Security Standards Council®

Standard: PIN Security–Requirements and Testing Procedures

Version: 3.1

Date: August 2021

Author: PCI Security Standards Council

Information Supplement: Implementing ISO Format 4 PIN Blocks

Document Changes

Date	Version	Description	Pages
August 2021	1.0	Initial Publication.	All
September 2021	1.01	Minor errata fixes	Cover, 8, 14

Table of Contents

Executive Summary

The effective dates for supporting ISO Format 4 PIN blocks that were previously communicated in v3.0 of the PCI PIN Security Requirements and Testing Procedures have been suspended at this time.

PCI SSC encourages all parties to continue their migration efforts to support ISO Format 4 PIN blocks. This Information Supplement provides guidance on the planning, migration, and testing of the implementation of ISO Format 4 PIN blocks.

Implementation of ISO Format 4 PIN blocks is a necessary step in the preparation for the payment card ecosystem to support a future migration to the Advanced Encryption Standard (AES).

1 Introduction

1.1 Intended Audience

This information supplement guides entities who are implementing ISO Format 4 PIN blocks. The reader is assumed to have access to and familiarity with the *PCI PIN Security—Requirements and Testing Procedures* document (PCI PIN Standard), a copy of which is available here. For other important sources of information, refer to *Reference Materials*.

1.2 Scope

The scope of this document is to provide guidance on the implementation of ISO Format 4 PIN blocks in conformance to requirements in the PCI PIN Standard. Notwithstanding, this document contains information that may be useful in migrating to the Advanced Encryption Standard (AES).

1.3 Structure and Content

This document answers the following questions:

- What are PIN blocks?
- What is the ISO Format 4 PIN block?
- Why is migrating to the ISO Format 4 PIN block important?
- What should be considered in a migration plan?
- What reference materials are available to help with the migration?

1.4 Glossary

The Glossary in the *PIN Security—Requirements and Testing Procedures* document is the definitive reference for most terms used in this supplement. However, the following glossary is provided for additional terms used in this document.

Term	Definition
BDK	Base Deviation Key
Fixed Key	Fixed key is a key management method whereby the fixed transaction key is either physically loaded or remotely loaded using asymmetric techniques. The fixed transaction key is used for transaction processing until a new key is similarly loaded. Note that "Fixed Key" is not the same as Master Key/Session Key.[1]
HSM	Hardware Security Module is a secure cryptographic device (SCD) used in the management of cryptographic keys.
JSON	JavaScript Object Notation is a lightweight data-interchange format.
LMK	Local Master Key is another term for Master Key; see MFK.
MFK	Master File Key: in a hierarchy of Key Encrypting Keys and Transaction Keys, the highest level of Key Encrypting Key is known as a Master Key or Master File Key.
PEK	PIN Encrypting Key
SDLC	Software Development Life Cycle
TMK	Terminal Master Key
XFS	Extensions for financial services: this provides a client-server architecture for financial applications on the Microsoft Windows platform.
XML	Extensible Markup Language

2 What Are PIN Blocks?

2.1 PIN Management

A Personal Identification Number (PIN), as used in the payment card industry, is a 4-to-6 digit[2] number used by a cardholder to authenticate that the person presenting a payment card is authorized to use the card. Although the payment ecosystem supports various cardholder verification methods, the cardholder method most commonly used is the PIN.

Several technical and procedural controls are required to ensure PIN security from the time that a cardholder enters the PIN at a payment-acceptance terminal to the time that the issuer, or their agent, verifies the PIN is correct. The objective of PIN management is to protect the PIN against unauthorized disclosure, compromise, and misuse throughout its life cycle and, in so doing, to minimize the risk of fraud occurring within the payment card ecosystem. The secrecy of the PIN is to

[1] A technical FAQ on Fixed [Transaction] Key vs. Master Key/Session Key will be available for further clarification.
[2] While ISO standards permit this to be up to 12 digits, most implementations do not support more than 4-to-6 digits.

be maintained at all times during its life cycle, which consists of its establishment, issuance, activation, storage, entry, transmission, validation, deactivation, and any other use made of it.[3]

PIN block use is a fundamental security element for securing the PIN.

[3] ISO 9564-1

2.2 PIN Blocks

Cryptography protects a PIN for most of its life cycle. Per *ISO 9564-1*, "the adopted encipherment procedure shall ensure that the encipherment of a plaintext PIN value using a particular cryptographic key does not predictably produce the same enciphered value when the same PIN value is associated with different accounts." To facilitate such encipherment, the PIN is formatted into a PIN block.

According to the ISO standard, PIN blocks come in five formats, as described in the following table.

Format	Description
0	This PIN block is constructed by modulo-2 addition of two 64-bit fields: the plain text PIN field and the account number field.
1	This PIN block is constructed by concatenation of two fields: the plain text PIN field and the transaction field.
2	The format 2 PIN block has been specified for use with IC cards. The format 2 PIN block shall be used only in an offline environment and shall not be used for online PIN verification. This PIN block is constructed by concatenation of two fields: the plain text PIN field and the filler field.
3	The format 3 PIN block is the same as format 0 PIN block, except for the fill digits.
4	Format 4, an extended PIN block format, is constructed using two 128-bit fields of PIN and PAN data, respectively. This format supports the use of a 128-bit block cipher (AES).

3 What is ISO Format 4 PIN Block?

The ISO Format 4 PIN block is a new PIN block format for supporting AES. It combines the PIN with the PAN by formatting each to a consistent length, and then encrypting them. *Figure 3.1* depicts the plaintext PIN field. *Figure 3.2* depicts the plaintext PAN field.

Figure 3.1 ISO Format 4 PIN Block – plaintext PIN Field

Bit 1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F
65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R

where:

C=Control field:	4-bit field value 0100 (4);
N=PIN length	4-bit binary number with permissible values of 0100 (4) to 1100 (12);
P=PIN digit	4-bit field with permissible values 0000;
P/F=PIN/Fill digit	Designation of these fields is determined by the PIN length field;
F=Fill digit	4-bit field value 1010 (A);
R=Random digit	4-bit field with a randomly selected value in the range 0000 (0) to 1111 (15).

Figure 3.2 ISO Format 4 PIN Block – Plain Text PAN Field

Bit 1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
M	A	A	A	A	A	A	A	A	A	A	A	A	A/0	A/0	A/0
65	**69**	**73**	**77**	**81**	**85**	**89**	**93**	**97**	**101**	**105**	**109**	**113**	**117**	**121**	**125**
A/0	A/0	A/0	A/0	0	0	0	0	0	0	0	0	0	0	0	0

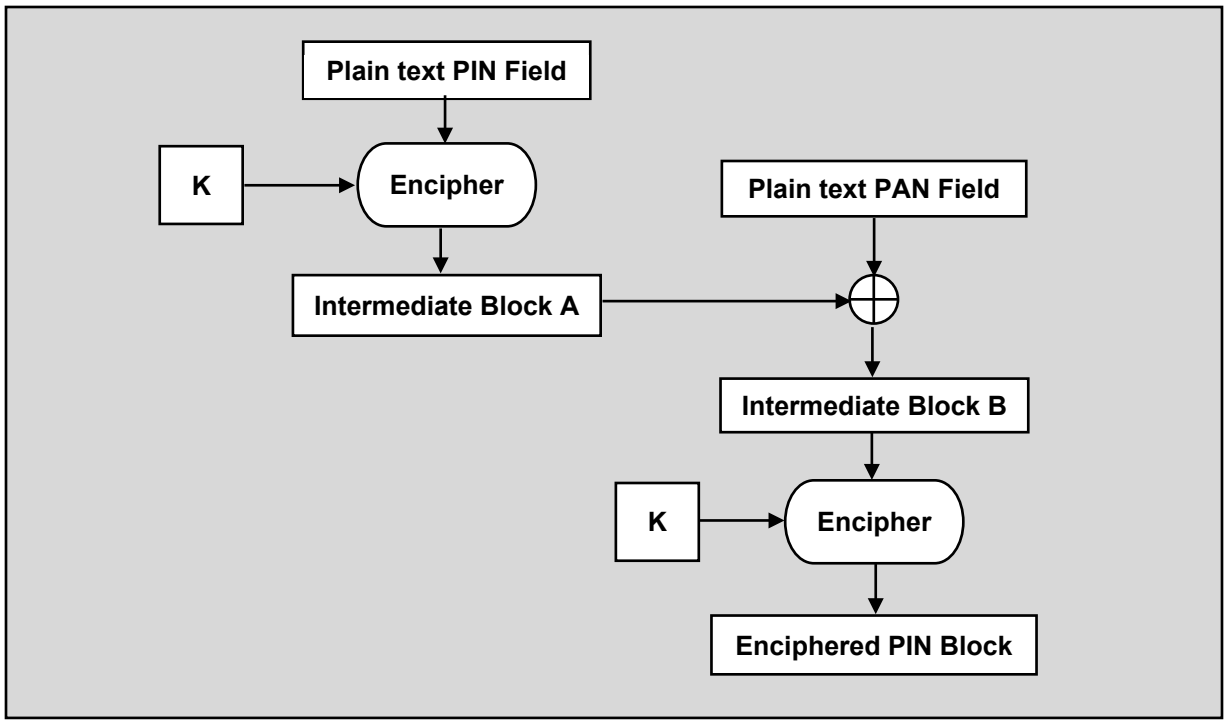
where:

M=Control field:	4-bit field with permissible values 0000 (zero) to 0111 (7) indicate a PAN length of 12 plus the value of the field (ranging then from 12 to 19). If the PAN is less than 12 digits, the digits are right justified and padded to the left with zeros, and M is set to 0;
A=PAN digit	4-bit field with permissible values of 0000 (0) to 1001 (9);
0=Pad digit	4-bit field with the only permissible value 0000 (zero);
A/0=PAN/Pad digit:	Designation of these fields is determined by the PAN length field;

Note: For Format 4, the PAN is required for PIN encipherment. For devices where the PAN is captured separately from the SCD where the PIN is entered, the PAN is to be transmitted to that SCD prior to the encipherment of the PIN.

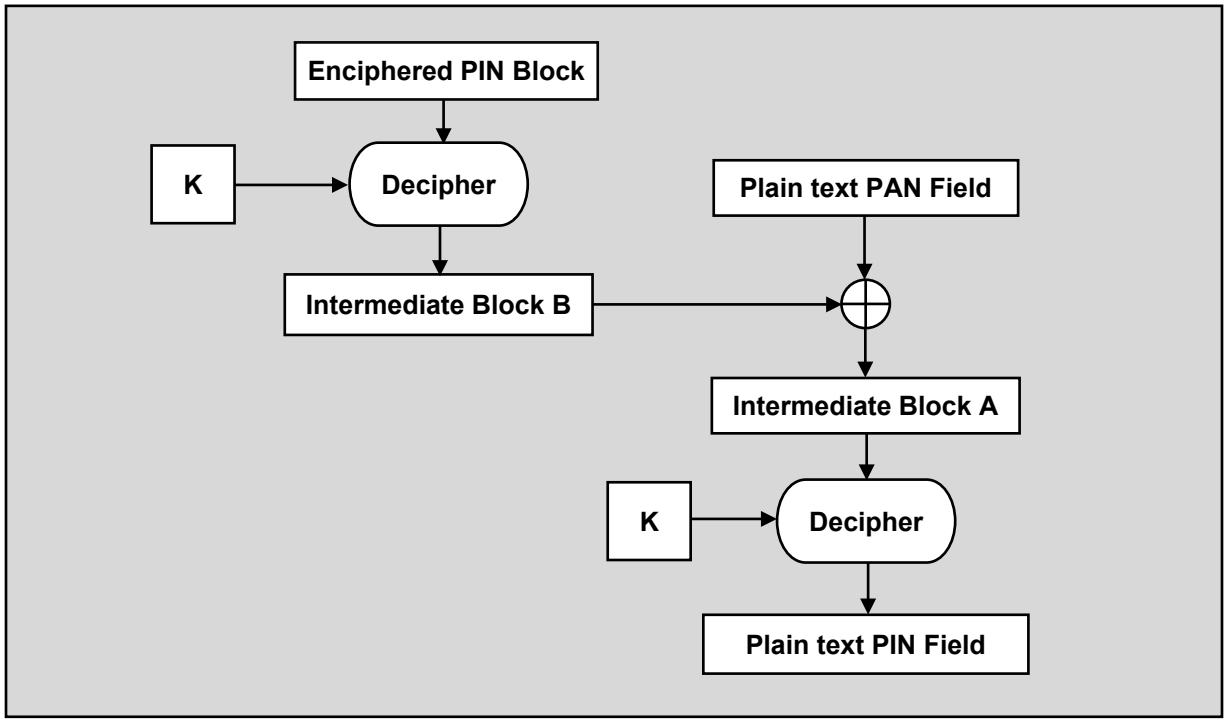
Figure 3.3 describes the process of combining the PIN field and the PAN field to produce the Format 4 PIN block.

Figure 3.3 ISO Format 4 PIN Block - Format 4 Encipherment



The process in *Figure 3.4* shows how an enciphered PIN block is decrypted. *ISO 9564-1* (§ 9) requires that both processes — the process creating the PIN block and the process deciphering the PIN block — occur within a secure cryptographic device (SCD).

Figure 3.4 ISO Format 4 PIN Block – Format 4 Decipherment



Because ISO Format 4 is the only format that supports AES, it may be necessary to convert to or from another format as part of a migration strategy. *Figure 3.5* shows which format translations are permitted. Cases shaded in gray indicate that the translation is allowed only in specific circumstances. In general, using Format 3-to-Format 4 or Format 4-to-Format 3 will accommodate TDEA usage.

Figure 3.5 ISO Format 4 PIN Block – PIN Block Format Translation Restrictions

Translate from	Translate to			
	Format 0	**Format 1**	**Format 2**	**Format 3 & 4**
Format 0	• Permitted anywhere without change of PAN • Change of PAN only permitted in sensitive state for card issuance • Change of PAN Token to real PAN permitted with cryptographic binding of PAN Token to real PAN.	Not Permitted	Permitted for submission to an IC card	Permitted
Format 1	Permitted	Permitted	Permitted for submission to an IC card	Permitted
Format 2	Not Permitted	Not Permitted	Permitted for submission to an IC card	Not Permitted
Format 3	• Permitted anywhere without change of PAN • Change of PAN only permitted in sensitive state for card issuance • Change of PAN Token to real PAN permitted with cryptographic binding of PAN Token to real PAN.	Not Permitted	Permitted for submission to an IC card	Permitted

***Note**: All PIN translations from one ISO format to another, where permitted (refer to Figure 3.5), are done within an SCD (usually a Host Security Module (HSM)).*

The PCI PIN Security Standard requires all cryptographic PIN key translations (plaintext PIN to enciphered PIN, enciphered PIN under one key to enciphered PIN under another key, and enciphered PIN to plaintext PIN) to occur within an SCD (Requirement 1).

4 Are There PCI Dates for ISO Format 4 PIN Blocks?

PCI PIN Security Requirements and Testing Procedures v3.1, published March 2021, suspends the sunrise dates for ISO Format 4 PIN blocks, which were originally in *PCI PIN Security Requirements and Testing Procedures v3.0*, published August 2018. The sunrise dates were for support of the new PIN block format (ISO Format 4) and not a requirement for its use.

Due to the nature of TDEA-to-AES migration and its effect across the payment ecosystem, PCI SSC is re-evaluating these dates. Revised effective dates will be communicated at a later time.

PCI SSC encourages all parties to continue their migration efforts to support ISO Format 4 PIN blocks and to contact the payment brands for additional information: *FAQ 1142. How do I contact the payment card brands?*

Although the dates were suspended, organizations may choose to implement ISO Format 4 PIN block with POI devices that support ISO Format 4 PIN block now. Online PIN acceptance devices approved to POI v5 and higher are required to support ISO Format 4 PIN block. Older POI devices may support ISO Format 4 PIN block format if the POI vendor has updated the firmware. This does not mean that the POI devices need to have AES PIN Encrypting Keys (PEKs) installed; however, organizations need to have implemented an AES MFK/LMK before implementing the processing of AES PIN Block Format 4 for POI, and it is prudent to implement an AES master key, such as AES 256, or the largest key size/strength supported.

Note: *This applies to organizations that directly drive the terminal devices. They may implement ISO Format 4 at any time (for devices that can support it), and continue to support TDEA (e.g., ISO Format 0 or 3). If they also implement AES PEKs, they can phase out TDEA support for the devices they drive, and translate at the HSM from Format 4 (AES) to Format 3 (TDEA) for outbound-to-processor/acquirer or brand until the processor/acquirer or brand can support Format 4.*

5 Why are PIN Blocks Essential?

Because PINs typically consist of only four to six digits, it would be easy for an attacker to create a table of PIN cryptograms under a given, but unknown, key where the attacker would only require access to the encrypted messages and the ability to test different PINs. When the attacker sees a future encrypted PIN, a simple table lookup would reveal the plaintext PIN. Furthermore, an attacker who obtains several examples of encrypted PINs, where the PIN was known, would have sufficient data for a known-plaintext attack against the underlying key. ISO standard PIN block formats 0, 1[4], 3 and 4 prevent both of these problems. Refer to *Figure 3.5*.

Some PIN block formats have the potential to prevent constructive reuse, such as a replay attack. Constructive reuse is when a cryptogram can be resubmitted and approved even though the perpetrator does not know or have access to the underlying cryptographic key. Format 4, for example, has a portion of the PIN field that contains random bits, which allow each block to be unique except by chance. If the receiving entity has controls in place to detect a repeated block and reject it, that entity can thwart constructive reuse.

6 Why is Migration to ISO Format 4 PIN Block Important?

The industry currently relies on TDEA, also known as TDES. This algorithm is based on the original Data Encryption Algorithm (DEA, also known as DES), which dates back to the mid-1970s when first introduced for standardization. Both NIST (FIPS 46 [1977]) and ANSI (X3.92 [1980]) standards codified DEA. However, with improvements in computer technology, by the 1990s, it was clear that DEA relied on a key length that was too short and that cryptanalytic weaknesses had been discovered. Efforts were made to find a replacement.

[4] If implemented using random values for padding, Format 1 can prevent an exhaustive attack; however, it otherwise leaks bits of information making it potentially weaker than 0, 3 or 4.

In 1997, DES was publicly broken for the first time; however, rapid improvements followed with faster and more cost-effective attacks. In 1998, *ANS X9.52, Triple Data Encryption Algorithm Modes of Operation* was published, effectively extending the life of DEA by introducing a way to use double- and triple-length keys. In 1999, NIST followed suit by publishing *FIPS 46-3* to standardize Triple DES (TDES/TDEA).

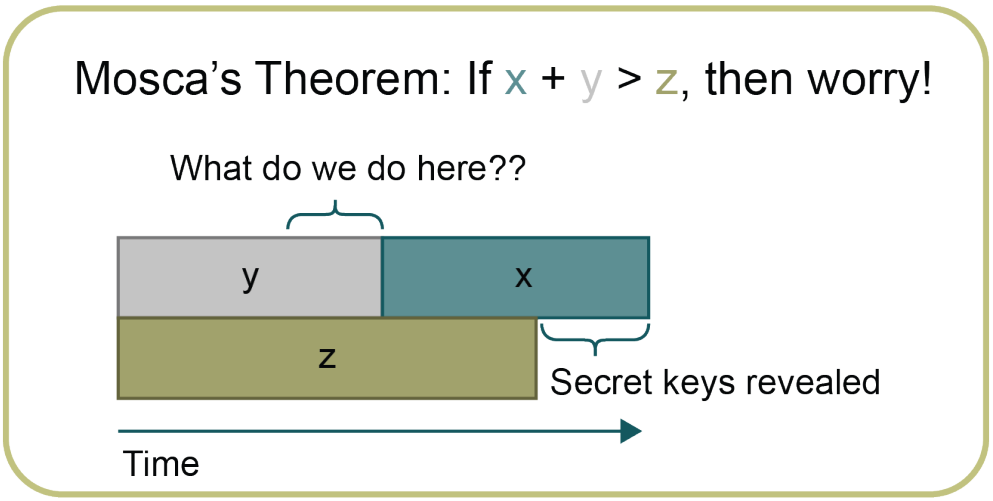
Recognizing that TDEA was a short-term extension for the life of DEA, a formal search began for a replacement algorithm. NIST published the *Advanced Encryption Standard (FIPS 197)* in 2001. In 2005, NIST withdrew *FIPS 46-3* and in 2008, ANSI withdrew *X9.52*. TDEA became a legacy algorithm.[5] *Advanced Encryption Standard* (AES) became the new standard.

ISO Format 4 is the only ISO format that supports AES. With NIST's deprecation[6] of TDEA and the pressure of Mosca's Theorem, the need to support AES is clear. Mosca's Theorem, as shown in *Figure 6.1*, states X + Y < Z, where:

- X is the amount of time that data has to be protected.
- Y is the amount of time it will take to migrate to a stronger algorithm.
- Z is when the current algorithm breaks or can be cost-effectively solved, such as by post-quantum cryptography.

ISO Format 4 support is an essential step in migrating to AES for PIN security.

Figure 6.1



For more information on the security risks associated with symmetric and asymmetric algorithms, refer to *NIST SP 800-57 Part 1, Rev. 5*, especially Table 2 and Table 4. Figure 2 in the NIST publication provides an example similar to Mosca's Theorem.

[5] Per *NIST SP 800-57 Part 1, Rev. 5*, 3-key TDEA was deprecated through 2023 and disallowed thereafter. Refer also to Table 1 of *NIST SP 800-131A Rev. 2*.

[6] NIST defines "deprecated" as "… the algorithm and key length may be used, but the user must accept some security risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection." "Disallowed means that the algorithm or key length is no longer allowed for applying cryptographic protection." [*NIST SP 800-131A rev. 2*]

7 Migration Planning

Migration planning includes many steps and always needs to be tailored to specific environments and circumstances. This section describes activities that are common in migrations. It is intended to assist the reader in developing migration planning materials for the reader's organization.

Note: *Migration planning should include internal discussions with stakeholders who may have related projects on the drawing board, for examples migration of ISO 8583 messages to ISO 20022 messages (ATICA)[7], migration of proprietary key blocks to ISO 20038 or X9.24 or X9 TR-31, discontinuance of TDEA fixed keys, or acquisition of new devices/SCD or payment software.*

7.1 Identification and Inventory

7.1.1. *What Cryptographic Keys Are You Using?*

Identifying the cryptographic keys your organization uses for PIN protection is an essential first step. This inventory includes:

- Keys used directly in the creation of the PIN block (e.g., PEK).
- Keys used to protect the PEK in storage or in transit.
- Keys used to generate or manage these keys.

This includes manual processes, such as the use of cryptographic key components or key shares (n-of-m secret-sharing schemes).

7.1.2. *What Devices (POI, HSM, or Other SCD) Participate in the PIN Process?*

An inventory of devices is essential to ensure that your equipment can support ISO Format 4 PIN blocks and the underlying AES algorithm. You may have equipment that:

- Is already ISO Format 4 PIN block ready,
- Can become ready with a firmware upgrade, or
- Will need to be replaced.

This inventory assists organizations to budget upgrades and replacements, and to schedule the phases of migration.

Note: *The inventory needs to include key-loading devices (if used).*

7.1.3. *What Transport Message Standards are You Supporting?*

ISO 8583-1[8] is an international standard for financial transaction card originated interchange messaging. The defined field for the transport of an ISO-formatted PIN block in earlier versions was Field 52, which is only 64-bits long. The current version is now a series of ISO 8583-n. ISO 13492 provides a method for using Field 52, Field 53, and Field 96 to accommodate TDEA; and Field110, Field 111, or Field 50 to accommodate AES.

[7] *ISO 13492:2019 Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption* augments ISO 8583-1 to include support for AES. Thus, if your organization has already implemented ISO 13492, it has a message mechanism for supporting AES. Notwithstanding, organizations should coordinate with any projects that potentially impact the acceptance or management of AES.

[8] Note that earlier versions of ISO 8583 (e.g., ISO 8583:1987 and ISO 8583:1993) may still be in use although they were formally withdrawn.

A new interchange message standard, *ISO 20022 Acquirer to Issuer Card Messages (ATICA)*, uses Extensible Markup Language (XML)/JavaScript Object Notation (JSON) format that supports variable length fields. This standard is self-documenting and uses tags to make the contents of the message easily decipherable. The migration to the ISO Format 4 PIN block should occur with your migration to *ISO 20022*, which is backwards compatible to *ISO 8583* for features/fields that *ISO 8583* supported, if such a migration is contemplated. Otherwise, planning should include ISO 13492 support.

7.1.4. *What Software Is Participating in the PIN Process?*

For some implementations, encrypted keys used for PIN processing might exist in a database. Although storing an encrypted PIN for longer than is required for initial authentication does not conform with our PIN Standard (§4-1), the storing of PIN (cleartext or encrypted) might exist. If it does, it is important to identify this issue and correct it.

Using software outside of an SCD to handle a plaintext PIN is also nonconforming[9]; however, using software to handle an encrypted PIN, especially in the appropriate ISO format, is common. Because older versions of commercial software and any proprietary software developed in-house or outsourced may require replacement or upgrading, it is important to identify and inventory all potentially impacted databases and application software.

7.1.5. *What Other Issues Can Impact the PIN Process?*

Consider the following:

- **Is equipment leased or owned?** When identifying equipment, such as POI and HSM devices, consider whether the equipment is leased or owned. This may impact who is responsible for maintenance, including software/firmware updates, and may also impact service contracts or licensing.
- **Does your organization use tokenization?** If it does, the token may be used as the PAN in the PIN block. Depending on your implementation, the syntax and format of the token might not mirror the format and syntax of the original PAN. Some ISO Format 4 PIN block implementations test for valid format and syntax, including Luhn checking and PAN length. To ensure interoperability, any token used in lieu of the PAN in the PIN block needs to preserve format and maintain syntax. Identifying whether your organization uses tokenization and how it impacts PIN processing is an important step.
- **Do you operate in multiple regions?** In multinational organizations, regional issues may require identifying and addressing differences in how PINs are processed. Organizations should work closely with acquirers, issuers, and brands to identify any jurisdiction-specific requirements.
- **Do you operate ATM/EPP devices?** For organizations that use or operate ATM or other EPP-embedded devices, there may be a dependency on the XFS platform/specifications, which is an intermediate layer between the ATM software application and the EPP. Usually, the XFS platform is maintained by the manufacturer, with whom you need to confirm AES support.
- **Do you support PIN change as a function (usually via ATM, for example)?** If you do, additional considerations may apply, depending on how this function is handled.

[9] Some PCI SSC standards make explicit exceptions within their respective realms, e.g., Software-based PIN Entry on COTS (SPOC); however, the PCI PIN Standard does not.

7.2 Prioritization

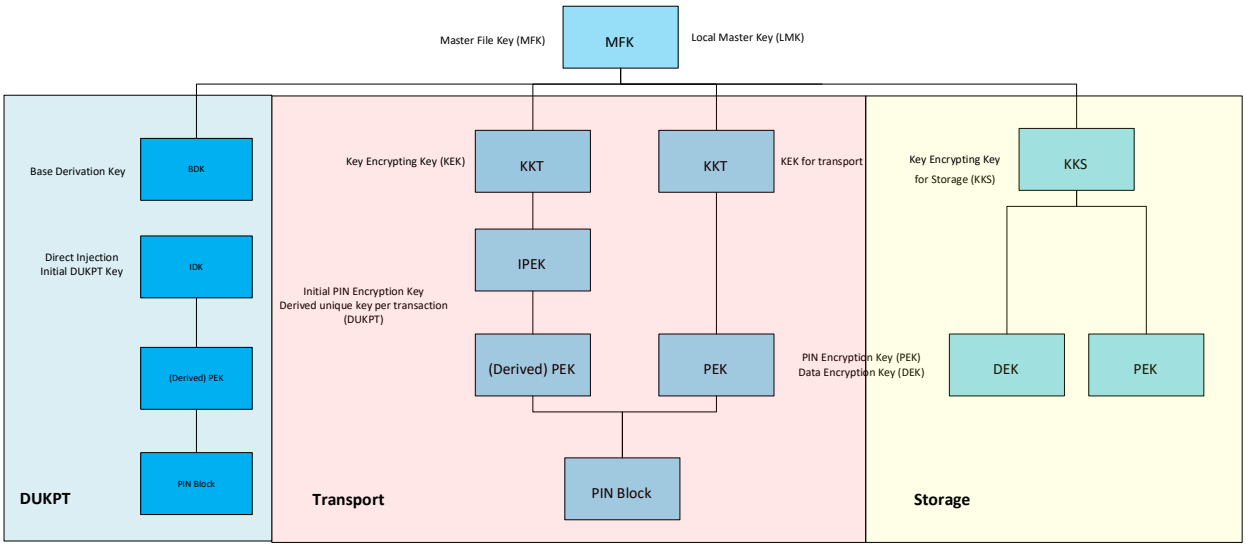
7.2.1. *In What Order Should Keys Change?*

The master file key (MFK), also known as a local master key (LMK), is the key under which other keys are protected. The MFK always required to be at least as cryptographically strong as the strongest key it protects. For example, if an enterprise plans to permit AES 256-bit key encrypting keys (KEK), , the MFK/LMK needs to be a 256-bit AES key.

Note: *Quantum computing using Grover's algorithm may[10] reduce the effectiveness of symmetric key algorithms by as much as half of its bit strength, depending on use case. For the longer term, the prudent course is to support AES 256, especially for MFK/LMK.*

Figure 7.1 shows a typical key hierarchy; your organization's key hierarchy may differ. This hierarchy is independent of the symmetric algorithm used. Both TDEA and AES keys can coexist under the same MFK. However, the MFK discussed above needs to be an AES key.

Figure 7.1



7.2.2. *Hierarchy and Description of Keys*

As shown in *Figure 7.1*, the protection of PIN blocks depends on a hierarchy of cryptographic keys:

- At the top is the MFK, also Local Master Key (LMK). The MFK protects subordinate keys, whether stored within the HSM or outside of the HSM as cryptograms in a database.
- KEKs are the next layer down. KEKs generally come in two types:
  - Keys that encrypt keys for transport (KKT)
  - Keys that encrypt keys for storage (KKS)

[10] This is not a near-term consideration; rather it supports planning for large-scale post quantum computing.

- In systems that use a derived unique key per transaction (DUKPT), a Base Derivation Key (BDK) is needed. This key is effectively at the same level in the hierarchy as the KEK, except that it does not encrypt anything else.
- For systems that do not use DUKPT, the PIN Encrypting Key (PEK) falls under the KEK (either KKT or KKS as appropriate).[11]
- For systems using DUKPT[12], the Initial DUKPT Key (IDK), historically referred to as an Initial PIN Encryption Key (IPEK) when used only for PIN, is next in the hierarchy. The IDK is a derived key created from the BDK, usually injected directly into the POI device. However, if remote rekeying is supported, it is sent under the KEK (KKT). Many other keys may exist and have some relevance to PIN protection or PIN verification (PVV). These might include:
  - Asymmetric keys (public key cryptography) used to authenticate device firmware.
  - Full public key infrastructures (PKI) with certificate authorities (CA), root and subordinate CAs.
  - Public/private keys involved in establishing secure sessions, transporting symmetric keys, or protecting stored symmetric keys.

While none of these keys directly relates to ISO Format 4 PIN blocks, requirements to protect AES keys may impact the appropriate asymmetric algorithms and key lengths. *Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms* is the authoritative reference within the *PCI PIN Security Standard*.

Because the process for generating PIN values and verifying PIN values (PIN Verification Value (PVV), PIN Offsets, or Issuer PIN verification) are proprietary, it is beyond the scope of this Information Supplement. However, the algorithms used in these methods may include cryptographic algorithms whose keys fall within the cryptographic key hierarchy of your organization, especially if your organization issues payment cards or acts as a stand-in for the verification of PIN.

As previously noted, other cryptography-related efforts, such as discontinuing use of fixed keys for TDEA and migrating to cryptographic key blocks (also known as key wrapping), affect additional keys, such as Message Authentication Keys (MAC or HMAC), which are not shown in *Figure 7.1*. Such keys may warrant inclusion in the identification and inventory process.

7.3 Plan Migrations, Including Rollback/Recovery Options

When feasible in your environment, the safest approach may be to offload ISO Format 4 PIN block processing to some bridging solution, keep legacy systems in place, and translate to and from ISO Format 4 PIN block for the legacy systems internally. This approach allows you to handle ISO Format 4 PIN blocks as you phase out legacy systems.

7.3.1. *Identification of Migration Systems*

To identify migrations systems:

1. Categorize devices based on existing capability to do ISO Format 4:
   - For devices capable of ISO Format 4, confirm the steps necessary to make this active.

[11] Historically, cleartext key injection was used for PIN encryption keys. Modern practice is only to inject encrypted key protected either under a KEK or using asymmetric cryptography.
[12] Refer to X9.24-3 for more information on DUKPT.

  - For devices not capable of ISO Format 4, develop a replacement or upgrade strategy.

2. For HSMs, confirm the ability to support AES master file key (MFK), also known as LMK.
   - If the HSM can support an AES MFK, include planning for generation and implementation of the AES MFK.
   - If the HSM cannot support an AES MFK, develop a replacement or upgrade strategy. When complete, include planning for generating and implementing the AES MFK, which may include manual key procedures, such as the use of key components or key shares.
3. Identify any third parties used for key generation, key injection, or key use:
   - Confirm each third party's capability to support ISO Format 4 PIN blocks.
   - For any third parties that cannot support ISO Format 4 PIN blocks at this time, determine with them their strategy and timeline for supporting ISO Format 4 PIN blocks. Your organization may have to support translation from ISO Format 4 PIN blocks to, for example, ISO Format 0 or 3 PIN blocks until the third parties are capable of accepting the required ISO Format 4 PIN block.

7.3.2. *Updating the Host Systems*

- Determine minimum hardware/software requirements. Some older (pre-millennial) HSMs may not be able to apply AES (non-firmware/software).[13]
- Does the HSM have firmware to support ISO Format 4 PIN blocks?
  - Commercial package to support it.
    - General purpose HSM vs. Payment HSM:
      - Payment HSM would be more likely to have native capability.
      - General purpose HSM might not conduct all operations within the cryptographic boundaries (which would make it nonconforming for PIN-based transactions).
    - Review design documentation provided by vendor.
  - If customized firmware is used on the HSM, for example to accommodate cryptographic algorithms or protocols not originally native to the HSM, the firmware should be reviewed to ensure that it 1) does not invalidate the HSM's certification (FIPS or PCI PTS HSM) and 2) supports AES; that is, it does not prevent the use of ISO Format 4 PIN blocks.
- Conduct all cryptographic functions within an SCD/HSM. Cryptographic functions include but are not limited to key generation, MACing, encryption, decryption, and key translation.

7.3.3. *Updating the Terminal Systems*

- Determine minimum hardware/software requirements:
  - Schedule a device for future replacement if it cannot perform ISO Format 4 PIN blocks.

[13] Some modern HSM vendors may charge a fee for the AES support feature which may mean that the existing implementation may require an upgrade despite the HSM models ability to become AES capable.

- POI terminals approved prior to PCI PTS POI v5 (released in 2016) may not have support for Format 4 PIN blocks. Vendors may have already added support for AES.
- Coordinate with the vendor or device provider.

7.4 Implement in Phases

- Identify initial implementation platforms, hardware, and software.
- Prerequisites for implementation:
  - Update software
  - Update existing keys (if appropriate)
- HSM to HSM followed by POI to HSM, HSM to POI:
  - Consider a POI→HSM→HSM (simulate transaction acceptance by acquirer).
  - If an acquirer/processor is not ISO Format 4 PIN block ready, ISO Format 4 PIN blocks have to be translated to a supported format, for example, ISO Format 0 or 3 PIN blocks within the HSM prior to sending the PIN block to the acquirer/processor.
- Recommend limited initial implementation (to test) on test devices where available.
- Key injection of updated BDK/ Terminal Master Key (TMK), as applicable.
- Conduct tests on initial devices prior to widespread implementation.

7.5 Test

- Testing should be conducted prior to deployment as provided in *NIST SP 800-57* rev. 5.
- Standardize a test plan:
  - Elements:
    - Unit testing followed by Integration testing
    - Completed phase testing
    - Type of software development life cycle (SDLC) will impact how and when testing is conducted (Agile vs. Waterfall vs. DevOps)
    - Functionality: Can the device accept keys securely?
    - Key loading: Do key elements exist at any time outside the secure boundary of an SCD?
    - Documentation of test plan
    - Success criteria for key loading and producing a PIN block
    - Test plan and result acceptance approval by authorized individuals
    - Test plan results
    - Remediation plan
    - Retesting
    - Roll-back plan
  - Scheduling
  - Budgeting

7.6 Go Live in Phases

Strategy for rolling out POI devices with new keys based on technology and business considerations:

- Age of devices (synchronize to coincide with refresh of devices)
- Possibly implement a limited number of devices at a single location until it is established that the roll-out is stable.

7.7 Assessments

Following initial implementation, assess the changes to ensure conformance with applicable PCI PIN requirements. This section highlights the elements specific to ISO Format 4 PIN blocks for which assessors should pay particular attention. A citation in braces {} denotes the requirement in the *PIN Security Standard*.

- Type of key (algorithm) and key sizes used to encrypt PIN blocks. {2-3}
- Online PINs must be encrypted using an algorithm and key size that is specified in *ISO 9564*. {2-3}
  - TDEA using the electronic code book (TECB) mode of operation
  - AES, as described in *ISO 18033-3*
- All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the *EMV IC Card Specifications for Payment Systems* and *ISO 9564*. {2-4}
  - Implementation of ISO Format 4 PIN blocks should not affect the enciphering of PIN blocks between the PIN entry device and the IC reader. Any diagnostic/debug/test PIN block transmission mechanisms used during the implementation process are to be disabled.
- PINs enciphered only for transmission between the PIN entry device and the IC reader must use one of the PIN block formats specified in *ISO 9564*. {3-2}
- Standard PIN-block formats (ISO formats 0, 1, 2, 3, and 4) shall not be translated into non-standard PIN-block formats. {3-3}
  - Implementing ISO Format 4 PIN blocks should not permit any PIN block formats beyond those specified. Any diagnostic/debug/test formatted PIN block translation mechanisms used during the implementation process are to be disabled.
- PINs enciphered using ISO Format 0, ISO Format 3, or ISO Format 4 must not be translated into any other PIN-block format other than ISO format 0, 3, or 4, except when translated to ISO Format 2. {3-3}
  - Implementing ISO Format 4 PIN blocks should not include the translation of ISO Format 2 PIN blocks to ISO Format 4 PIN blocks.
- Translations between PIN-block formats that both include the PAN shall not support a change in the PAN. {3-3}[14]
  - Implementing ISO Format 4 PIN blocks should not use any mechanism by which the PAN is changed during any translation to Format 4.

[14] This translation restriction does not apply to surrogate PANs used in tokenization implementations.

- PIN blocks, even when encrypted, must not be retained in transaction journals or logs. {4-1}
  - Implementing ISO Format 4 PIN blocks should not permit the retention of PIN blocks in journals or logs, even where encrypted. Any diagnostic/debug/test modes used during the implementation that provide retention of PIN blocks in journals or logs should be disabled.
- PIN blocks are required in messages sent for authorization, but must not be retained for any subsequent verification of the transaction. {4-1}
  - Implementing ISO Format 4 PIN blocks should not permit the retention of PIN blocks for any subsequent verification of the transaction. Any diagnostic/debug/test modes used during the implementation that provide retention of PIN blocks should be disabled.
- Transaction PINs shall exist only for the duration of a single transaction (the time between PIN entry and verification; that is, store and forward). {4-1}
  - Implementing ISO Format 4 PIN blocks should allow the existence of transaction PINs only for the duration of a single transaction. Any diagnostic/debug/test mechanism used during the implementation that instantiates the existence of a transaction PIN time between the PIN entry and verification should be disabled.

8 Frequently Asked Questions

The questions and answers in this section cover a broader range of topics that may affect your organization's planning and implementation of ISO Format 4 PIN blocks or provide clarification of how other PIN requirements may fit into a larger strategy.

8.1 Are PIN Blocks and Key Blocks the Same Thing?

Answer: No. Key blocks protect keys while PIN blocks protect PINs. Their respective formats and methods of creation are different. For more information on Key blocks, refer to Information Supplement: Cryptographic Key Blocks.

8.2 After What Date Is Fixed key for TDEA PIN Encryption Disallowed?

Answer: 1 January 2023; however, fixed key for AES PIN encryption is unaffected.

9 Reference Materials

The following materials may provide additional information to assist organizations in planning, implementing, and testing their migration to ISO Format 4 PIN blocks and to AES more generally.

9.1 International Standards

- I*SO 9564 Financial services - Personal Identification Number (PIN) management and security* — [all parts]
- *ISO 11568 Banking - Key management (retail)* — [all parts]
- *ISO 13491 Financial services - Secure cryptographic devices (retail)* [all parts]
- *ISO/NP TR 14742 - Financial services - Recommendations on cryptographic algorithms and their use*

9.2 National Standards

- *ANSI X9.24-3-2017 Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction*
- *NIST Special Publication (SP) 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths*
- *NIST Special Publication 800-57 Part 1, Rev. 5 Recommendation for Key Management: Part 1 – General*

9.3 Other Publications

- *EMV Book 2, Integrated Circuit Card Specifications for Payment Systems Security and Key Management*
- ECRYPT: Algorithms, Key Size and Protocols Report (2018), 28 February 2018
- Guidelines on cryptographic algorithms usage and key management [EPC342-08 / Version 9.0 / 9 March 2020]
- J. Stapleton and R. Poore, "Cryptographic transitions," *2006 IEEE Region 5 Conference*, 2006, pp. 22-30, doi: 10.1109/TPSD.2006.5507465.
- R. Poore, “Cryptographic Transitions,” *Information Security Management Handbook*, Sixth Edition, Auerbach Publications, Boca Raton, 2007.
- Eli Biham, Lars R. Knudsen, “Cryptanalysis of the ANSI X9.52 CBCM mode,” *Advances in Cryptology – EUROCRYPT’98*, International Conference on the Theory and Applications of Cryptographic Techniques, pp 100-111.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.