Key Management in WAY4™

Contents

Overview

This document describes encryption key management procedures in WAY4™.

Chapter 1. Basic Principles of Key Management

Key management procedures, such as generation, transfer, storage, revocation and deletion, must meet the requirements specified below.

Key Generation

Private keys must be generated using procedures or processes that fully guarantee that it is impossible to predict generated private key values and determine that generation of one key is more probable than the generation of others. For this reason, procedures for generating secret keys use the Hardware Security Module (HSM), which randomly generates random secret keys or secret key components.

Only strong keys may be generated. Secret keys for symmetric cryptographic algorithms, such as 3DES or AES, must consist of at least 112 unpredictable bits.

Secret keys must be generated in the presence of at least two authorised individuals (security officers). These individuals must ensure that it is impossible to disclose an unencrypted secret key component during its transfer from the key generation device (HSM) to the device (printer) receiving the secret key or key component.

Key components must be printed in PIN mailers or sealed immediately after printing so that only an authorised party has access to each component and so that tampering with the envelope can be easily detected.

A security officer having access to one component of a key, or to the media conveying this component, must not have access to any other component of this key. Any security officer who has access to a key component must completely understand and accept his or her responsibility as a key custodian, and sign a key custodian form containing information about this responsibility. An example of a key custodian form:

- Last name, first name and middle name of security officer.
- Identification number and type of key.
- Key generation date (mm.dd.yy).
- Key expiry date (mm.dd.yy).
- Key component cleartext.
- Key component check value (if available).
- I completely understand and accept my key custodian responsibility including but not limited to:taking all necessary measures to prevent key components from being disclosed to any party, reporting immediately if such disclosure has occurred or suspected.
- Personal signature of security officer.

Any printed or recorded material that might disclose a component must be destroyed before an unauthorised party can obtain it.

Secret key components for the 3DES algorithm must be at least two double-length values and must be combined to form the actual key by such a process that no "active" bit of the key can be determined if even one of its components is missing.

An encryption key is created by automatically combining all entered key components inside the HSM. With regard to the 3DES algorithm, separate 32 (or 48) hexadecimal character components must be assembled using the bitwise exclusive 'OR' operation (XOR) to create a unique key.

Note that concatenated values do not satisfy this requirement.

Each full-sized hexadecimal character component, as well as the resulting key, must have a check value calculated for verification purposes according to the procedure defined for the particular cryptographic algorithm. For example, 3DES requires use of the entire 128 (192) bits in an Encrypt, Decrypt, Encrypt operation on zero-bits block, where the lowest-order five bytes of the resulting value are discarded and the highest-order three bytes are the check value.

Key Transfer

Secret keys can only be transferred in the following ways:

- By physically transmitting separate full-length components (hard copy, magnetic media, electronic device) using secure communication channels. This method is used to transmit "master" keys, i.e. keys used to encrypt other keys.
- By transmitting keys in encrypted form.

Key Storage

Keys may be stored in clear form inside a Hardware Security Module only. If it is necessary to store key components, they must be stored securely in the fewest locations and form possible. It is recommended that clear key components be destroyed immediately after using.

Restrict access to keys and key components to the fewest number of custodians necessary.

Key Revocation

Keys that are compromised or suspected of being compromised must be immediately revoked and changed. If a compromised key is a master key, all keys encrypted under the master key must be considered compromised.

Each key must have the following usage restrictions:

- Time frame, i.e. a key must be revoked and changed after its expiration date.

- Number of uses, i.e. a key must be revoked and changed when the current usage counter is equal to or above the limit.

To specify the maximum possible length of the period during which a key can be used, and to specify the maximum number of times a key can be used, it is necessary to comply with industry recommendations, for example, NIST Special Publication 800-57.

Key Deletion

All revoked or unused keys and their components must be securely deleted so that the keys or key components cannot be used after deletion.

Key Management Log

In the absence of automatic system tools for recording key management, each key management operation (generation, deletion, transfer and revocation) must be manually registered in the key management log by the responsible security officer. The following information must be logged:

- Last name, first name and middle name of security officer.
- Identification number and type of secure storage.
- Key generation date.
- Key expiry date.
- Type of action performed with the key.
- Personal signature of security officer.

Chapter 2. Secure Storage Key Management

Secure storage is used to protect data such as interchange files or stop lists sent from WAY4 to other systems. Secure storage is third-party software such as TrueCrypt or PGP Disk or hardware providing file system encryption. For the aforementioned applications, for PCI DSS compliance, it is recommended to use software using logical access organisation not depending on operating system access tools. The decryption key must not be bound to the operating system user record.

Key Generation

Keys must be generated according to the corresponding type of secure storage documentation conforming to the basic principles described in the "Basic Principles of Key Management" chapter. The best key generation method is random key generation without key output.

Key Transfer

No special procedure is necessary to transfer keys to other parties. Key transfer, if this option is supported by the secure storage used, must be performed in full accordance with the basic principles described in "Basic Principles of Key Management" chapter of this document.

Key Storage

In the case of an actual need, keys must be stored according to the principles described in "Basic Principles of Key Management" chapter of this document.

Key Revocation

Keys must be revoked and changed upon their expiration and at least annually. To determine when key revocation is necessary, use the security officer log. The simplest way to revoke and change keys is to re-initialise the secure storage after all data is deleted from it.

After a key is revoked, the corresponding record must be made in the security officer log.

Key Deletion

If key deletion is necessary for the used secure storage type, keys must be deleted according to the basic principles described in "Basic Principles of Key Management" chapter of this document.

Key Management Log

It is mandatory to keep a key management log for this key type (see the section "Key Management Log").

Chapter 3. Oracle Transparent Data Encryption Key Management

The Oracle Transparent Data Encryption mechanism allows sensitive data to be stored in encrypted form. See Oracle's documentation for details.

Key Generation

Keys must be generated according to the basic principles listed in section "Basic Principles of Key Management". Please refer to Oracle's documentation (see "Oracle Database Advanced Security Administrator's Guide 10g Release 2 (10.2)", Chapter 3 "Transparent Data Encryption") for details.

Key Transfer

It is not necessary to share keys with other parties, so this procedure is usually not used.

Key Revocation

Keys must be revoked and changed upon expiration and at least annually. To determine when key revocation is necessary, use the security officer log. After a key is revoked, the corresponding record must be made in the security officer log.

See Oracle's documentation for details.

Key Deletion

Keys must be deleted according to the basic principles described in "Basic Principles of Key Management" chapter of this document.

Key Management Log

It is mandatory to keep a key management log for this key type (see the section "Key Management Log").

Chapter 4. Terminal Key Management

The procedures for managing POS terminal and ATM encryption keys are described in the "Terminal Key Management Administrator Manual".