PCI PIN VERSION 2.0-3.0
REQUIREMENTS

PCI PIN SECURITY

- There has been increase in cybercrimes due to increase in electronic transactions.
- That’s why, its important to keep PIN (Personal Identification Number) save in order to secure transactions.
- PCI PIN, a global forum committed to keep payments secure, has formulated a set of requirements for secure, transaction, processing and management PIN data during transactions both online and offline.
- 33 requirements has been organised in 7 groups named as Control Objectives to ensure protection of PIN data during electronic payments.

PCI PIN VERSION 2.0-3.0 REQUIREMENTS

- Requirements has been presented along with:

1. Section (Overview, Annex A, Annex B, TPO etc.)
2. Type (Clarification OR Addition)
3. Description

Requirement	Section	Type
General	Organization	Clarification

PCI PIN 3.0 Description

- Clarified that entities may be subject to requirements in multiple sections, depending on the activities that they perform.

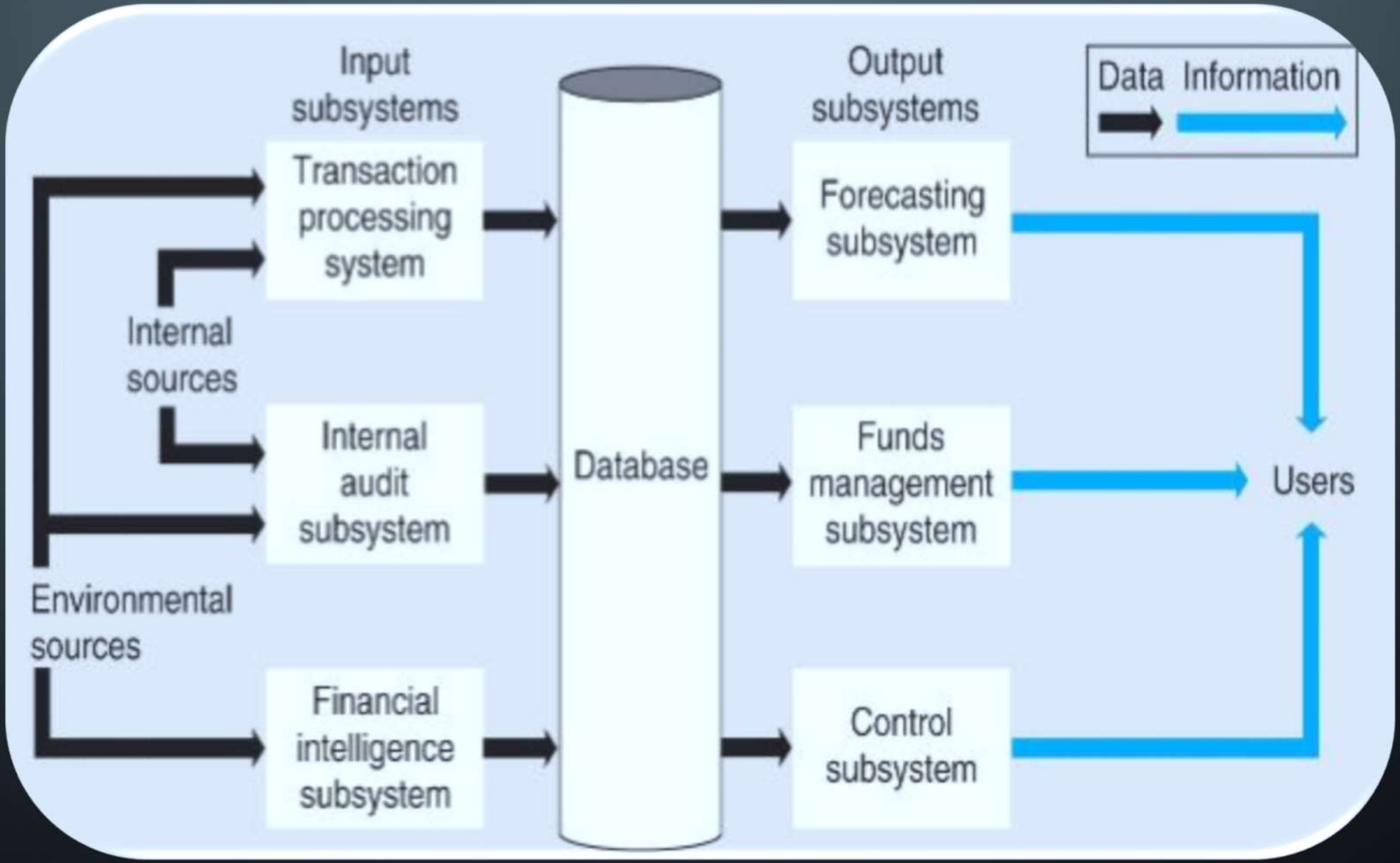
Requirement	Section	Type
General	Summary Listings and Schematics	Addition

PCI PIN 3.0 Description

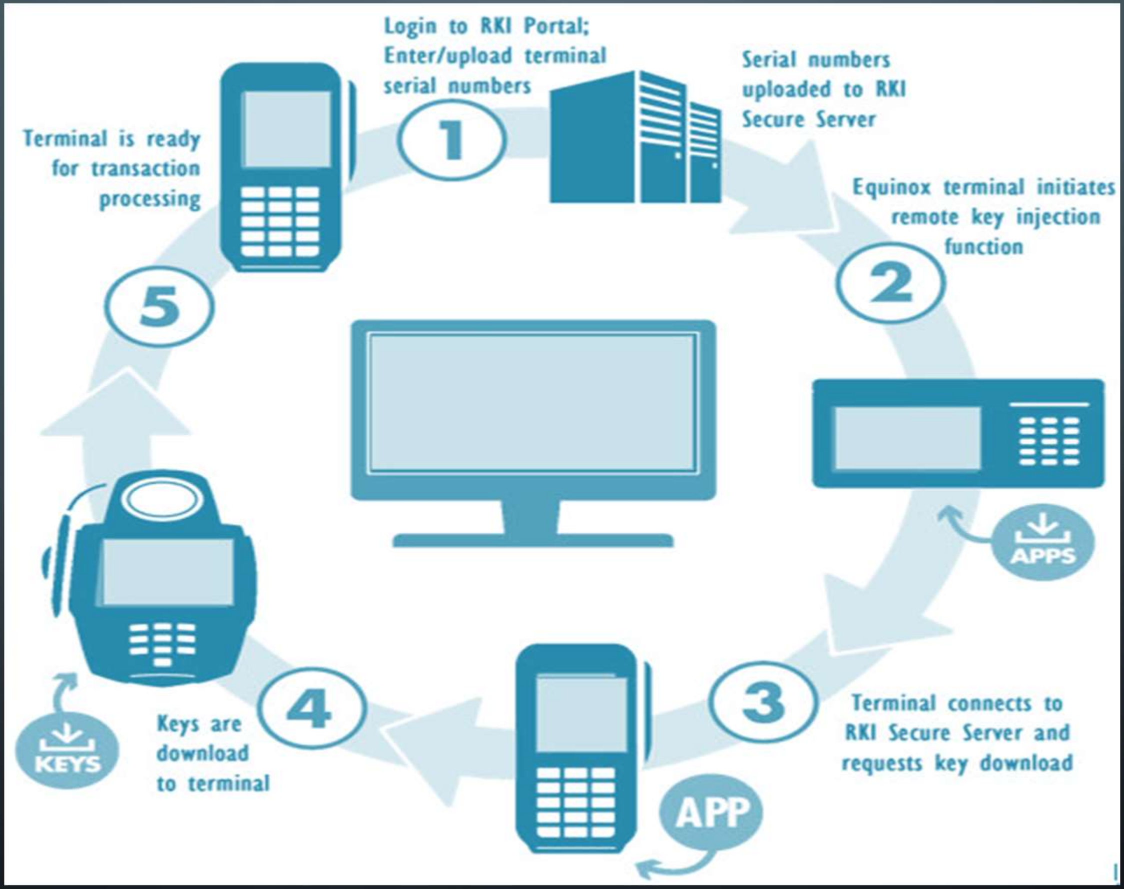
- Added criteria to facilitate reviews that all entities subject to these requirements must maintain a summary listing of the cryptographic keys used, including identification of the algorithm (e.g., AES, TDES, RSA) used and key size (e.g., 128, 2048) for each key type for activities in which they engage, whether for:

1. Transaction Processing Operations.
2. Symmetric Key distribution Using Asymmetric Techniques.
3. Key-Injection Facilities (KIFs).

TRANSACTION PROCESSING OPERATIONS



KEY-INJECTION FACILITIES (KIFS)



Login to RKI Portal; Enter/upload terminal serial numbers

Serial numbers uploaded to RKI Secure Server

Equinox terminal initiates remote key injection function

Terminal connects to RKI Secure Server and requests key download

Keys are download to terminal

Terminal is ready for transaction processing

SYMMETRIC KEY DISTRIBUTION USING ASYMMETRIC TECHNIQUES

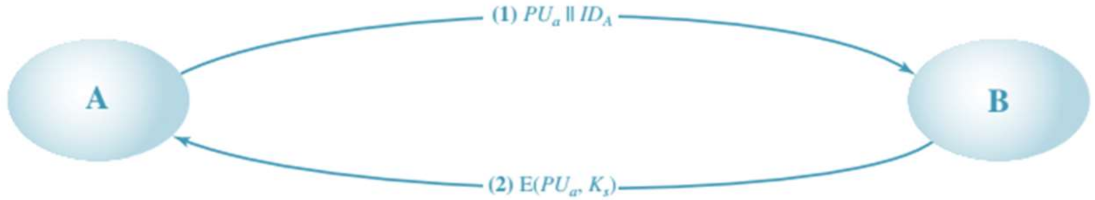


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

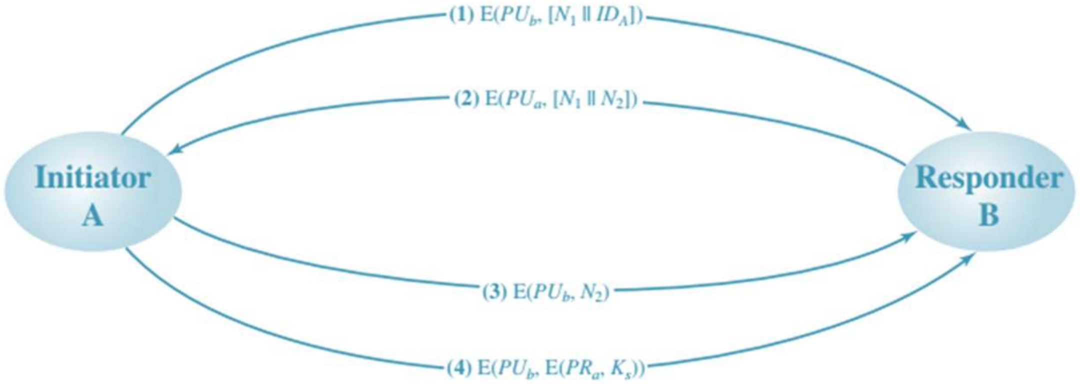

(1) $E(PU_b, [N_1 \| ID_A])$
(2) $E(PU_a, [N_1 \| N_2])$
Initiator A
Responder B
(3) $E(PU_b, N_2)$
(4) $E(PU_b, E(PR_a, K_s))$

Figure 14.8 Public-Key Distribution of Secret Keys

Requirement → General

Section → Organization

Type → Clarification

PCI PIN 3.0 Description

- Fixed key TDES Sunset dates have been added:

1. Effective January 1, 2023: Fixed key for TDES PIN encryption in POI devices is disallowed.
2. Effective January 1, 2023: Fixed keys for TDES PIN encryption in host-to-host connections is disallowed.

- ISO PIN block format 4 effective dates added:

1. Effective January 1, 2023: All hosts must support ISO PIN block format 4 decryption.
2. Effective January 1, 2025: All hosts must support ISO PIN block format 4 encryption.

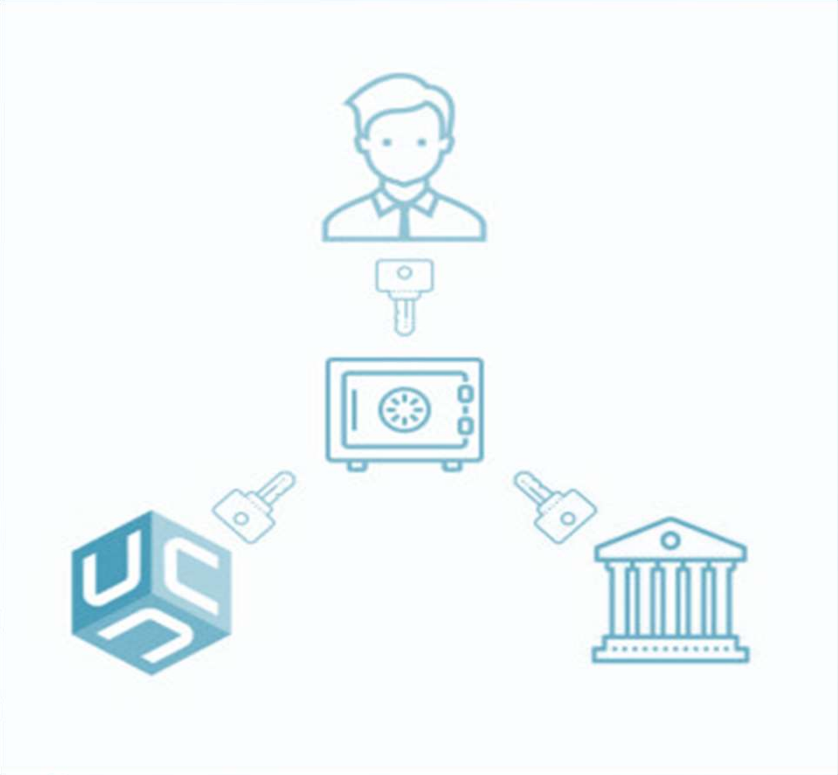
Requirement	Section	Type
3-Feb	TPO Annex B	Addition

PCI PIN 3.0 Description

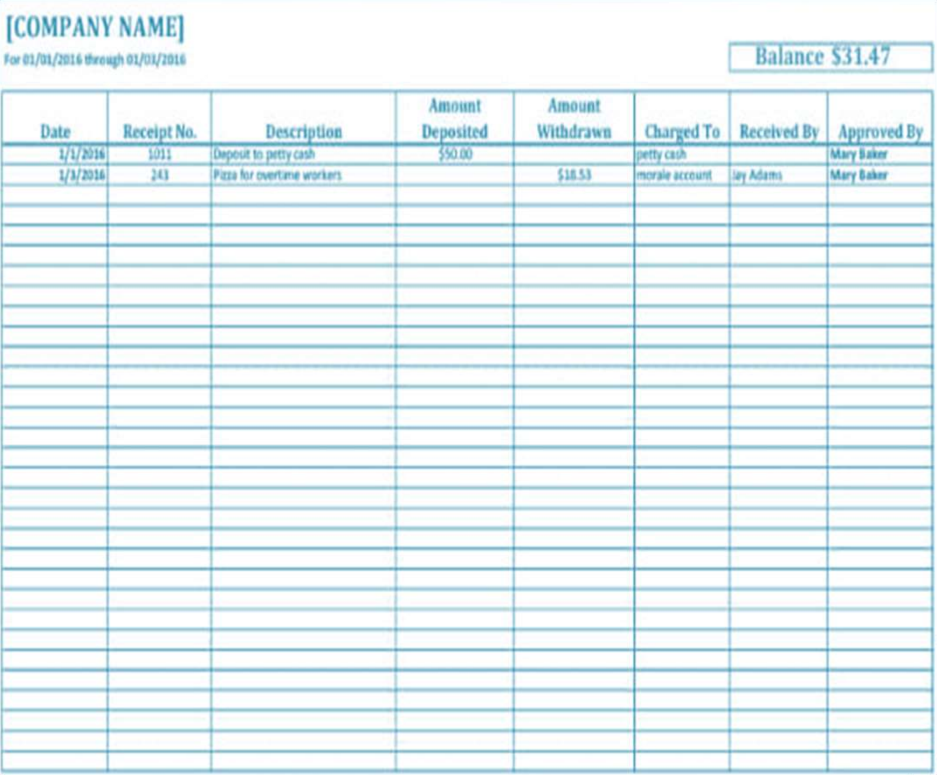
- Added note for sunset dates for use of fixed key TDES:

1. Effective January 1, 2023: Fixed key for TDES PIN encryption in POI devices is disallowed.
2. Effective January 1, 2023: Fixed keys for TDES PIN encryption in host-to-host connections is disallowed.

THREE KEY CUSTODIANS



LOGBOOK



[COMPANY NAME]

For 01/01/2016 through 01/03/2016

Balance $31.47

Date	Receipt No.	Description	Amount Deposited	Amount Withdrawn	Charged To	Received By	Approved By
1/1/2016	1011	Deposit to petty cash	$50.00		petty cash		Mary Baker
1/3/2016	243	Pizza for overtime workers		$18.53	morale account	Jay Adams	Mary Baker

Requirement	Section	Type
3-Feb	TPO Annex B	Addition

PCI PIN 3.0 Description

- ISO PIN block format 4 effective dates added:

1. Effective January 1, 2023: All hosts must support ISO PIN block format 4 decryption.
2. Effective January 1, 2025 All hosts must support ISO PIN block format 4 encryption.

Requirement
1-May

Section
TPO
Annex B

Type
Addition

PCI PIN 3.0 Description

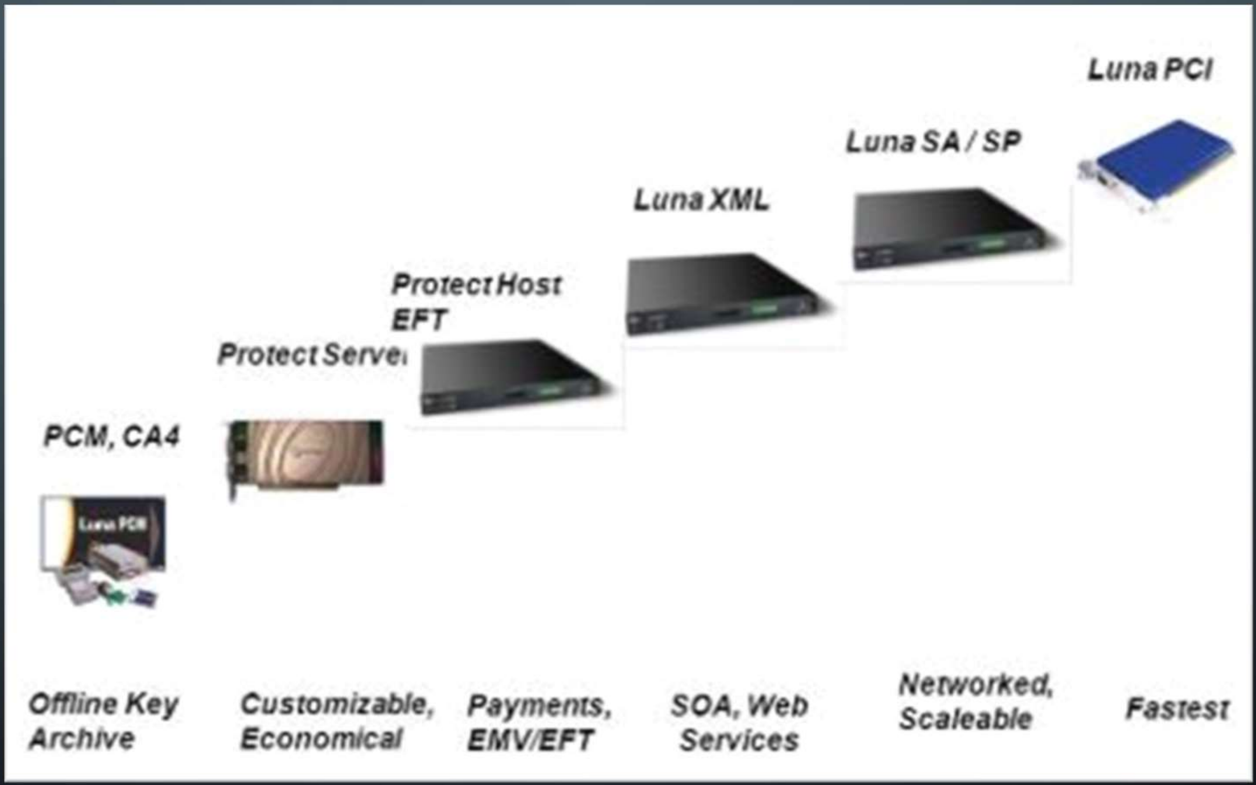
- Added that that key generation must occur within an approved SCD.
- Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Generation of cryptographic keys or key components must occur within an SCD. They must be generated by one of the following:

Requirement	Section	Type
1-May	TPO Annex B	Addition

PCI PIN 3.0 Description

1. An approved key generation function of a PCI approved HSM or POI.
2. An approved key generation function of a FIPS 140-2 Level 3 (or higher) HSM.
3. An SCD that has an approved random number generator that has been certified by an independent laboratory to comply with *NIST SP 800-22*.

HOST SECURITY MODULES (HSMS)



Requirement
6-1.1

Section
TPO
Annex B

Type
Clarification

PCI PIN 3.0 Description

- Clarified that only assigned custodian can have access to clear text keys.
- Any clear-text output of the key generation process must be managed under dual control.
- Only the assigned custodian can have direct access to the clear text of any key component/share. Each custodian’s access to clear-text output is limited to the individual component(s)/share(s) assigned to that custodian, and not the entire key.

Requirement	Section	Type
6-1.4	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Clarified that equipment used for the generation of clear-text key components must be inspected for signs of tampering prior to the initialization of key-generation activities.
- Key-generation equipment used for generation of clear-text key components must not show any signs of tampering (for example, unknown cables) and must be inspected prior to the initialization of key-generation activities.
- Ensure there isn't any mechanism that might disclose a clear-text key or key component (e.g., a tapping device) between the key-generation device and the device or medium receiving the key or key component.

Note: This does not apply to logically partitioned devices located in data centres that are concurrently used for other purposes.

Requirement	Section	Type
2 June	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Clarified that multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory outside the tamper-protected boundary of an SCD.
- Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in memory outside the tamper-protected boundary of an SCD.

Requirement	Section	Type
2 June	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Clarified that dedicated computers using an SCD meeting Requirement 5.1 may be used for key generation.
- For example, it is not permitted for the cryptographic key to be passed through the memory of a computer unless it has been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed and used solely for key loading are permitted for use if all other requirements can be met, including those of Requirement 5 and the controls defined in Requirement 13 of Annex B.

Requirement	Section	Type
2 June	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Additionally, this requirement excludes from its scope computers used only for administration of SCDs, or key-generation devices that do not have the ability to access cleartext cryptographic keys or components.
- Single-purpose computers with an installed SCD or a modified PED where clear keying material is injected directly from a secure port on the key-generating SCD to the target SCD (e.g., a POI device) meet this requirement. Where the components pass through memory of the PC, Requirement 13 of Annex B must be met
- SCDs used for key generation must meet Requirement 5.1.

Note: See Requirement 5 and Annex B, Requirement.

Requirement

3 June

Section

TPO
Annex B

Type

Clarification

PCI PIN 3.0 Description

- Clarification for printers used for printing key components.
- Printed key components must be printed within blind mailers or sealed in tamper-evident and authenticable packaging immediately after printing or transcription to ensure that:

1. Only approved key custodians can observe the key component.
2. Tampering can be visually detected.

Requirement	Section	Type
3 June	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Printers used for this purpose must not be used for other purposes, must not be networked (i.e., locally connected), and must be managed under dual control, including use of a secure room that meets the requirements of 32- 9 in Annex B.

Requirement

2 July

Section

TPO
Annex B

Type

Clarification

PCI PIN 3.0 Description

- Specified minimum requirements for logs for the generation of higher-level keys.
- Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs.
- The minimum log contents include date and time, object name/identifier, purpose, name and signature of individual(s) involved, and tamper-evident package number(s) and serial number(s) of device(s) involved.

Requirement	Section	Type
4 August	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Clarified that self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data.
- Self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data.
- The authenticity of the root certificate is based on the use of secure procedure to distribute them.
- Specifically, they must be directly installed into the PIN pad of the ATM or POS device and not remotely loaded to the device subsequent to manufacture.

Requirement

10

Section

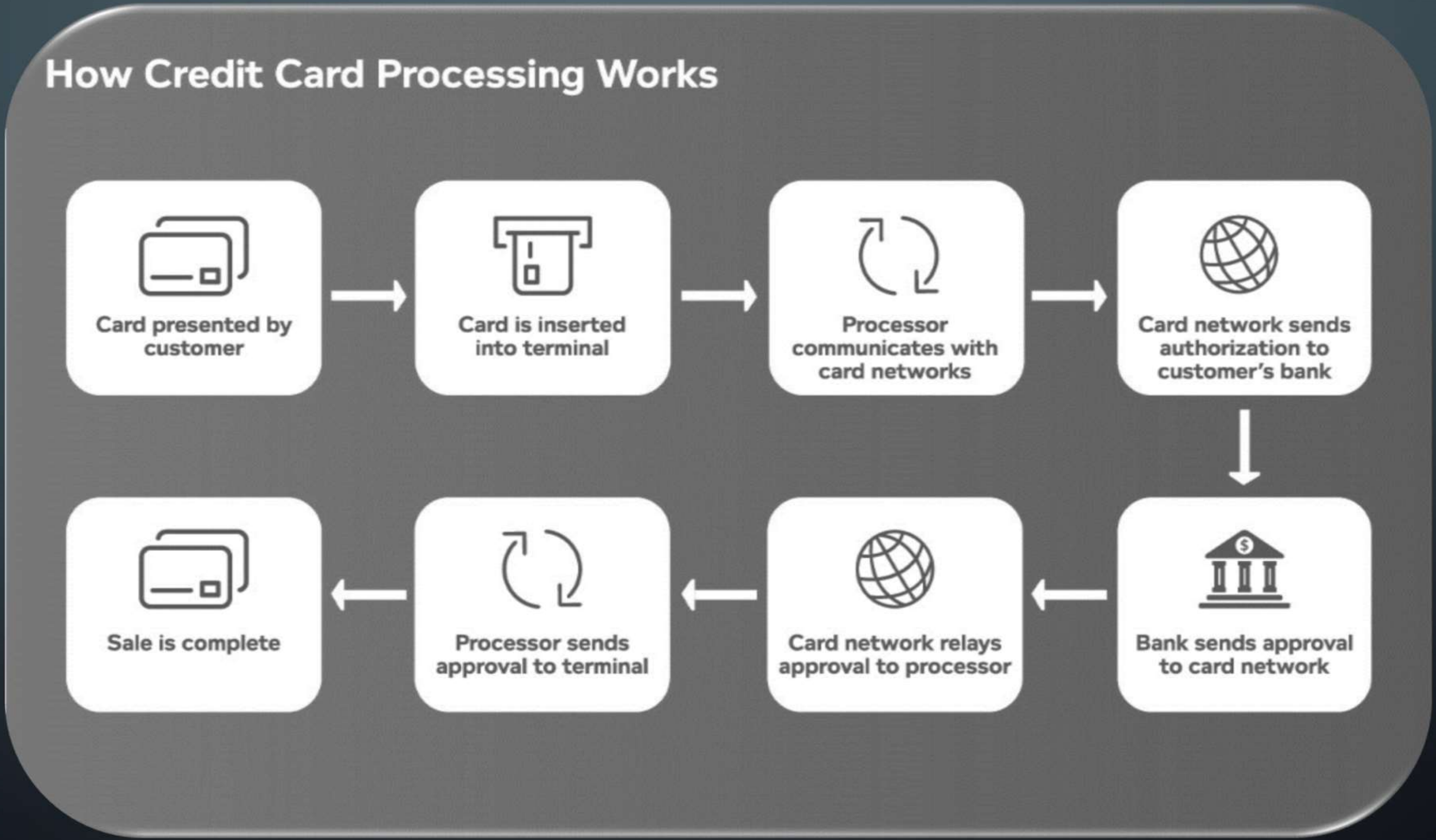
Annex B

Type

Clarification

PCI PIN 3.0 Description

- Clarified that key-conveyance requirements apply to between locations or systems within the same key-injection facility.
- Key-encryption keys used to convey keys to a key-injection facility or between locations or systems within the same key-injection facility must be at least as strong as any key transmitted or conveyed.
- Such keys include but are not limited to, key-encryption keys used to encrypt the BDKs when the BDKs are conveyed between entities, locations, or systems (e.g., from the BDK owner to a device manufacturer that is performing key-injection on their behalf, or from a merchant to a third party that is performing key-injection on their behalf) for system migration, or transport between injection locations owned by the same organization.



How Credit Card Processing Works

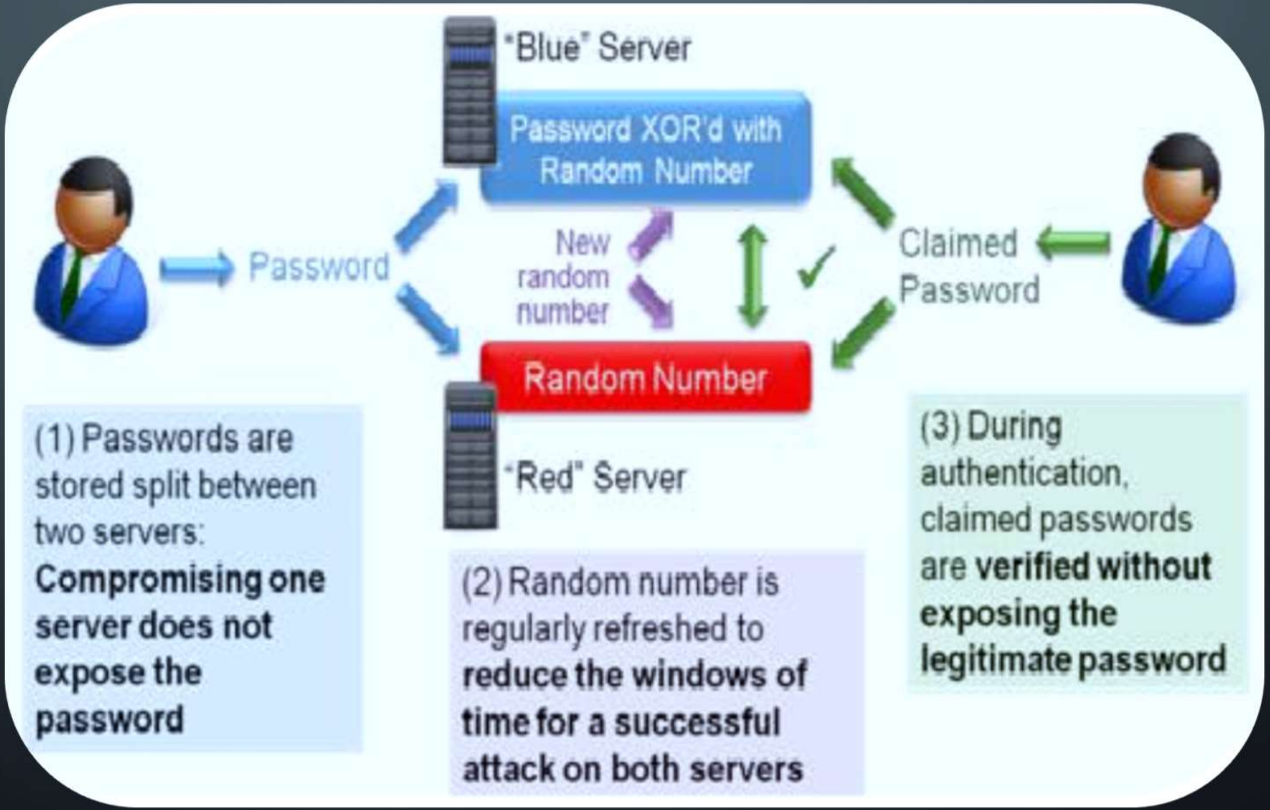
1. Card presented by customer
2. Card is inserted into terminal
3. Processor communicates with card networks
4. Card network sends authorization to customer's bank
5. Bank sends approval to card network
6. Card network relays approval to processor
7. Processor sends approval to terminal
8. Sale is complete

Requirement	Section	Type
3 December	TPO Annex B	Clarification

PCI PIN 3.0 Description

- Clarification that dual control includes separate key-loading devices for each component/share.
- Added that for devices that do not support two or more passwords, this may be achieved by splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian.

TWO OR MORE PASSWORDS

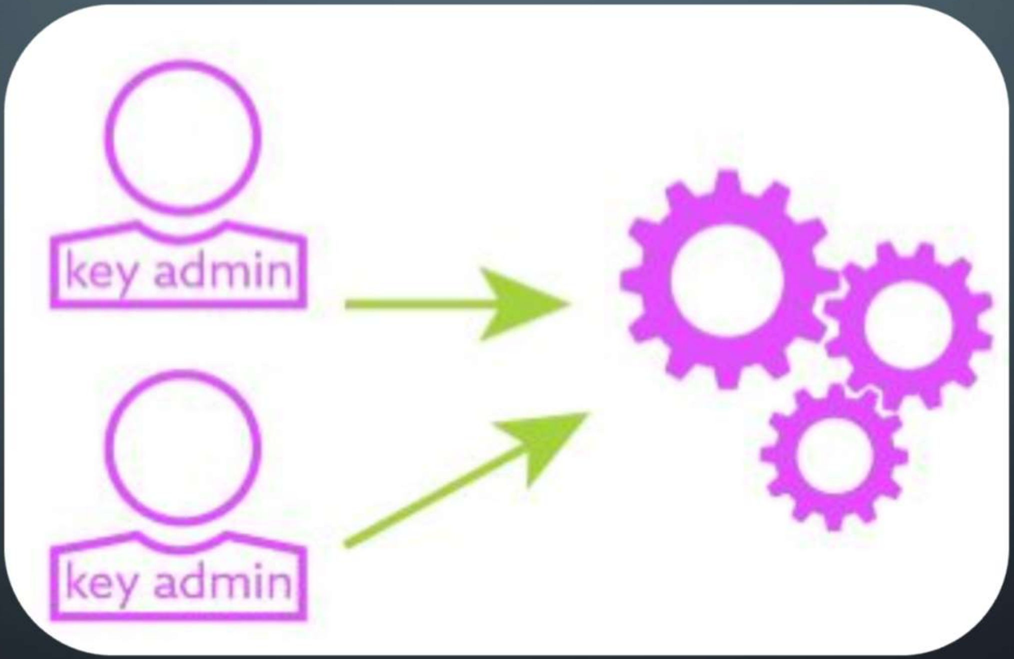


(1) Passwords are stored split between two servers: **Compromising one server does not expose the password**

(2) Random number is regularly refreshed to **reduce the windows of time for a successful attack on both servers**

(3) During authentication, claimed passwords are **verified without exposing the legitimate password**

DUAL CONTROL



Requirement

13

Section

Annex B

Type

Addition

PCI PIN 3.0 Description

- Added sunset dates for allowed usage of PCs to load clear- text secret and/or private keys and/or their components where they exist in unprotected memory outside the secure boundary of an SCD. Specifically:

1. Effective 1 January 2021, entities engaged in key loading on behalf of others shall not be allowed to use PC-based key-loading methodologies where clear-text secret and/or private keying material appears in the clear in unprotected memory outside the secure boundary of an SCD.
2. Effective 1 January 2023, entities only performing key loading for devices for which they are the processor shall no longer have this option.

Requirement	Section	Type
13-2	TPO Annex B	Modification

PCI PIN 3.0 Description

- Keyboards attached to an HSM shall never be used for the loading of cleartext secret or private keys or their components.

Requirement	Section	Type
15-1	Annex B	Addition

PCI PIN 3.0 Description

- Added the optional key check value method for TDEA keys, but it is mandatory for AES keys.

Note: Check values are computed by encrypting an all-zero block using the key or component as the encryption key, using the leftmost n-bits of the result where n is at most 24 bits (6 hexadecimal digits/3 bytes). Either this method must be used for TDEA or TDEA must use, and AES shall use a technique where the KCV is calculated by MACing an all-zero block using the CMAC algorithm as specified in ISO 9797-1 (see also NIST SP 800-38B). The check value will be the leftmost n-bits of the result, where n is at most 40 bits (10 hexadecimal digits). The block cipher used in the CMAC function is the same as the block cipher of the key itself. A TDEA key or a component of a TDEA key will be MACed using the TDEA block cipher, while a 128-bit AES key or component will be MACed using the AES-128 block cipher.

Requirement
18-3

Section
TPO
Annex B

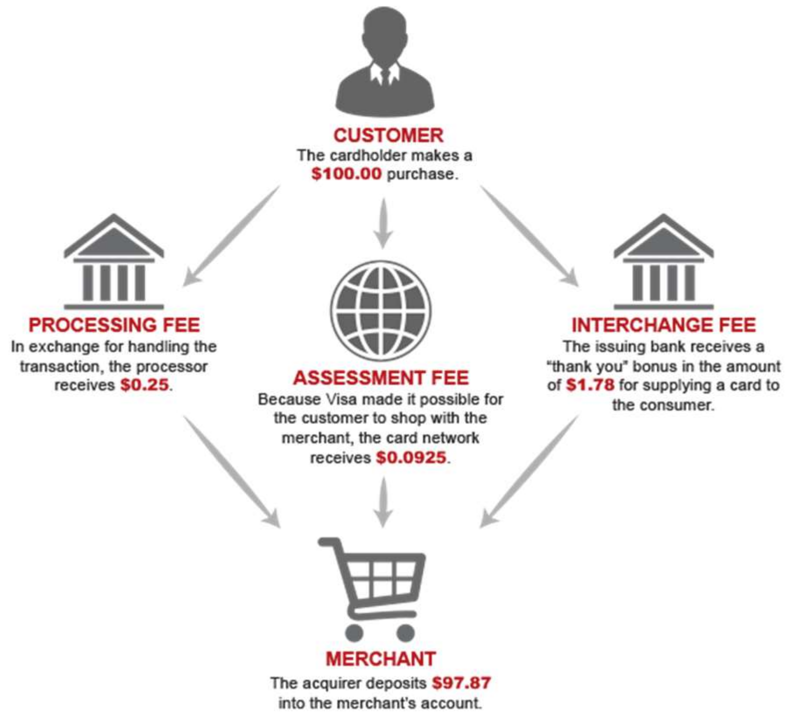
Type
Modification

PCI PIN 3.0 Description

- The dates for managing encrypted symmetric keys as key b locks have been modified, and the new dates are now divided into three phases. The phased implementation dates are as follows:

1. Phase 1 – Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to hardware security modules (HSM). Effective date: June 1st, 2019.
2. Phase 2 – Implement Key Blocks for external connections to Associations and Networks. Effective date: June 1st, 2021.
3. Phase 3 – Implement Key Blocks to extend to all merchant hosts point-of sale (POS) devices and ATMs. Effective date: 1 June 2023.

MERCHANT ACQUIRER, TRANSACTIONS BEING PROCESSED



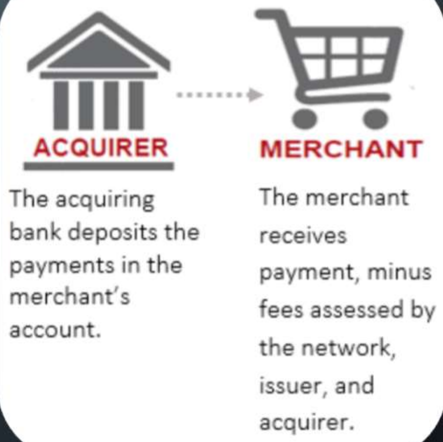
CUSTOMER
The cardholder makes a $100.00 purchase.

PROCESSING FEE
In exchange for handling the transaction, the processor receives $0.25.

ASSESSMENT FEE
Because Visa made it possible for the customer to shop with the merchant, the card network receives $0.0925.

INTERCHANGE FEE
The issuing bank receives a "thank you" bonus in the amount of $1.78 for supplying a card to the consumer.

MERCHANT
The acquirer deposits $97.87 into the merchant's account.



ACQUIRER
The acquiring bank deposits the payments in the merchant's account.

MERCHANT
The merchant receives payment, minus fees assessed by the network, issuer, and acquirer.

Requirement
25-2

Section
Annex A

Type
Clarification

PCI PIN 3.0 Description

- Clarified that individual user IDs may be assigned to a role or group.
- All user access to material that can be used to construct secret and private keys (such as key components or key shares used to reconstitute a key) must be directly attributable to an Individual user for example, through the use of unique IDs.

Note: individual user IDs may be assigned to a role or group.