Crypto Tidbits

Introducing CryptoTidbits

CryptoTidbits are short whitepapers published by Cryptera. They explain various subjects related to cryptography, security or electronics.

Useful information in the blink of an eye!

WHITE PAPER | FEBRUARY 2022

Do You need new EPPs for the PCI PIN key block deadline?

Introducing TR-31 formatting of Key Blocks

Why does PCI require Key Blocks?

How does TR-31 enchance security in Key Management?

www.cryptera.com

CRYPTERA®

Introducing TR-31 formatting of Key Blocks

The TR-31 key block format is a popular subject in security discussions in the world of electronic payment.

In order to strengthen security in management of cryptographic keys related to PIN encryption, PCI have set requirements to remove use of older key handling methods in payment solutions. According to these requirements, older EPPs not supporting TR-31 will have to be replaced.

The original deadline for introducing Key Blocks was in 2023, but it has been postponed till January 1st 2025 (see Visa).

A Key Block is a package of data (typically bytes) that forms a message used to pass a cryptographic key from one system to another.

A typical scenario in relation to PCI, is the transport of a key value from the Hardware Security Module (HSM) of the bank host system to an Encrypting PIN Pad (EPP) in an ATM installed at a branch office of the bank.

Why does PCI require Key Blocks?

Some traditional methods used to transfer cryptographic keys to devices – like an EPP – focus solely on keeping the key value protected by encryption. The format doesn't necessarily ensure that the key value is used for the intended purpose.

The concern of PCI is that some types of fraud rely on using key values for a different purpose than intended.

How does TR-31 enhance security in Key Management?

In secure operations it is good security practice that keys are used for a specific purpose. *As examples:* The same key value cannot be used for encryption of both PIN and card data, different keys are needed for encryption and signing etc.

Imagine that the message passing an encrypted key value to a device can be loaded for encryption as well as for decryption. That would leave the device compromised, as anyone with access to this key message and the device will be able to load the key and use the same device to decrypt the information sent.

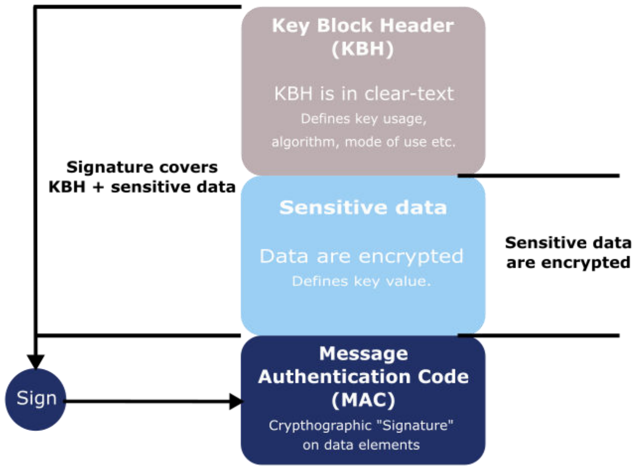
Real fraud scenarios are more complex. This is a simplified example to illustrate the point. A secure device shouldn't be able to use the same key value for different purposes. This is achieved by a clearly defined key hierarchy in which all keys have a well-defined purpose.

The TR-31 key block provides the information needed to ensure that the key is protected in transport and that it can only be loaded in a register matching it's intended usage. The secure device accepting the key will verify that keys are only used as intended. In PCI terms this is called "key binding".

A TR-31 key block consists of 3 part:

- A Key Block Header (KBH) which holds public information about the key
- An encrypted block that holds the key value and other protected information
- A Message Authentication Code (MAC) calculated on the two blocks above

TR-31 Key Block Structure


Key Block Header (KBH)
KBH is in clear-text
Defines key usage, algorithm, mode of use etc.
Signature covers KBH + sensitive data
Sensitive data
Data are encrypted
Defines key value.
Sensitive data are encrypted
Sign
Message Authentication Code (MAC)
Crypthographic "Signature" on data elements

The KBH holds information on the intended key usage. Examples are key exchange, data encryption, PIN encryption etc.

When a device receives this TR-31 Key Block, it will recalculate the MAC on the two first parts and verify that it matches the MAC included in the Key Block.

Since the KBH is covered by the MAC, it can’t be modified as this would invalidate the signature. The device will verify that the key usage information matches the function of the register targeted. It will reject the key loading if attempts are made to load the key for a purpose for which it isn’t intended.

Disclaimer

The information in this document is provided “as-is” to give a general overview of the subject.

It is correct to the best of our knowledge, but readers should always be advised to seek specific information in relation to their products and markets.

Cryptera cannot be held liable for any damage or loss resulting from the use of the information provided in this document.