Standard: PCI PTS PIN

Date: June 2017

Author: PTS Working Group
PCI Security Standards Council

Information Supplement:
Cryptographic Key Blocks

Document Changes

Date	Document Version	Description	Pages
June 2017	1.0	Initial release	All

Table of Contents

Executive Summary

PCI PIN Security Requirements v2.0, published December 2014, introduced a new requirement to increase security for encrypted keys. Implementation of key blocks—sometimes referred to as “key bundling”—greatly improves the security of symmetric keys that are shared among payment participants to protect PINs and other sensitive data. Requirement 18-3 states:

> Effective 1 January 2018, 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.

In April 2017, the effective date was modified to allow the implementation to occur in three phases, each with its own effective date. This will allow organizations to focus resources to address implementation tasks specific to their environment and support a smooth migration across the payments network. 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 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 **June 2023**.

The use of cryptographic key blocks for the secure exchange of keys is a means of using one or more blocks to bind key parts with information about the resulting key—e.g., an identifier, a purpose/function code, or an origin authenticator. The use of cryptographic key blocks, especially as it applies to Triple Data Encryption Algorithm (TDEA) keys, is known as key bundling[1]; however, more generally, it includes key wrapping. (See ISO, NIST, and IETF citations in Section 5, “References.) A key bundle in the context of TDEA is the ordered set of key parts k_1, k_2, and k_3, where each k_n is a single DEA key. See Appendix B for more technical details. A key bundle is clear text—i.e., not encrypted and not protected from modification. When it is "bundled" or "wrapped" into a key block, cryptographic operations are performed to provide both confidentiality and integrity protection.

Cryptographic key blocks may be used to protect both TDEA and AES keys.

[1] See ANSI X9.24-1 §7.4.

1. Introduction

For cryptographic keys to provide security reliably, they require mechanisms that accomplish the following:

1. Associate the type/purpose of the key to ensure that the key isn't used for other than its designated purpose—e.g., as a key-encrypting key or as a PIN-encrypting key.

2. Protect the integrity of the key including the order of key parts for algorithms that require multiple key parts—e.g., Triple Data Encryption Algorithm (TDEA).

The first objective has been accomplished historically through the use of proprietary processes known as variants and by a standardized process known as key wrapping. The second objective is also addressed by key wrapping and by X9 TR-31, *Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*.

Use of key variants is an earlier manner of limiting key usages. Key variants are created by the imposition of a binary mask associated with a given key type. The mask is combined with the underlying key in a proprietary manner.

Key wrapping is a form of cryptographic key protection that includes the use of key blocks. The purpose of key wrapping is to bind the key (e.g., an AES key or all of the key parts of a TDEA key) to additional information. It provides integrity protection for the key and associated information and may provide confidentiality protection to all or part of the resulting block.

For a comparison of current and new methods, refer to Appendix A. For a more technical discussion of key blocks, variants, and key wrapping, see Appendix B.

1.1 Risk Associated with use of only a Variant

The key variant provides an association with the key's intended purpose, which allows the Secure Cryptographic Device (SCD) to enforce a specific use. However, it does not by itself provide for key-block integrity or authentication. Because of this, there are known attacks that weaken the underlying key's security, resulting in key recovery and thereby compromising the encrypted data.

Since variants are vendor-specific implementations, they also involve a business risk. The proprietary nature of variants—that is, a lack of interoperability—may make future migrations more difficult, especially if migrating from one vendor to another or to a new product line of the same vendor where variants may not be supported.

2 Why Key Blocks

For TDEA (also known as Triple DES), the Data Encryption Algorithm (DEA) is applied three times using either two or three keys (referred to as key parts since they form one effective TDEA key). This is known as 2-key (or double-length key) TDEA or 3-key (or triple-length key) TDEA, respectively. The order of the key parts is critical to the strength of the resulting TDEA encryption. Without the use of key blocks, the order of the key parts is not assured. By changing the order of the key parts, TDEA can be made to function as if it were only DEA—thereby reducing the effective key strength from 80 bits to less than 56 for 2-key TDEA.

For any symmetric cryptographic key (e.g., TDEA or AES), restricting its use to a specific purpose is also important. When a key is used for more than one purpose, an attacker gains additional material that increases the means and likelihood of solving for the key, thereby reducing the security the key would otherwise provide. Also, associating a key with a single, specific use allows a system to enforce policies on its use. This is especially important for keys used to encrypt PINs where the PIN is not allowed as clear text outside of a secure cryptographic device (SCD). An SCD—for example a host security module (HSM)—may have keys for encrypting and decrypting data that the host computer would use. The HSM would have a policy that permits data-encrypting keys to decrypt data for use within the host computer. If an attacker were able to convince the HSM that a PIN was just data, access to the cryptogram of the PIN key and the encrypted PIN would permit the attacker to obtain the clear-text PIN from the HSM without the need for solving for the PIN key. However, if the PIN key is within a key block that identifies it as a PIN key, the HSM can enforce the policy that the clear-text results of using this key never leave the HSM.

3 Answers to Some Questions about Key Blocks

This Q&A is provided as guidance and does not supersede or extend any PCI standards or authoritative FAQ. Contact your acquirer or payment brand to understand implementation, interoperability, and compliance requirements associated with the use of cryptographic key blocks.

Q 1 In addition to the PTS PIN Standard, where else should I look for authoritative information?

A *Current FAQs from* PIN Transaction Security (PTS) POI Security Requirements: Technical FAQs for use with Version 5 *(See Requirement B11), and* PTS PIN Security Requirements: Technical FAQs for use with Version 2*.* In addition, see the documents identified in the Section 5, “References.”

Q 2 Does everyone have to convert to use key blocks at the same time?

A *No. Encrypted keys can continue to be shared between organizations without key blocks; however, both parties must use key blocks before the risks associated with not using key blocks are eliminated. For example, a POS device may not be converted to support key blocks, but the host to which it is connected might be. Communication between the POS device and the host still occurs as it had in the past; therefore, no improvement in security is realized.*

Q 3 As a service provider, can I still support variants after the applicable phase effective date?

A *Contact your acquirer or brand for their position on this.*

Q 4 What happens if one side does not convert to key blocks?

A *Regardless of whether the other side converts when you do or not, you must still ready your system.*

Q 5 Must I use key blocks for all encryption keys (e.g., encrypting any data) or just for PIN-encryption keys?

A *For the purposes of this document, the requirement is specific to PIN-encryption keys and any keys associated with PIN protection—for example, key-encipherment keys used to protect PIN-encryption keys—however, best practice is to use key blocks for all symmetric keys.*

Q 6 Am I required to purchase new hardware to support key blocks?

A *Key-block compatible hardware, PIN entry devices (PEDs) and encrypting PIN pads (EPPs), have been in the marketplace since 2007. All PCI PTS PEDs and EPPs version 2 and greater, and all PCI-approved HSMs for PIN decryption support key blocks.*

Q 7 Do I need to replace cryptographic keys with new ones when I implement key blocks?

A *Changing to new keys properly protected as key blocks is a best practice. Contact your acquirer or payment brand to understand implementation requirements.*

Q 8 Do key-management processes change?

A *Yes. With the TR-31 interoperable methodology, for example, the introduction of a key-block protection key (from which other keys are derived) and the processes around its generation, distribution, etc., will be new.*

Other implementations—for example, key wrap and some proprietary or regional approaches that accomplish the same objectives—will also impact the key-management process.

Q 9 I was able to e-mail a cryptogram; may I e-mail a key bundle?

A *Under the same security requirements and conditions, yes.*

Q 10 Do I have to migrate to AES at the same time?

A *No. However, it should be considered as it may be more efficient and will avoid the need to do so at a later date.*

Q 11 Do I have to change my master file key to support key bundling?

A *No. However, a migration to AES will require a new MFK (an AES one), which may impact previously generated keys. Contact your acquirer or payment brand to understand implementation requirements.*

Q 12 Some devices allow the use of a decrypt-data function that if not controlled may allow sensitive information—e.g., keys or PINs—to be output in the clear. How must a device protect against the outputting of sensitive data?

A *It must be managed using at least one of five techniques:*

1. *The key-usage information of any downloaded key must be cryptographically bound to the key value using accepted methods, and the device must enforce that the key is only used for the intended use.*
2. *The addition of a new key type (slot) subsequent to the initial configuration of the device causes the zeroization of all other secret keys. Devices supporting remote key-distribution techniques using asymmetric techniques shall only support the use of such techniques for the loading of TMKs. Support shall not exist to use remote key-distribution techniques for working keys (e.g., PIN, data, or MAC) unless the key-usage information is cryptographically bound to each individual key.*
3. *Downloaded-data key types must not be accepted by the device unless enciphered by a different terminal master key than sensitive keys such as the PEK or MAC key types.*
4. *The device does not provide any support for a decrypt-data or similar function.*
5. *The device must ensure that keys with different purposes can never have the same value. This requirement must be maintained until the device is decommissioned—or until the applicable TMK(s) changes.*

4 Glossary

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

Term	Definition
AES	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). Algorithm specified in ISO/IEC 18033-3 §5.2.
ANSI	American National Standards Institute (www.ansi.org) is the umbrella organization for accredited standards organizations in the U.S.
CBC	Cipher-block-chaining mode
CFB	Cipher-feedback mode
Encryption Key	The cryptographic key used in the process of converting information into an unintelligible form except to holders of a specific cryptographic key.
Key Block	Per X9 TR-31, a key block consists of 3 parts: • Key-block header, which contains attribute information about the key and the key block • The confidential data that is being exchanged/stored • The key block binding method
Key-Block Protection Key	The derivation key from which the key-block encryption key and the key-block MAC key are derived; this key is used for no other purpose. This is also known as a key-wrapping key.
Key Bundle	The three cryptographic keys (K_1, K_2, K_3) used with a TDEA mode.
Key Wrap	A symmetric encryption algorithm designed to encapsulate (encrypt) cryptographic key material.
ISO	International Organization for Standardization. An international standards setting organization composed of representatives from various national standards organizations.
MAC Key	A message authentication code (MAC) key is the cryptographic key used in the generation of a MAC. A MAC is a short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed (has integrity).
Master File Key (MFK)	This is a symmetric key used to encrypt other cryptographic keys which are to be stored outside of the hardware security module (HSM).
NIST	National Institute of Standards and Technology. The U.S. Government standards organization responsible for cybersecurity and cryptographic standards.
TDEA	Triple Data Encryption Algorithm (TDEA), also known as TDES, is a block cipher based on the Data Encryption Algorithm (DEA). TDEA is specified in ISO/IEC 18033-3 §4.2.

5 References

ANSI X9.24-1 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

ANSI X9.102-2008 [Reaffirmed 2017] Symmetric Key Cryptography for the Financial Services Industry – Wrapping of Keys and Associated Data

ANSI X9 TR-31 Technical Report: Interoperable Secure *Key Exchange Key Block Specification for Symmetric Algorithms*

ANSI X9 TR-37-2010 Technical Report: Migration from DES

ISO 19038: Banking and related financial services – Triple DEA – Modes of operation – Implementation Guidelines

ISO DIS 20038 – Banking and related financial services – Key wrap

ISO/IEC 18033-3 – Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers

ISO/IEC 19772:2009 – Information technology – Security techniques – Authenticated encryption

NIST – AES Key Wrap Specification. November 2001

NIST Special Publication 800-38C – Recommendation for Block Cipher Modes of Operation, Methods and Techniques: the CCM Mode for Authentication and Confidentiality, May 2004

NIST Special Publication 800-38E – Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010

NIST Special Publication 800-38F – Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012

NIST Special Publication 800-67 (Revision 1) – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012

RFC 3394 – Advanced Encryption Standard (AES): Key Wrap Algorithm. IETF, September 2002

RFC 5649 – Advanced Encryption Standard (AES): Key Wrap with Padding Algorithm. IETF, August, 2009

Appendix A: Comparison of Methods

Implementation of key blocks—sometimes referred to as “key bundling”—greatly improves the security of symmetric keys that are shared among payment participants to protect PINs and other sensitive data. Key blocks cryptographically bind the key usage to the key and prevent double-length TDEA keys from being attacked as two single-length keys. Attacking a TDEA key as a pair of single-length keys greatly reduces the effective strength of the TDEA key. Previously, two methodologies were primarily in use for the conveyance and/or storage of symmetric keys, such as TDEA. A comparison of the methodologies follows:

	Current Methods		New Method
	ANSI X9.17[2]/ECB	**Variant Method**	**Key Blocks—e.g., TR-31**
Overview	Key halves of double-length TDEA key are individually encrypted as single-length keys. Used as the default mechanism for key conveyance between organizations.	Same as ECB, with the addition of a fixed known value (similar to a salt) to the key-encipherment key used to encrypt the subordinate key.	The key block contains the encrypted key itself along with other associated data. The key block is protected so that secret data cannot be disclosed (encryption) and neither the encrypted key nor the associated data can be modified without detection (integrity). It includes one or more attributes that define the operations for which the key can be used and one or more attributes that define the cryptographic algorithm and mode for which the key can be used. These attributes are intended to prevent the misuse of a key using a different cryptographic algorithm or mode that could facilitate an attack to determine the value of the key.
Implementation	Key conveyance	Key conveyance/ local storage	Key conveyance/local storage
Key Usage	Unbound: Key usage can be readily manipulated. Manipulation of usage has occurred in known attacks: See Annex below.	Limited usage restrictions: Key usage can be readily manipulated.	Cryptographically bound to key. Key usage cannot be manipulated.

[2] ANSI X9.17 was withdrawn in 1999 by X9 TG26, which was, in turn, withdrawn by ANS [X9] TR-37 2009.

	Current Methods		New Method
	ANSI X9.17[2]/ECB	**Variant Method**	**Key Blocks—e.g., TR-31**
Key Bundles	Not supported. Double-length TDEA keys can be broken apart and attacked as individual, single DES keys.	Not supported. Double-length TDEA keys can be broken apart and attacked as individual, single DES keys.	Cryptographically binds the entire TDEA key as a single block of data that prevents attacking a TDEA key as a pair of single DES keys.

A.1 Annex

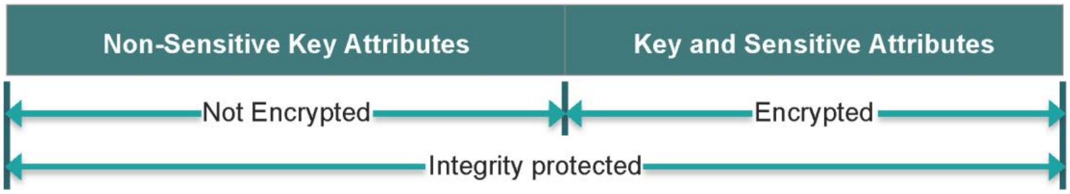
PCI PIN Security Requirements v2.0, published December 2014, contains the following requirement statement:

> Effective 1 January 2018, 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.

The *PCI PIN Security Requirements* language is consistent with *ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques* and with *ISO 19038: Banking and related financial services – Triple DEA – Modes of operation – Implementation Guidelines* where key blocks are mandated. ANSI originally promulgated the requirement in 1998 in the Triple Data Encryption Algorithm Modes of Operation standard. ANSI further promulgated the use of key blocks in 2004, as part of the update to require TDEA for the protection of messages and other sensitive information in a financial services environment.

In support of this, ANSI published in 2005, and updated in *2010 ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms.* TR-31 is intended to provide an interoperable method for implementing key blocks consistent with ANSI X9.24.

The key block is protected so that secret data cannot be disclosed (encryption) and so that neither the encrypted key nor the associated data can be modified without detection (integrity). In particular this is used to protect the integrity of double-length TDEA keys, so that they cannot be unbundled and attacked as two single-length DEA keys; and for any symmetric key, that its key usage cannot be manipulated by an attacker.



X9.24 Key Block Overview Illustration

For any symmetric key, the cryptographic binding of the key usage to the key prevents attacks that use manipulation of this usage. For example, what became known as the Russian Malware attack during 2009-10 involved the ability to change the key-usage tag for the PIN-encryption key to that of a data key, which allowed the capture of PIN data at ATMs.

For TDEA, this further prevents double-length TDEA keys from being treated as a pair of single-length keys for purposes of brute force attacks. The effect is to require that instead of the set of all possible keys being equal to 2^{112} (5,192,296,858,534,830,000,000,000,000,000,000) possible key values for 2-key TDEA, it is reduced to only $2^{56} + 2^{56} = 2^{57}$ (144,115,188,075,856,000) possible key values. Single DEA keys became trivial to attack in 1999 as shown by the DES Cracker machine built by the Electronic Freedom Frontier, which demonstrated that data encrypted by a single DEA key could be determined by a brute force attack in less than 24 hours using a device that cost less than $250,000.

Other DES-cracking implementations have followed, including in 2006 with the COPACOBANA (Cost-Optimized Parallel Code Breaker) machine, which is optimized for running crypt-analytical algorithms, and could be realized for less than $10,000 ten years ago. This machine is built entirely with off-the-shelf components. Time and cost constraints have declined significantly since then.

As a result, starting in 2007 with version 2 of POI, POI devices were required to support TR-31 or an equivalent method in order to provide infrastructure. PCI-approved HSM devices have been required to support TR-31 or an equivalent method beginning in 2009, when version 1 of the requirements was published.

Appendix B: Key Blocks and Key Wrapping

The use of cryptographic key blocks for the secure exchange of keys is not the same as the cryptographic block cipher modes of operation, e.g., cipher-block-chaining (CBC) and cipher-feedback (CFB) mode. Rather, it is a means of using one or more blocks to bind key parts with information about the resulting key—e.g., an identifier, a purpose/function code, or an origin authenticator.

The use of cryptographic key blocks, especially as it applies to Triple Data Encryption Algorithm (TDEA) keys, is referred to as "key bundling" (see ANSI X9.24-1 §7.4). However, more generally the use of key blocks is a form of key wrapping. (See ISO, NIST, and IETF in Section 5, "References".)

B.1 Why are those attributes important?

We depend on keys performing their assigned functions—no more and no less. This allows implementers to establish specific policies for specific key types. For example, if the HSM knows that a given key is a PIN key, it will not allow its use for non-PIN data. Similarly, if the HSM knows that a key is a key-encrypting key, it will not allow it to encrypt data. The ability for devices to enforce these policies helps prevent attacks against these keys. Actual frauds have occurred where the cryptographic keys were manipulated in situations where these attributes were not effectively enforced. (For example see: https://www.wired.com/2009/04/pins/.)

B.2 TDEA Key Blocks

The term "key block" refers to the creation of a block that includes the encrypted key and associated information. It was also referred to as "key bundling" (which harkens back to early X9 standards that have subsequently abandoned the term). ISO, NIST, and IETF all use the term "key wrapping." A "key bundle," however, is defined in *Payment Card Industry PTS POI Modular Security Requirements*, where it is only used in the context of TDEA. A TDEA key bundle specifically addresses assuring the order of the key parts used (k_1, k_2, k_3). It is referenced in B11 where the reader is referred to TR-31 or "equivalent methodology." NIST SP 800-67 provides the following description for a key bundle.[3]

> A TDEA key consists of three keys for the cryptographic engine (Key1, Key2 and Key3); the three keys are also referred to as a key bundle (KEY). Two options for the selection of the keys in a key bundle are approved. Option 1, the preferred option, employs three unique keys (i.e. Key1, Key2 and Key3, where Key1 ≠ Key2, Key2 ≠ Key3, and Key3 ≠ Key1). Option 2 employs two unique keys and a third key that is the same as the first key (i.e. Key1, Key2 and Key3, where Key1 ≠ Key2 and Key3 = Key1). A key bundle shall not consist of three identical keys. [4]

A TDEA key bundle does not provide cryptographic protections or bind the resulting TDEA key to attributes. To accomplish those objectives, appropriate cryptographic operations must be performed to format it into a key block. This process is generally referred to as key wrapping.

[3] *Payment Card Industry PTS POI Modular Security Requirements, v5.0*

[4] NIST SP 800-67.

B.3 Key Wrapping

Key wrapping is a form of cryptographic key protection that includes the use of key blocks, but is not limited to symmetric key cryptography.

The purpose of key wrapping is to bind the key (e.g., an AES key or all of the key parts of a TDEA key) to additional information. It provides integrity protection for the key and associated information and may provide confidentiality protection to all or part of the resulting block. Some key-wrapping mechanisms encrypt the entire block, while others provide authentication over the entire block, but only encrypt part of the block—e.g., the key. The following depicts a typical key block.

Header	**Key Length**	**Key**	**Padding**

ANSI X9.102 defines four key-wrap mechanisms ("modes") and their underlying block ciphers. Those mechanisms are given in the table below:

Identifier	Description
AESKW	An authenticated encryption mechanism that features an ASC X9-approved block cipher with a block size of 128 bits, such as the AES algorithm.
TDKW	The analog of AESKW in which the block size of the underlying block cipher is 64 bits—e.g., TDEA. Thus, a semi-block consists of 32 bits; and, in order to provide integrity protection comparable to that of AESKW, TDKW devotes two semi-blocks to this purpose.
AKW1	An authenticated encryption mechanism with TDEA as the underlying block cipher. It is essentially equivalent to the mechanism specified in x9.24-1.
AKW2	Essentially CBC mode encryption followed by CBC-MAC authentication of the associated data and ciphertext, where the two keys are related to the key-wrapping key, and hence to each other, by a constant exclusive-OR difference.

While X9.102 provided four mechanisms, X9.102 also references NIST SP 800-38C for the CCM mode. Many more modes are defined in other documents from ISO, X9, NIST, and IETF. Because key-wrap methods and modes exist that provide differing features to accommodate different use cases, no single choice suffices. Also, modes exist to accommodate both symmetric and asymmetric algorithms (i.e., secret and private keys) with different key lengths and structures. X9 TR-31 is an attempt to provide limited, interoperable choices specific to the X9.24 use case.

B.4 Variant[5]

Key variants are created by the imposition of a binary mask associated with a given key type. The mask is combined with the underlying key in a proprietary manner. Since the masks/methods are proprietary to specific vendors, they are referred to by the vendor's name—e.g., Atalla Variant and IBM Variant (also known as "control vectors"). Atalla has subsequently adopted the industry standard key wrapping, but provides legacy support for the Atalla Variant. IBM also supports key wrapping.

Since the variant approach relies on a specific use of the Master File Key (MFK), any migration from variants to industry standard key wrapping may require the use of an additional HSM(s) and an associated new MFK not configured for the variant method.

[5] The term "variant" is also used in cryptographic key generation where a base key is used to create a series of related keys or "variants." This, however, is not the type of variant addressed in this paper.

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. Created in 2006 by the founding payment card brands American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 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: pcisecuritystandards.org.