

PIN Security Requirements 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: _____

Processing Environment

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
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			

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:

Encrypted PIN Pads (EPPs) & Triple Data Encryption Standards (TDES)

9. Are EPPs installed in all your ATMs?

yes no

10. Are approved EPPs installed in your newly-deployed ATMs?

yes no

If answer is 'no', provide EPP deployment plan and specify expected completion date _____

11. Are approved PIN Entry Devices (PEDs) installed in your newly-deployed POS terminals that support PIN-based transactions?

yes no

If answer is 'no', specify date where the deployment expected completion date _____

12. Can Visa's deadline of July 1, 2007 for end-to-end TDES encryption be met?

yes no

If answer is 'yes', specify expected completion date _____

If answer is 'no', provide action plan and explain which part of the network will not be in compliance. The expected completion date is _____

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

OBJECTIVE 1

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

- | | Yes | No | N/A |
|---|--------------------------|--------------------------|--------------------------|
| 1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). PINs must never appear in the clear outside of a TRSM. The following two instances of TRSMs are considered: <ul style="list-style-type: none"> • Tamper responsive or physically secure devices: penetration of the device will cause immediate erasure of all PINs, cryptographic keys and all useful residues of PINs and keys contained within it. • Tamper-evident or minimum acceptable PIN Entry Devices: any attempt to penetrate the device will be obvious. Such a device can only be used for PIN encryption and key management schemes where penetration of the device will offer no information on previously entered PINs or secret keys. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2a. All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2b. All cardholder PINs processed offline using IC Card technology must be protected in accordance with the requirements in Book 2 of the EMV2000 IC Card Specifications for Payment Systems. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. For online interchange transactions, PINs are only encrypted using ISO 9564-1 PIN block formats 0, 1 or 3. Format 2 must be used for PINs that are submitted from the IC reader to the IC. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

OBJECTIVE 2

Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.

5.	All keys and key components are generated using an approved random or pseudo-random process.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
7.	Documented procedures exist and are demonstrably in use for all key generation processing.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

OBJECTIVE 3

Keys are conveyed or transmitted in a secure manner.

8.	Secret or private keys are transferred by:	Yes	No	N/A
	a. Physically forwarding the key in at least two separate full-length components (hard copy, smart card, TRSM) using different communication channels, or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	b. Transmitting the key in ciphertext form.			
	Public keys must be conveyed in a manner that protects their integrity and authenticity.			
9.	Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities:	Yes	No	N/A
	a. Under the continuous supervision of a person with authorized access to this component, or	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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.			
10.	All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	Yes	No	N/A
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	Yes	No	N/A
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OBJECTIVE 4

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

12. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
13. The mechanisms used to load keys, such as terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
14. All hardware and passwords used for key loading are managed under dual control.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
16. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

OBJECTIVE 5

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

- | | | | |
|--|---------------------------------|--------------------------------|---------------------------------|
| 17. Unique cryptographic keys must be in use for each identifiable link between host computer systems. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 18. Procedures exist to prevent or detect the unauthorized substitution of one key for another or the operation of any cryptographic device without legitimate keys. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 20. All cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (PED) that processes PINs must be unique (except by chance) to that device. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |

OBJECTIVE 6

Keys are administered in a secure manner.

21. Keys used for enciphering PIN-Encryption keys, or for PIN Encryption, must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
22. Procedures exist and are demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
23. Key variants are only used in devices that possess the original key.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
24. Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
25. Access to cryptographic keys and key material must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
26. Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
27. 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.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>
28. Documented procedures exist and are demonstrably in use for all key administration operations.	Yes <input type="checkbox"/>	No <input type="checkbox"/>	N/A <input type="checkbox"/>

OBJECTIVE 7

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

- | | | | |
|--|---------------------------------|--------------------------------|---------------------------------|
| 29. PIN-processing equipment (PEDs and HSMS) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 30. Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 31. Any TRSM capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following:

a. Dual access controls are required to enable the key encryption function.

b. Physical protection of the equipment (e.g., locked access to it) under dual control. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |
| 32. Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMS) placed into service, initialized, deployed, used, and decommissioned. | Yes
<input type="checkbox"/> | No
<input type="checkbox"/> | N/A
<input type="checkbox"/> |