a** ❑

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

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

---

yes ❑ **no** ❑ **n/a** ❑

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

Objective 4

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

yes ❑ no ❑ n/a ❑

13. 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.

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

Host Security Module (HSM) Master File Keys, including those generated internal to the HSM and never exported, must be at least double-length keys and use the TDEA electronic codebook mode of operation for key encipherment.

yes ❑ no ❑ n/a ❑

14. 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.

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

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

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

- Use public and private key lengths that are deemed acceptable for the algorithm in question; for example, 1024-bits minimum for RSA.
- Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question.

- Provide for mutual device authentication for both the host and the PED, including assurance to the host that the PED actually has (or actually can) compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key.

---

yes ❑ no ❑ n/a ❑

15. The transfer mechanisms, such as terminals, external 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 type of monitoring that could result in the unauthorized disclosure of any component.

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

A TRSM must transfer a plaintext key only when at least two authorized individuals are identified by the device, for example, by means of passwords.

Plaintext keys and key components must be transferred into a TRSM only when it can be ensured that there is not any tap at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys and that the device has not been subject to prior tampering which might lead to the disclosure of keys or sensitive data.

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

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

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

- The key-loading device is a physically secure TRSM, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected; *and*
- The key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it; *and*

- The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another TRSM. Such personnel must ensure that there is not a key-recording device inserted between the TRSMs; *and*
- The key-loading device must not retain any information that might disclose the key or a key that it has successfully transferred.

---

yes ❑ no ❑ n/a ❑

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

Any hardware used in the key-loading function must be controlled and maintained in a secure environment under dual control. Use of the equipment must be monitored and a log of all key-loading activities maintained for audit purposes. All cable attachments must be examined before each application to ensure that there has not been any tampering.

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

---

yes ❑ no ❑ n/a ❑

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

The media upon which a component resides must be physically safeguarded at all times.

Any tokens, EPROMs, or other key component holders used in loading encryption keys must be maintained using the same controls used in maintaining the security of hard copy key components. These devices must be in the physical possession of only the designated component holder and only for the minimum practical time.

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

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

Printed key component documents are not opened until just prior to entry.

The component is never in the physical possession of an entity when any one such entity is or ever has been similarly entrusted with any other component of this same key.

---

yes ❑ no ❑ n/a ❑

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

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

---

yes ❑ no ❑ n/a ❑

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

Objective 5

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

yes ❑ no ❑ n/a ❑

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

Where two organizations share a key to encrypt PINs (including key encipherment keys used to encrypt the PIN encryption key) communicated between them, that key must be unique to those two organizations and must not be given to any other organization. This technique of using unique keys for communication between two organizations is referred to as zone encryption and is required. Keys may exist at more than one pair of locations for disaster recovery or load balancing (for example, dual processing sites).

yes ❑ no ❑ n/a ❑

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

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

Key component documents showing signs of tampering result in the discarding and invalidation of the component and the associated key at all locations where they exist to prevent substitution of a compromised key for a legitimate key.

yes ❑ no ❑ n/a ❑

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

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

yes ❑ no ❑ n/a ❑

23. 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.

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

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

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

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

Objective 6

Keys are administered in a secure manner.

yes	no	n/a
❑	❑	❑

24. 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.

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

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

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

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

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

Keys that are used to encipher other keys or to encipher PINs, and which exist outside of a TRSM, must be enciphered using at least double-length keys and be enciphered using the TDEA electronic codebook mode of operation. A double- or triple-length DES key must not be encrypted with a DES key of a shorter length.

Symmetric secret keys may be enciphered using public key cryptography for distribution to PEDs as part of a key-establishment protocol as defined in Question 14.

yes ❑ no ❑ n/a ❑

25. 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.

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

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

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

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

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

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

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

yes ❑ no ❑ n/a ❑

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

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

yes ❑ no ❑ n/a ❑

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

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

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

Visa requires the destruction of the Visa ZCMK after successful loading and verification.

yes ❑ no ❑ n/a ❑

28. 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 effective use.

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

yes ❑ no ❑ n/a ❑

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

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

---

yes ❑ no ❑ n/a ❑

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

The backup copies must be securely stored with proper access controls and under at least dual control and subject to at least the same level of security control as keys in current use (see question 24).

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

---

yes ❑ no ❑ n/a ❑

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

III. Equipment Security and Control

The purpose of this section is to ensure that all equipment is managed consistent with requirements in this document and that proper controls have been implemented to maximize the operational security of that equipment.

Objective 7

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

yes ❑ **no** ❑ **n/a** ❑ **32. 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.**

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

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

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

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

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

- Devices incorporate self-tests to ensure their correct operation. Devices are not re-installed unless there is assurance they have not been tampered with or compromised.
- Controls exist and are used to ensure that all physical and logical controls and anti-tamper mechanisms used are not modified or removed.

Documented inventory control and monitoring procedures must exist to track equipment by both physical and logical identifiers in such a way as to protect the equipment against unauthorized substitution or modification until a secret key has been loaded into it and to detect lost or stolen equipment.

Procedures should include ensuring that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.

---

yes ❑ no ❑ n/a ❑

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

TRSMs known to be permanently removed from service must have all keys stored within the device destroyed, which have ever been used, or potentially could be, for any cryptographic purpose.

- All critical initialization, deployment, usage and decommissioning processes enforce dual control and split knowledge, for example, key- or component-loading, firmware- or software-loading, and verification and activation of anti-tamper mechanisms.
- Key and data storage are zeroized when a device is decommissioned.

If the erasure of all cryptographic keys, keying material, and sensitive data cannot be assured, the device must be physically destroyed such that it cannot be placed into service again, or allow the disclosure of any secret data or keys.

yes ❑ no ❑ n/a ❑

34. 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) under dual control.

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

---

yes ❑ no ❑ n/a ❑

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

Glossary

Access Controls

Ensuring that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.

Acquirer

The institution (or its agent) that receives from a card acceptor the data relating to financial transactions with PINs. The acquirer is the entity that forwards the financial transaction into an interchange system.

Algorithm

A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.

ANSI

American National Standards Institute. A U.S. standards accreditation organization.

ATM

An unattended terminal that has electronic capability, accepts PINs, and disburses currency or cheques.

Authentication

The process for establishing unambiguously the identity of an entity, organization or person.

Authorization

The right granted to a user to access an object, resource or function.

Authorize

To permit or give authority to a user to communicate with or make use of an object, resource or function.

Base (master) derivation key

See Derivation key.

Business Identifier

The Visa Business Identifier (BID) is an eight-character identifier assigned by Visa to a member financial institution. The combination of BID and country code uniquely identifies a Visa entity.

Cardholder

An individual to whom a card is issued or who is authorized to use the card.

Card issuer

The institution or its agent that issues the identification card to the cardholder.

Check value

A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible.

Ciphertext

Data in its enciphered form.

Cleartext

See Plaintext.

Communicating nodes

Two entities (usually institutions) sending and receiving transactions. This is to include alternate processing sites either owned or contracted by either communicating entity.

Compromise

In cryptography, the breaching of secrecy and/or security.

A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other keying material).

Cryptographic key

A parameter used in conjunction with a cryptographic algorithm that determines:

- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- A digital signature computed from data,
- The verification of a digital signature computed from data,
- An authentication code computed from data, or
- An exchange agreement of a shared secret.

Cryptographic key component

A parameter used in conjunction with other key components in an approved security function to form a plaintext cryptographic key or perform a cryptographic function.

Data Encryption Algorithm (DEA)

A published encryption algorithm used to protect critical information by enciphering data based upon a variable secret key. The Data Encryption Algorithm is defined in ANSI X3.92: "Data Encryption Algorithm" for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.

Decipher

See Decrypt.

Decrypt

A process of transforming ciphertext (unreadable) into plain text (readable).

Derivation key

A double-length key, which is used to cryptographically compute another key. A double-length derivation key is normally associated with the Derived Unique Key Per Transaction key management method.

Derivation keys are normally used in a transaction-receiving (e.g., acquirer) TRSM in a one-to-many relationship to derive or decrypt the Transaction (the derived keys) Keys used by a large number of originating (e.g., terminal) TRSMs.

DES

Data Encryption Standard (see Data Encryption Algorithm). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. government as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the data encryption algorithm.

Double-length key

A cryptographic key having a length of 112 active bits plus 16 parity bits.

Dual control

A process of using two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see "split knowledge."

DUKPT

Derived Unique Key Per Transaction: a key management method that uses a unique key for each transaction, and prevents the disclosure of any past key used by the transaction originating TRSM. The unique Transaction Keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.

ECB

Electronic codebook.

Electronic Code Book (ECB) Operation

A mode of encryption using the data encryption algorithm, in which each block of data is enciphered or deciphered without an initial chaining vector.

EEPROM

Electronically-Erasable Programmable Read-Only Memory.

Electronic key entry

The entry of cryptographic keys into a secure cryptographic device in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.

Encipher

See Encrypt.

Encrypt

The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.

EPROM

Erasable Programmable Read-Only Memory.

Exclusive-OR

Binary addition without carry, also known as modulo 2 addition, symbolized as "XOR" and defined as:

- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 0

FIPS

Federal Information Processing Standard.

Firmware

The programs and data (i.e., software) permanently stored in hardware (e.g., in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.

Hardware (Host) Security Module

A physically and logically protected hardware device that provides a secure set of cryptographic services.

Hash

A (mathematical) function which is a non-secret algorithm, which takes any arbitrary length message as input and produces a fixed length hash result. It must have the property that it is computationally infeasible to discover two different messages, which produce the same hash result. It may be used to reduce a potentially long message into a "hash value" or "message digest" which is sufficiently compact to be input into a digital signature algorithm. A "good" hash is such that the results of applying the function to a (large) set of values in a given domain will be evenly (and randomly) distributed over a smaller range.

Hexadecimal character

A single character in the range 0-9, A-F (upper case), representing a four-bit string.

Initialization Vector

A binary vector used as the input to initialize the algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.

Integrity

Ensuring consistency of data; in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.

Interchange

The exchange of clearing records between members. The Visa International Operating Regulations refers to domestic and international interchange.

Interface

A logical section of a cryptographic device that defines a set of entry or exit points that provide access to the device, including information flow or physical access.

Irreversible transformation

A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.

ISO

International Organisation for Standardisation. An international standards accreditation organization.

Issuer

The institution holding the account identified by the primary account number (PAN).

Key

See Cryptographic key.

Key agreement

A key establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. that is, the secret key is a function of information contributed by two or more participants.

Key backup

Storage of a protected copy of a key during its operational use.

Key component

See Cryptographic Key Component.

Key derivation process

A process, which derives one or more session keys from a shared secret and (possibly) other, public information.

Key destruction

Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.

Key encrypting (encipherment) key

A cryptographic key that is used for the encryption or decryption of other keys.

Key establishment

The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.

Key generation

Creation of a new key for subsequent use.

Key instance

The occurrence of a key in one of its permissible forms, i.e., plaintext key, key components, enciphered key.

Key loading

Process by which a key is manually or electronically transferred into a secure cryptographic device.

Key management

The activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction and archiving.

Key replacement

Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.

Key storage

Holding of the key in one of the permissible forms.

Key transport

A key establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.

Key usage

Employment of a key for the cryptographic purpose for which it was intended.

Key variant

A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.

Keying material

The data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships.

Key-loading device

A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Manual key loading

The entry of cryptographic keys into a secure cryptographic device from a printed form, using devices such as buttons, thumb wheels or a keyboard.

Master derivation key

See Derivation key.

Master key

In a hierarchy of Key Encrypting Keys and Transaction Keys, the highest level of Key Encrypting Key is known as a Master Key.

Member

An entity that is a member of Visa. Refer to the *Visa International Operating Regulations* for information about the different types of members.

Merchant

An entity that contracts with an acquirer to originate transactions and that displays the Visa symbol, Electron symbol, or both. Refer to the *Visa International Operating Regulations* for information about the different types of merchants.

Message

A communication containing one or more transactions or related information.

Node

Any point in a network that does some form of processing of data, such as a terminal, acquirer, or switch.

Non-reversible transformation

See Irreversible Transformation.

Personal Identification Number (PIN)

A personal identification code that identifies a cardholder in an authorization request that originates at a terminal with authorization-only or data capture-only capability. A PIN may be alphabetic, numeric, or a combination of both.

Physical protection

The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.

PIN

See Personal Identification Number.

PIN Entry Device (PED)

A keypad, laid out in a prescribed format, combined with electronic components housed in a tamper resistant or tamper evident shell that can capture and encrypt cardholder PINs.

PIN pad

See PIN Entry Device.

Plaintext

Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as cleartext.

Plaintext key

An unencrypted cryptographic key, which is used in its current form.

Private key

A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and is not made public.

In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.

Processor

A member, Visa, or a Visa-approved nonmember acting as the agent of a member, that provides authorization, clearing, or settlement services for merchants and members.

PROM

Programmable Read-Only Memory.

Pseudo-random

A value that is statistically random and essentially random and unpredictable although generated by an algorithm.

Public key

A cryptographic key, used with a public key cryptographic algorithm, uniquely associated with an entity, and that may be made public

In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Public key (asymmetric) cryptography

A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation.

A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system.

With asymmetric cryptographic techniques, there are four elementary transformations: sign and verify for signature systems, and encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exists asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation and where used the four elementary transformations and the corresponding keys should be kept separate.

Random

The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware based 'noise' mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.

ROM

Read-Only Memory.

Secret key

A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. A secret key (symmetrical) cryptographic algorithm uses a single secret key for both encryption and decryption. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.

Sensitive data

Data which must be protected against unauthorized disclosure, alteration or destruction, especially plaintext PINs and cryptographic keys, and includes design characteristics, status information, and so forth.

Session key

A key established by a key management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, e.g., an encryption key and a MAC key.

Shared Secret

The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key derivation function to derive session keys.

Single-length key

A cryptographic key having a length of 56 active bits plus 8 parity bits.

Software

The programs and associated data that can be dynamically written and modified.

Split knowledge

A condition under which two or more entities separately have key components that, individually, convey no knowledge of the resultant cryptographic key.

Symmetric key

A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.

System software

The special software (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.

Switch

A node that can route data from a node to other nodes.

Tamper-evident

A characteristic that provides evidence that an attack has been attempted.

Tampering

The penetration or modification of internal operation and/or insertion of active or passive tapping mechanisms to determine or record secret data.

TECB

TDEA electronic codebook.

Terminal

A device/system that initiates a transaction.

Transaction

A series of messages to perform a predefined function.

Triple Data Encryption Algorithm (TDEA)

The algorithm specified in ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.

Triple Data Encryption Standard (TDES)

See Triple Data Encryption Algorithm.

Triple-length key

A cryptographic key having a length of 168 active bits plus 24 parity bits.

TRSM

Tamper-Resistant Security Module: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Variant of a key

A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.

Verification

The process of associating and/or checking a unique characteristic.

Working key

A key used to cryptographically process the transaction. A Working Key is sometimes referred to as a Data Key, communications key, session key, or transaction key.

XOR

See Exclusive-Or.

Zeroize

The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.

Zone Control Master Key

A master key used to encrypt working keys conveyed between nodes on a network. Visa generates and conveys ZCMKs to all members and processors connected to VisaNet.