GEOBRIDGE

GUIDE TO IMPLEMENTING KEY BLOCKS

Table of Contents

All rights reserved. No part of this publication may be duplicated, reproduced, or disclosed, except for the purpose of review, without the permission of the copyright owners.

©2018 GEOBRIDGE Corporation
All rights reserved

1. INTRODUCTION

In 2004, a potential vulnerability for the wrapping mechanisms employed when working with DES keys was published in association with the usage of double or triple length keys. Prior to 2010, the payment industry had been relying primarily on single length keys. As such, the vulnerability was largely ignored by the industry. The DES algorithm itself is still considered to be strong cryptography. Yet, the eight Byte blocks associated with the DES algorithm are subject to replacement techniques that ultimately lower the effective intended security of the key. This is mitigated by binding the blocks together using strong cryptography techniques.

Presently, PCI PIN (2014) offers the only enforcement for binding keys. There are no other industry mandated audits or assessments that evaluate the usage of cryptography in the payment space. As such, a common misconception is that the requirement for binding or "key bundling," is only associated with PIN keys. This vulnerability exists for every DES key, and is not confined to keys used with PIN.

Binding can be achieved in any number of ways. This flexibility is at the root of delayed adoption. A traditional double length DES key is most commonly represented as 32 hexadecimal characters. Applying strong cryptography to these existing characters can only serve to lengthen the expected string. While the concept is simple, proprietary techniques that would otherwise be acceptable, create interoperability challenges when keys must be shared, as is often the case for payment keys.

In an effort to promote interoperability, ANSI X9 TR-31 (2017) was published as a reference for all to follow. As a published technical report, those who follow the guidance offered in this report, have the ability to mitigate the potential vulnerability and remain interoperable with business partners when keys must be shared.

GEOBRIDGE is committed to helping our clients achieve a basic understanding of what it means to implement Key Blocks. This document was created as guide to effectively address our customers concerns associated with mitigating the potential vulnerabilities, meeting the enforcement guidelines offered by PCI PIN, and remaining interoperable.

©2018 GEOBRIDGE Corporation
All rights reserved

2. PCI PIN KEY BLOCKS REQUIREMENT

PCI PIN Req. 18-3 Effective 1 January 2018 (see New Implementation Dates below), 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,
- A digital signature computed over that same data,
- 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.

As of March 2017, the PCI SSC revised the implementation date for PCI SSC for PCI PIN Security Requirements v2 Requirement 18-3.

The new implementation dates are broken into phases, allowing organizations to focus resources on associated risk in order to achieve compliance. 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:* ***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* ***June 2021.***

- ***Phase 3*** *– Implement Key Block 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* ***June 2023****.*

©2018 GEOBRIDGE Corporation
All rights reserved

3. STAKEHOLDER IMPACTS

3.1 Key Injection Facilities

- SCDs must utilize Key Blocks for-storage within their Environments, i.e., BDK, KEK – this includes all applications and databases connected to Hardware Security Modules (HSMs) on or before, June 2019.
- This will necessitate the ability to convert standard X9.17 wrapping to key bundling, as keys will still be transferred as X9.17, but will need to be stored as key blocks.
- New or repaired PEDs must be injected using Key Block keys on or before, June 2023.
- Merchant PEDs with legacy variant keys, must be replaced and injected with new Key Block keys on or before, June 2023.
    - ➢ This requirement requires project planning well ahead of the deadline.

3.2 Aquirers and Processors

- Keys must be stored as bundles or key blocks prior to June 2019.
- All Acquirers and Processors who share Key Encrypting Keys (KEKs) with external entities such as the Card Associations for EVM, and the Networks for PIN Debit transactions must replace those keys with Key Blocks Protection Keys (KBPKs) on or before, June 2021.
    - ➢ This requirement requires project planning well ahead of the deadline.
- This will necessitate the maintenance of at least two separate HSM master keys.
- This will necessitate the ability to convert standard X9.17 wrapping to key bundling, as keys will still be transferred as X9.17, but will need to be stored as key blocks.

©2018 GEOBRIDGE Corporation
All rights reserved

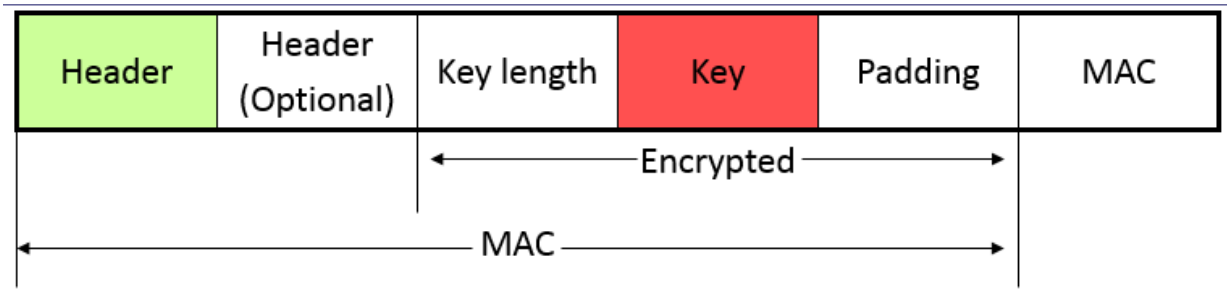
4. TR-31 KEY BLOCK DEFINED

A TR-31 Key Block is an interoperable format defined by the American National Standards Institute (ANSI) to support the interchange of keys in a secure manner with key attributes included in the exchanged data. TR-31 was developed because there is a problem with the security for the interchange of symmetric keys. In the payments environment, it is very important that each symmetric key have a specific set of attributes attached to it, specifying such things as the cryptographic operations for which that key can be used.

The TR-31 Key Block format has a set of defined key attributes that are securely bound to the key so that they can be transported together between any two systems that both understand the TR-31 format.

Key Blocks, which are also known as Key Bundling, or Key Wraps, applies to both when keys are transported and when they are at rest (stored). Key Blocks are used to protect the secrecy and integrity of the encrypted key. The Key Block contains the encrypted key itself along with other data associated with it. The Key Block is protected so that secret data cannot be disclosed and so that neither the encrypted key nor the associated data can be modified without detection. This method may also be used for the storage of keys under asymmetric key.

4.1 Key Block Structure



TR-31 Key Block -Two important features:

1. The key is protected in such a way that it meets the *Key Block* requirements of various standards, and specifically PCI PIN Requirement 18-3. These standards state that the individual 8-byte blocks of a double-length or triple-length TDES key must be bound in such a way that they cannot be individually manipulated. TR-31 accomplishes this mainly by computation of a MAC across the entire structure, excluding the MAC value itself.

©2018 GEOBRIDGE Corporation
All rights reserved

2. Key usage attributes, defined to control how the key can be used, are securely bound to the key itself. This makes it possible for a key and its attributes to be securely transferred from one party to another while assuring that the attributes of the key cannot be modified to suit the needs of an attacker.

4.2 Breaking Down the TR-31 Key Block

Byte #	Header Field Name
0	Key Block Version ID
1-4	Key Block Length
5 -6	Key Usage
7	Algorithm
8	Mode of Use
9-10	Key Version Number
11	Exportability
12-13	Number of Optional Blocks
14-15	Reserved for future use

Byte #	Optional Header Field Name
16-17	First Optional Block ID
18-19	Optional Block 1 Length
20-n	Optional Block 1 Data
n-m	Additional Optional Blocks, if present

©2018 GEOBRIDGE Corporation
All rights reserved

Byte #	Field Name	Description
0	Key Block Version ID	'A' 0x41 (Or Current version). Numeric Version IDs are reserved for proprietary Key Block definitions
1-4	Key Block Length	Key Block length after encoding. Length includes the entire block (Header + encrypted confidential data + MAC)
5-6	Key Usage	Intended function of the protected key/sensitive data. Common functions include encrypting data, PINs, calculating MAC. etc.
7	Algorithm	Algorithm for which the protected key may be used.
8	Mode of Use	Defines the operation the protected key can perform. For example, a MAC key may be limited to verify-only.
9-10	Key Version Number	Version number. Optionally used to indicate that contents of the Key Block is a component, or to prevent re-injection of old keys.
11	Exportability	Defines whether the protected key may be transferred outside the cryptographic domain in which the key is found.
12-13	Number of Optional Blocks	Defines the number of Optional Blocks included in the Key Block.
14-15	Reserved for future use	Field reserved for future use and is filled with ASCII zero (0x30) characters.
16-17	First Optional Block ID	ID field for the First Optional Block, if one is present as indicated by a value other than '00' in bytes 12 and 13.
18-19	Optional Block 1 Length	Length of Optional Block including the field' s ID, length, and data.
20-n	Optional Block 1 Data	If the first Optional Block is present, this field contains the Data for that Optional Block.
n-m	Additional Optional Blocks, if present	A variable number of Optional Blocks can follow the first Optional Block, as indicated by the count in bytes 12-13. Each Optional Block contains a 2-byte ID, 2-byte length, and variable-length data field following the same format described above for Optional Block 1.

4.3 Thales Key Block Defined

Thales Key Blocks can be used to meet the PCI PIN Requirement 18-3, however Thales Key Blocks are propritory and cannot be used interoperabaly. This means that the exchange of Key Blocks between HSMs can on be done only with another Thales HSM (payShield), and does not allow for exchange of Key Blocks with any other HSM vendors (i.e, Attala, Safenet, etc.).

A distinguishing characteristic of the Thales Key Block, as compared with the traditional TR-31 Key Block is that header values, are more flexible, and can support a larger number of types of Optional Header blocks than the TR-31 Key Blocks.

If desired, the Thales and TR-31 Key Blocks can be supported and utilized independently of one

©2018 GEOBRIDGE Corporation
All rights reserved

Another in the payShield. When a combination of Thales Key Blocks and TR-31 Key Blocks are used, this will establish a "trusted" HSM environment. This trusted HSM enviroment ensures that the security of the keys will be fortified to protect against any any possible intruders.

©2018 GEOBRIDGE Corporation
All rights reserved

5. KEYBRIDGE 3100 KEY BLOCK SUPPORT

GEOBRIDGE has supported TR-31 Key Blocks on the KeyBRIDGE 3100 appliance since 2009. Listed below are the critical functionalities that have been developed for the KeyBRIDGE 3100 to assist our customers in being compliant with PCI PIN Requirement 18-3 Key Blocks.

- KeyBRIDGE System Master Key (SMK) and all keys are wrapped under that AES key, and so meet the requirements for storage of keys using TR-31 Key Block Format.
- KeyBRIDGE 3100 AES keys are stored in a Key Block format designed for interoperability with Thales ® HSMs and devices for both key import and export.
- The KeyBRIDGE 3100 Custom Key Usages allows proprietary TR-31 key usages to be defined and used for keys generated and/or stored on KeyBRIDGE.
- KeyBRIDGE 3100 supports the import of keys in electronic form using the both the TR-31 Key Block format for TDES Keys and the Thales ® Key Block format for AES keys.
- KeyBRIDGE 3100 supports the generation, import and export of keys with the Key Usages, as defined in X9 TR-31.
- KeyBRIDGE 3100 supports exporting as a Key Block File, encrypted under a Key Block Protection Key (KBPK) already existing in the KeyBRIDGE Key Inventory.
- When a Key is added to KeyBRIDGE either as a newly generated key or an imported Key, the Key Block attributes are required for before the new key is added to the KeyBRIDGE key database.
- When a Key is exported from the KeyBRIDGE in the format of a Key Block, some of the attributes of the exported Key Block may be specified.
- Within the KeyBRIDGE system, user defined attributes are applied at the key level that allow the adding and editing of TR-31 Headers.
- KeyBRIDGE supports the generation, import and export of keys with the following Key Usages, as defined in X9 TR-31 2010 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms.
- Key BRIDGE supports Custom Key Usages – allows proprietary TR-31 key usages to be defined and used for keys generated and/or stored on KeyBRIDGE.
- KeyBRIDGE has a Manage Custom Key Attributes feature which supports up to twelve user-defined custom key attributes at the key usage level, including the addition and editing of TR-31 Optional Headers.

©2018 GEOBRIDGE Corporation
All rights reserved

6. PAYSHIELD KEY BLOCK SUPPORT

The payShield 9000 HSM supports both the the Thales ® Key Block method and the ANS X9 TR-31 Key Blocks, for the encryption and authentication of keys. The Thales ® Key Blocks are different, since they include proprietary extensions they can be used only to transfer keys between Thales ® payment HSMs. The Thales ® Key Blocks and TR-31 Key Blocks can both be supported independently of one another.

The payShield 9000 has the ability to install 1 or 2 LMKs without additional licensing. One LMK must be a Variant type and one must be a Key Block Type. Additional licenses can be purchased for the payShield 9000 to allow up to 20 LMKs to be installed.

Implementation of an LMK Key Block type on the payShield 9000 requires changing from a Variant Regular LMK to either of two types of Thales ® Key Block LMKs:

- **Triple Length Variant TDES Key Block LMK**
- **AES Key Block LMK***

GEOBRIDGE recommends going straight from Variant Regular LMK to AES Key Block LMK, bypassing the Triple Length Variant TDES Key Block LMK.

6.1 Generation of New Key Block LMK

To generate a new Key Block LMK, three key custodians will need to be assembled, and six new LMK component cards will first need to be created (3 primary cards, and 3 backup cards) to key components on the cards.

The two types of LMK cards (Determine which type your organization uses):

- HSM LMK cards - using the card reader built into the HSM. This type of card is created and used by operators using a console and the HSM card reader.
- payShield Manager RLMK cards - created by operators using payShield Manager and the card reader attached to the remote management PC.

Once the new Key Block LMK has been created from the Smartcard components, the following Migration steps will need to occur:

1. Both the old and new LMKs will need to be installed in the payShield 9000.
2. The current Variant LMK will be placed in Live Storage (LK) to continue transaction processing.
3. The new Key Block LMK will be placed in Key Change Storage (LN) for the migration process.
4. Translation (re-encryption) of any operational keys in the current databases under the current Variant regular LMK.
5. After the translation is complete, the keys will be held in a “pending” new Key Block LMK databases.

©2018 GEOBRIDGE Corporation
All rights reserved

6. Once the Key Block LMK is ready to go live it must be loaded into Live Storage before any transactions can be processed.
7. The "pending" new Key Block LMK databases become live transaction processing databases.

* AES Key Block LMKs must be used to protect AES keys and RSA keys longer than 2048 bits. The payShield can only use AES as a Key Block.

6.2 HSM Key Block Protection Keys

The Key Block Protection Keys (KBPKs) will take the place of the ZMKs and KEKs being used. The Key Block Protection Key (KBPK) using CMAC, is the derivation key from which the Key Block Encryption Key and the Key Block Authentication key are derived. The KBPK is used for no other purpose. The KBPK is also known as a Key Wrapping Key.

The Key Block Encryption Key is used solely for enciphering the Key Block.

The Key Block Authentication Key is the key that is used solely for calculating the MAC over the Key Block.

6.2.1 NEW KEY BLOCK HSM KEY SCHEMES

Key Block LMKs introduce two new key Schemes. The table below will demonstrate all possible key schemes for use with the Thales HSM. Specifically, key schemes "R" & "S" are relevant to the use of key blocks.

Key Scheme Tag	Notes
None/Z	Encryption of a single-length DES key using X9.17 methods. Used for encryption of keys under a variant LMK, and can also be used for the import or export of keys.
U	Encryption of a double-length DES key using the variant method; used for encryption of keys under a variant LMK.
T	Encryption of a triple-length DES key using the variant method; used for encryption of keys under a variant LMK.
X	Encryption of a double-length key using X9.17 methods; only available for import and export of keys. This mode is enabled within the Configure Security command,
Y	Encryption of a triple-length key using X9.17 methods; only available for import and export of keys. This mode is enabled within the Configure Security command.
V	Encryption of keys using Verifone/GISKE methods; used for export of DES keys.
R	Encryption of keys using TR-31 Key Block methods; only used for import or export of keys. The use of this scheme requires optional license HSM9-LIC006.
S	Encryption of DES, AES, RSA & HMAC keys using Thales Key Block methods; used for encryption of keys under a key block LMK.

©2018 GEOBRIDGE Corporation
All rights reserved

6.3 Current and Custom HSM Commands

Not all console commands and host commands can be used with Key Block LMKs. Most commands that do not support the use of a Key Block LMK have a newer, alternative command that should be used in their place. Additionally customers with custom commands will need to ensure those commands are converted to support Key Blocks. This will need to be addresssed on an individual basis to determine the functionality of those commands, along with the conversion process will be required to move commands from the Variant LMK to to the new Key Block LMK. The table below comes from the Thales payShield Host Programmers Manual V 3.1d. This maps standard keys from the Variant table to the appropriate Key Block Usage.

6.3.1 VARIANT TO KEY BLOCK MAP

Key Name	Variant		Key Block		
	Key Type	LMK	Key Usage	Algorithm	Mode of Use
BDK-1	009	28-29/0	"B0"	"T"	"X", 'N'
BDK-2	609	28-29/6	"41"	"T"	"X", 'N'
BDK-3	809	28-29/8	"42"	"T"	"X", 'N'
BDK-4	909	28-29/9	"43"	"T"	"X", 'N'
CSCK	402	14-15/4	"C0", "11"	"D", "T"	"C", "G", 'N', "V"
CVK	402	14-15/4	"C0", "12", "13"	"D", "T"	"C", "G", 'N', "V"
DEK	00B	32-33/0	"D0", "21"	"D", "T", "A"	"B", "D", "E", 'N'
HMAC	10C	34-35/1	"61", "62", "63", "64", "65"	"H"	"C", "G", 'N', "V"
IKEY®	302	14-15/3	"B1"	"T"	"X", 'N'
KML	200	04-05/2	"E6", "31"	"T"	'N'
MK-AC	109	28-29/1	"E0"	"T"	'N'
MK-CVC3	709	28-29/7	"E6", "32"	"T"	'N'
MK-DAC	409	28-29/4	"E3"	"T"	'N'
MK-DN	509	28-29/5	"E4"	"T"	'N'
MK-SMC	309	28-29/3	"E1"	"T"	'N'
MK-SMI	209	28-29/2	"E2"	"T"	'N'
PVK	002	14-15/0	"V0", "V1", "V2"	"D", "T"	"C", "G", 'N', "V"
RSA Private Key	00C	34-35/0	"03"	"R"	"B", "D", 'N', "S"
RSA Public Key	00D	36-37/0	"02"	"R"	"B", "E", 'N', "S"
TAK	003	16-17/0	"M0", "M1", "M3", "M5", "M6"	"D", "T", "A"	"C", "G", 'N', "V"
TEK	30B	32-33/3	"D0", "23"	"D", "T", "A"	"B", "D", "E", 'N'
TKR	002 or 90D	14-15/0 or 36-37/9	"P0", "73"	"D", "T"	'N'
TMK	002 or 80D	14-15/0 or 36-37/8	"K0", "51"	"D", "T", "A"	"B", "D", "E", 'N'
TPK	002 or 70D	14-15/0 or 36-37/7	"P0", "71"	"D", "T"	"B", "D", "E", 'N'
WWK	006	22-23/0	"01"	"D", "T"	"C", "G", 'N', "V"
ZAK	008	26-27/0	"M0", "M1", "M3", "M5", "M6"	"D", "T", "A"	"C", "G", 'N', "V"
ZEK	00A	30-31/0	"D0", "22"	"D", "T", "A"	"B", "D", "E", 'N'
ZMK	000	04-05/0	"K0", "52"	"D", "T", "A"	"B", "D", "E", 'N'
ZPK	001	06-07/0	"P0", "72"	"D", "T"	"B", "D", "E", 'N'

©2018 GEOBRIDGE Corporation
All rights reserved

7. GEOBRIDGE COMPLIANCE ADVANTAGE

The table below identifies the phases and dates that are now mandated for Key Blocks by PCI. This provides GEOBRIDGE guidance on the KeyBRIDGE 3100 and payShield 9000 compliant implementation and what can be done to meet those dates, if not already being done.

Phase/Effective Date	Implementation Requirement	GEOBRIDGE Guidance
Phase 1 **June 2019**	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 (HSMs).	**KeyBRIDGE 3100** • The KeyBRIDGE 3100 currently has an AES System Master Key (SMK) and all keys are wrapped under that AES key, and are stored using TR-31 Key Block Format. • The KeyBRIDGE 3100 Custom Key Usages allows proprietary TR-31 key usages to be defined and used for keys generated and/or stored on KeyBRIDGE. • The KeyBRIDGE 3100 AES keys are stored in a Key Block format and is designed for interoperability with Thales ® ® HSMs and devices for both key import and export. **payShield HSM** • Key Block LMKs can created and be authorized on the payShields. • GEOBRIDGE recommends customers go directly to AES LMK Key Block, rather than TDES LMK. AES LMKs force ALL keys, including TDES keys, to be wrapped as Key Blocks.
Phase 2 **June 2021**	Implement Key Blocks for external connections to associations and networks.	**KeyBRIDGE 3100** • KeyBRIDGE 3100 supports the import of keys in electronic form using the both the TR-31 Key Block format for TDES Keys and the Thales ®® Key Block format for AES keys. • KeyBRIDGE 3100 supports the generation, import and export of

©2018 GEOBRIDGE Corporation
All rights reserved

		keys with the Key Usages, as defined in X9 TR-31. • KeyBRIDGE 3100 supports exporting as a Key Block File, encrypted under a Key Block Protection Key (KBPK) already existing in the KeyBRIDGE Key Inventory. • When a Key is added to KeyBRIDGE either as a newly generated key or an imported Key, the Key Block attributes must be defined for the new key. • When a Key is exported in the format of a Key Block, the attributes of the exported Key Block can be specified. • Within KeyBRIDGE system, user defined attributes applied at the key level allow the adding and editing of TR-31 Headers. **payShield HSM** • The Key Block protection Keys (KBPKs) will take the place of the ZMKs being used. • KBPKs will need to be shared with partners sharing dynamic keys.
Phase 3 **June 2023**	Implement Key Blocks to extend to all merchant hosts, POS devices and ATMs.	**KeyBRIDGE 3100** • KeyBRIDGE does supports the generation, import and export of keys Key Usages, as defined in X9 TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms. • Key BRIDGE does supports Custom Key Usages – allows proprietary TR-31 key usages to be defined and used for keys generated and/or stored on KeyBRIDGE. • KeyBRIDGE has a Manage Custom Key Attributes feature which supports up to twelve user-defined custom key attributes at the key usage level, including the

©2018 GEOBRIDGE Corporation
All rights reserved

		addition and editing of TR-31 Optional Headers.

8. STANDARDS AND REFERENCES

X9 TR-31, 2017: ***Interoperable Secure Key Exchange Block Specification***

ANS X9.24, 2017: ***Retail Financial Services Symmetric Key Management Part 1***

NIST 800-38b: ***Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication***

PCI PIN v2.0, 2014: ***PCI PIN Security Requirements***

1270A542-033: ***Thales payShield 9000 Host Programmers Guide***

NIST 800-108: ***Recommendation for Key Derivation Using Pseudorandom Functions***

©2018 GEOBRIDGE Corporation
All rights reserved