Standard: PCI PIN Security Requirements

Date: July 2022

Author: PIN Assessment Working Group
PCI Security Standards Council

Information Supplement:

PIN Security Requirement 18-3 – Key Blocks

Document Changes

Date	Document Version	Description	Pages
June 2019	1.0	Initial release	All
July 2022	1.1	Updated dates and references	All

Table of Contents

Executive Summary

Per *PCI PIN Security Requirements,* Requirement 18-3, “Key Blocks,” encrypted symmetric keys must be managed in structures called Key Blocks. The key usage must be cryptographically bound to the key using accepted methods, such that it must be infeasible for the key to be used if the usage attributes have been altered.

The phased implementation dates are as follows:

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: **1 June 2019.**

Phase 2 – Implement Key Blocks for external connections to associations and networks. Estimated timeline for this phase is 24 months following Phase 1, or **1 January 2023.**

Phase 3 – Implement Key Blocks to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. Estimated timeline for this phase is 24 months following Phase 2, or **1 January 2025**.

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the Key Block, which includes the key itself - e.g., *ANSI X9.143*
- A digital signature computed over that same data - e.g., *ASC X9 TR 34*
- An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in *ANSI X9.102.*

References to Key-Block Protection Keys are specific to implementations using *ANSI X9.143: Retail Financial Services – Interoperable Secure Key Block Specification* and *ISO 20038: Banking and related financial services – Key wrap using AES.*

Note: ASC X9 TR 31: Interoperable Secure Key Exchange Key Block Specification has been classified as ‘historical’ by ANSI and X9.143 Retail Financial Services: Interoperable Secure Key Block Specification is the newer version. All references to TR-31 are being updated to X9.143.

1 Technical FAQs

1.1 Key Blocks

Q 1 Do Key Blocks apply to all symmetric keys?

A *Key Blocks must be used for all PIN security-relevant symmetric keys exchanged or stored under another symmetric key—for example, Zone Master Keys (ZMKs), Key-Encipherment Keys (KEKs), Base Derivation Keys (BDKs), Terminal Master Keys (TMKs), and PIN-Encryption Keys (PEKs). They may optionally be used as a best practice for account data security-relevant symmetric keys. Check with applicable payment brands to understand applicability of Key Blocks to symmetric keys used for non-PIN-related purposes.*

Q 2 Does phase 1 ("…internal connections and key storage with service provider environments…") apply to HSM connections on incoming transactions?

A *No. Incoming transactions from an external organization is Phase 2. Incoming transactions from POI devices is Phase 3. However, in Phase 1, service provider applications creating command strings to HSMs will need to account for the increased length of a Key Block as compared to legacy cryptograms.*

Q 3 What are Key Blocks and how do they work?

A *A Key Block contains a protected key, its usage constraints, and other data that is wrapped (encrypted) using a key-wrapping mechanism. Details of how Key Blocks work are described in ISO 20038: Banking and related financial services — Key wrap using AES and ANSI X9.143: Retail Financial Services – Interoperable Secure Key Block Specification.*

Q 4 Regarding the implementation dates, does that mean all previously established keys have to be changed, or that only from that point onwards newly exchanged keys must use Key Blocks?

A *All previously established keys can still be used. Key-Block Protection Keys (KBPKs) must be established for all connections sending keys after the implementation date. However, there is no expectation for existing Key-Encipherment Keys (KEK) to be reissued as KBPKs. An existing KEK can be converted to a KBPK if your HSM vendor has a method to accomplish this or you have the components or shares to recreate it as a KBPK.*

Q 5 In implementing Key Blocks, can existing Key-Encipherment Keys be converted to Key-Block Protection Keys?

A *Yes. KEKs may be converted to Key-Block Protection Keys through mechanisms provided by the HSM vendor.*

Q 6 How is the Key-Block Protection Key established with another organization or POI devices?

A *The KBPK effectively replaces the function of a KEK, and as such, it is to be established in the same manner as Key-Encipherment Keys—such as using manual mechanisms, asymmetric techniques, or via a key-injection mechanism—for example at a key-injection facility for POI devices.*

Q 7 How do Key Blocks affect (or relate to) the dates published in PCI PIN v3 regarding fixed key TDES and support for ISO PIN block format 4?

A *There isn't any relationship between fixed keys used for PIN-block encryption and Key-Encrypting Keys subject to the new Key-Block requirements. However, consideration should be given to coordination in any future changes. For example, migration to AES PIN blocks should be considered in line with the establishment of AES KBPKs for key exchange to utilize efficiencies for the organization and limit disruptions.*

Q 8 What PCI PTS POI versions support Key Blocks? And what phase requires Key-Block usage in PIN acceptance devices?

A *All POI PIN acceptance devices beginning with v2 in 2007 support ANSI X9.143 or equivalent. Implementation of Key Blocks in POS PIN acceptance devices and ATMs is required in Phase 3.*

Q 9 How will a PIN assessor determine compliance with the various Key-Block implementation phases?

A *The assessor shall examine (a) configuration settings on HSMs and commercial applications, and (b) design documentation for proprietary software—using techniques similar to determining the propriety of ISO PIN blocks. Additional guidance will be provided as part of PCI PIN Security Training.*

Q 10 What if my commercial processing software has not implemented support for Key Blocks by the required effective date?

A *Contact the payment brand(s) of interest at: https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands.*

Q 11 Are issuers required to exchange symmetric PIN keys in Key Blocks?

A *Yes. Issuers must be able to support Key Blocks for connections involving PIN-Encryption Key exchange with processors or switches (to be compliant with Phase 2 migration). Phase 1 and Phase 3 effective dates are intended primarily for PIN acquiring environments.*

Q 12 Why are issuers required to support Key Blocks for PIN keys when the PCI PIN Security Requirements (PSR) is intended for the acquiring domain?

A *Issuer support is required for interoperability purposes in order to receive PIN blocks for cardholder authentication by the issuer or its agent.*

Q 13 Do Key Blocks apply to issuer keys such as PVV, CVV, EMV personalization keys, etc.?

A *No. The scope of the PIN Security Requirements does not include issuer keys used for the purpose of cardholder authentication, whether for usage at the issuer, usage at or conveyance to an Issuer Processor or a Card Personalization vendor. However, it is recommended as a best practice.*

Q 14 Is it required for Key Blocks to be implemented to specify key usage directional flow between two organizations—for example, encrypt only or decrypt only?

A *No. The PIN Security Requirements are not that granular and the requirement for Key Blocks does not require organizations to change anything they currently do as far as mode of use. Specifically, Key-Block implementation as delineated in the PIN Security Requirements does not require that for transactions received, the key usage is defined as decrypt only, or for transactions sent, the key usage is defined as encrypt only. However, organizations should contact the entities they are exchanging keys with to understand if there are additional considerations regarding this setting.*

Q 15 When implementing Key Blocks, are there any Modes of Use options included in ANSI X9.143 that are not permitted for use?

A *No. The PIN Security Requirements do not include restrictions on the use of any of the available Modes of Use identified in ANSI X9.143.*

Q 16 Per Requirement 18-3: ***Encrypted symmetric keys must be managed in structures called Key Blocks. The key usage must be cryptographically bound to the key using accepted methods. Acceptable methods of implementing the integrity requirements include, but are not limited to:***

- ***A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the Key Block, which includes the key itself – e.g., ANSI X9.143***
- ***A digital signature computed over that same data - e.g., ASC X9 TR 34***
- ***An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.***

What is an example of an acceptable interoperable method?

A *ISO-20038 illustrates an acceptable interoperable standard.*

For all methods used, the encrypted key and its attributes in the Key Block shall have integrity protection such that they cannot be modified without detection. Modification includes, but is not limited to:

- *Changing or replacing any bit(s) in the attributes or encrypted key*
- *Interchanging any bits of the protected Key Block with bits from another part of the block*

Q 17 Where can an organization get environment-specific implementation details for its use?

A *Each organization differs regarding its processing, architecture, and services; therefore it is recommended to consult with your HSM vendors, application providers, internal architects, and the like to understand specific implementation requirements for your organization.*

Q 18 What are the considerations for HSMs?

A *HSMs must support Key Blocks, and entities should check with their HSM vendor(s).*

1.2 Additional Relevant Existing PIN Security Requirements Technical FAQs – PIN Security Requirement 18

Q December (update) 2016: When encrypted symmetric keys are managed in structures called Key Blocks, does this apply to both when the keys are transported and when stored?

A *Yes. It applies to the secure exchange of keys between two devices that share a symmetric Key-Exchange Key and for the storage of keys under a symmetric key. It is applicable to any time an encrypted key exists outside of an SCD.*

This applies for both fixed and master/session key scenarios. It does not apply to working keys for DUKPT or similar unique-key-per-transaction implementations where these keys are stored inside an SCD. However, it does apply to related keys such as Base Derivation Keys and initial DUKPT keys.

Q November 2015: Is the implementation of ANSI X9.143 the only method for meeting the requirement that encrypted symmetric keys must be managed in structures called Key Blocks?

A *No. ANSI X9.143 or any equivalent method can be used. Any equivalent method must include the cryptographic binding of the key-usage information to the key value using accepted methods. Any binding or unbinding of key-usage information from the key must take place within the secure cryptographic boundary of the device.*

Q November 2018: PIN Security Requirement 18 states that encrypted symmetric keys must be managed in structures called Key Blocks. This applies to both conveyance and storage. Does this apply only to TDEA keys?

A *No. As stipulated in* ANSI X9.24-1: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques, *both AES and TDEA keys are required to be managed in Key Blocks.*

Q June (update) 2021: Organizations must implement Key Blocks for external connections to Associations and Networks by 1 January 2023. If a service provider cannot implement Key Blocks for all connections to other organizations because one or more of the external organizations do not support key blocks, what are the service provider's options for meeting the requirement?

A *The service provider must implement Key Blocks for all external organizations that support Key Blocks by the deadline. The assessor must validate the service provider is capable of implementing Key Blocks for the other organization(s) who do not yet support Key Blocks when those organizations become capable.*

Furthermore, the assessor must note in the PSR report the organizations for which it has implemented key blocks and those organizations for which the service provider has not with the reason stated—e.g., the other organization does not support Key Blocks.

Q November 2020: Requirement 18 states that Key Blocks must be implemented for internal connections and key storage within Service Provider Environments. Does this apply to key conveyance between secure cryptographic devices within an organization?

A *Yes. It applies to all key conveyance between systems within an organization, including keys stored on databases or in a device's unprotected memory.*

Q April 2021: Key Blocks for the transport and storage of symmetric keys—i.e., AES and TDES keys—are required to be implemented in accordance with a three phased approach. Allowed formats for these Key Blocks are defined by the standards bodies, ASC and ISO. In addition, proprietary—i.e., non-ANSI or ISO-recognized—methods have been allowed if "equivalent." In September 2020, specific criteria that proprietary methods must meet in order to be verified as equivalent was published in the PCI PTS HSM Security Requirements Technical FAQs and in the PCI PTS POI Security Requirements Technical FAQs.

PTS vendors or other third parties providing proprietary methods have until 1 January 2023 to meet these criteria. How does that impact assessments of Service Providers who have implemented these proprietary methods that have not yet achieved validation?

A *Until January 2023, Service Providers, where applicable, can continue to operate using existing proprietary methods that have not yet been validated under the defined process. Any newly developed proprietary methods must undergo the defined process prior to any implementations.*

Q July 2019: PIN Security Requirement 18-3 requires the implementation of key blocks. Interoperable methods include those defined in ANSI X9.143 and ISO 20038. The requirement also allows for any equivalent method whereby the equivalent method includes the cryptographic binding of the key-usage information to the key value using accepted methods. How are equivalent methods determined?

A *Equivalent methods must be subject to an independent expert review and said review is publicly available:*

- *The review by the independent expert must include proof that in the equivalent method the encrypted key and its attributes in the Key Block have integrity protection such that it is computationally infeasible for the key to be used if the key or its attributes have been modified. Modification includes, but is not limited to:*
  - *Changing or replacing any bit(s) in the attributes or encrypted key*
  - *Interchanging any bits of the protected Key Block with bits from another part of the block*
- *The independent expert must be qualified via a combination of education, training, and experience in cryptology to provide objective technical evaluations that are independent of any ties to vendors and special interests. Independent expert is further defined below.*
- *The PTS laboratory will validate that any device vendors implementing this methodology have done so following all guidelines of said evaluation and peer review, including any recommendations for associated key management.*

An Independent Expert possesses the following qualifications:

- *Holds one or more professional credentials applicable to the field—e.g., doctoral-level qualifications in a relevant discipline or government certification in cryptography by an authoritative body such as NSA, CES, or GCHQ;*

- *Has 10 or more years of experience in the relevant subject;*
- *Subscribes to an ethical code of conduct and would be subject to an ethics compliance process if warranted; and*
- *Has published at least two articles in peer-reviewed publications on the relevant subject or is recognized by his/her peers in the field—e.g., awarded the Fellow or Distinguished Fellow or similar professional recognition by an appropriate body such as ACM, BCS, IEEE, IET, IACR.*

Independence requires that the entity is not subject to control, restriction, modification, or limitation from a given outside source. Specifically, independence requires that a person, firm, or corporation who holds itself out for employment as a cryptologist or similar expert to more than one client company is not a regular employee of that company, does not work exclusively for one company, and where paid, is paid in each case assigned for time consumed and expenses incurred.

1.3 Additional Relevant Existing Point of Interaction (POI) Security Requirements Technical FAQs

Q ANSI X9.143 defines three keys: a Key-Block Protection Key (KBPK), a Key-Block Encryption Key (KBEK), and a Key-Block MAC key (KBMK). The KBPK is used to calculate the KBEK and the KBMK. Can the KBPK be used for any other purpose?

A *No. In order to meet the requirement that a key is used only for a single purpose as defined in ANSI X9.24, the Key-Block Protection Key is only used to calculate the KBEK and the KBMK and is not used for any other purpose. Only the KBPK is used to generate the KBEK and the KBMK key; no other key is used for this purpose.*

Q ANSI X9.143 or an equivalent methodology must be used whenever a symmetric key is downloaded from a remote host enciphered by a shared symmetric key. Are there other circumstances where X9.143 or an equivalent methodology applies or does not apply?

A *Devices must support X9.143 or an equivalent methodology for key loading whenever a symmetric key is loaded encrypted by another symmetric key. This applies whether symmetric keys are loaded manually—i.e., through the keypad—using a key-injection device, or from a remote host. It does not apply when clear-text symmetric keys or their components are loaded using standard dual-control techniques.*

Q In support of the conversion of deployed devices to the use of ANSI X9.143, can a key previously loaded for another purpose, such as a KEK, be re-statused as an ANSI X9.143 Key-Block Protection Key.

A *No. Loading of a key into a slot (register) must set the slot to its given function. If the slot's function is changed—or if a new clear-text key is loaded into the slot without authentication using dual control - all other keys in the device (or at least all keys that were previously protected under the key that was previously in the slot) must be erased. This mechanism helps ensure that a device cannot be maliciously taken over.*

Q May (update) 2018: ANSI X9.143 or equivalent support is required as an option for any device that allows the loading of symmetric keys that are encrypted by another symmetric key as a configuration option. To implement ANSI X9.143 or equivalent for devices that are currently implementing a non-ANSI X9.143 symmetric methodology, what characteristics must the device have to support this migration?

A *The device must enforce the following where applicable:*

- *The conversion from a less secure methodology (non-ANSI X9.143 or non-ANSI X9.143 equivalent) to a more secure (ANSI X9.43 or equivalent) methodology must be nonreversible.*
- *When entering the plaintext KBPK (or equivalent) through the keypad, it must be entered as two or more components and require the use of at least two passwords/authentication codes. The passwords/authentication codes must be entered through the keypad or else conveyed encrypted into the device.*

These passwords/authentication codes must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Passwords/authentication codes that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/authentication codes are at least seven characters.

Entry of key components without the use of at least two separate passwords/authentication codes results in the zeroization of pre-existing acquirer secret keys—i.e., the invoking of the key-loading function/command causes the zeroization prior to the actual loading of the new key. For devices supporting multiple-acquirer key hierarchies (e.g., multi-acquirer devices), only the hierarchy (e.g., specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, authentication codes, or similar) for each user on a given device must be different for each user.

- *Loading of a plaintext KBPK (or equivalent) using a key loader must be done using dual control and require the use of two or more passwords/authentication codes before injection of the key. These passwords/authentication codes are entered directly through the keypad of the applicable device or are conveyed encrypted into the device and must be at least seven characters in length. These passwords/authentication codes must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Plaintext keys or their components are never permitted over a network connection.*

  Injection of plaintext secret keys or their components where the receiving device does not itself require the use of at least two passwords/authentication codes for injection results in the zeroization of pre-existing acquirer secret keys. For devices supporting multiple-acquirer key hierarchies (e.g., multi-acquirer devices), only the hierarchy (e.g., specific TMK and working keys) associated with the key being loaded must be zeroized. In all cases, the authentication values (passwords, authentication codes or similar) for each user on a given device must be different for each user.

- *It is not permitted to load the KBPK to the device encrypted by a non-ANSI X9.143 or non-ANSI X9.143-equivalent symmetric key. However, the KBPK may be loaded using asymmetric techniques.*

Q The Guidance for DTR B9 states, “*A device may include more than one compliant key-exchange and storage scheme. This does not imply that the device must enforce ANSI X9.143 or an equivalent scheme, but it must be capable of implementing such a scheme as a configuration option.”* If the use of ANSI X9.143 as the key-exchange mechanism is optional, must there be an explicit device configuration change to enable/disable ANSI X9.143 as the "active" key-exchange scheme?

A *Yes. An explicit configuration change is required. The change is considered a sensitive service and must meet the requirements of B5, “Protection of Sensitive Services.”*

Q August 2011: When a device is converted to or otherwise implements ANSI X9.143, the conversion must be one-way. On a device supporting multiple independent key hierarchies, such as one designed to support multiple acquirers, does the implementation apply to all key hierarchies on the device?

A *No. A device supporting multiple independent hierarchies may implement ANSI X9.143 (or equivalent) on a hierarchy-by-hierarchy basis.*

2 Glossary

The following terms and acronyms used within this document have the meanings provided below.

Term	Definition
Base Derivation Key (BDK)	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the Derived Unique Key Per Transaction key-management method.
Key Block	Block containing a protected key, its usage constraints, and other data that is wrapped (encrypted) using a key-wrapping mechanism
Key-Block Encryption Key (KBEK)	The key that is derived from the Key-Block Protection Key and that is used solely for enciphering the Key Block described in this document.
Key-Block Authentication Key (KBAK)	The key that is derived from the Key-Block Protection Key and that is used solely for calculating the MAC over the Key Block described in this document.
Key-Block Protection Key (KBPK)	The derivation key from which the Key-Block Encryption Key and the Key-Block Authentication Key are derived; this key is used for no other purpose.
Key-Encrypting (Encipherment or Exchange) Key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys.
PIN-Encipherment Key PIN-Encryption Key (PEK)	A PEK is a cryptographic key that is used for the encryption or decryption of PINs.
Service Provider	An entity (that is not a payment brand), acting on behalf of an Acquiring organization for any of the following activities: ▪ Acquiring, processing, storage, or transmission of PIN-based payment transactions ▪ Management of cryptographic keys associated with PIN-based payments—e.g., Certificate Authority, Key-Injection Facility ***Note:*** *If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although it may be considered a service provider for other services).*
Terminal Master Key (TMK)	This is a symmetric key used to encrypt other cryptographic keys at the point of interaction.
Zone Master Key (ZMK)	Also known as a Key-Encipherment Key.

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, JCB International, Mastercard, and Visa Inc., the Council has over 700 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: https://www.pcisecuritystandards.org.