

# Terminal Key Management

# Contents

OVERVIEW	1
CHAPTER 1. BASIC PRINCIPLES OF KEY MANAGEMENT	2
Key Generation	2
Key Transfer	3
Key Storage	3
Key Revocation	3
Key Deletion	3
CHAPTER 2. TERMINAL KEY MANAGEMENT	4
Used Terminal Key Types	4
Storing Terminal Keys	4
Storing POS Terminal Keys	4
Storing ATM Keys	5
Key Generation	7
"Generate Key & Component Print"	8
"Generate Key & Split Print"	8
"Generate Key (No Printing)"	9
"Generate Device Key under KLK or TMK & LMK"	9
"Generate XOR Component"	9
"Verify KCV"	9
"DES Key Management" Pipe Parameters	10
Key Printing Templates	10
Variables Used in Key Printing Templates	11
Printing KCV on a PIN Mailer Containing the Last Component	12
Key Distribution	13
Key Revocation	13
Key Deletion	13



## Overview

The document describes the procedures for managing encryption keys in WAY4™ and is intended for WAY4 administrators overseeing ATMs and POS terminals.

While working with this document, it is recommended that users refer to the following reference material from OpenWay's documentation series:

- ATM Controller
- Acquiring Module User Manual

The following conventions are used throughout this document:

- Field labels in screen forms are typed in *italics*.
- Button labels used in screen forms are placed in square brackets, such as [Approve].
- Menu selection sequences are shown with the use of arrows, such as Issuing → Contracts Input & Update.
- Item selection sequences, in the system menu, are shown with the use of different arrows, such as Database => Change password.
- Key combinations used while working with WAY4 DB Manager are shown in angular brackets such as <Ctrl>+<F3>.
- The names of directories and/or files that vary for each local instance of the program are also displayed in angular brackets, like <OWS\_HOME>.
- Warnings of possible erroneous actions are marked with the  sign.
- Messages marked with the  sign contain information about important features, additional facilities, or the optimal use of certain functions of the system.

# 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 a specific key is more probable than others. For this reason, the secret key generation procedures use a hardware security module (HSM), which generates random secret key or secret key components at random.

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.

The output of the secret key generation process must be monitored by at least two authorised individuals (security officers) ensuring that there is no unauthorised part that might disclose an unencrypted secret key component as it is transferred between the hardware security module (HSM) and the device (printer) receiving the secret key or key component.

Printed key components must be printed within blind mailers or sealed immediately after printing so that only an authorised party can observe each component and tampering can be 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 printed or recorded material that might disclose a component must be destroyed before an unauthorised person 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 could be determined not knowing all of the components.

An encryption key is created by automatically combining all entered key components within an HSM. 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 32 (48) hexadecimal character component, as well as the resulting key, must have a check value calculated for verification purposes using the entire 128 (192) bits in an Encrypt, Decrypt, Encrypt operation on zero-bits block, whereby the resulting low order five bytes are discarded and the high 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 different 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 possible. It is recommended that clear key components be destroyed immediately after using.

## 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

## 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.

## Chapter 2. Terminal Key Management

This chapter describes the main points of terminal key management, which deals with keys used by POS terminals and ATMs for PIN encryption and MAC calculation. All keys are stored in a database in encrypted form. Keys are encrypted during key generation in a hardware security module (HSM).

### Used Terminal Key Types

Four types of terminal keys are used in WAY4:

- **TMK – Terminal Master Key.** This key is used to encrypt TPK and TAK keys inputted into a terminal or sent to it online.
- **TPK – Terminal PIN Key.** This key is used to encrypt PIN blocks sent by a terminal to the system.
- **TAK – Terminal Authentication Key.** This key is used to add a MAC code to messages that a terminal and the system exchange
- **Power-Up TPK – Power-Up Terminal PIN Key.** These are TPK and TAK values activated by an ATM after electricity is switched back on. This is an auxiliary value for the system, and it is not used during transactions processing.

The following conventions are used below:

- **LMK – HSM's local master key;**
- **LMK xx-yy – a pair of HSM's local master keys with numbers xx-yy.**

### Storing Terminal Keys

#### Storing POS Terminal Keys

Fig. 1 shows a diagram of POS terminal key storage.

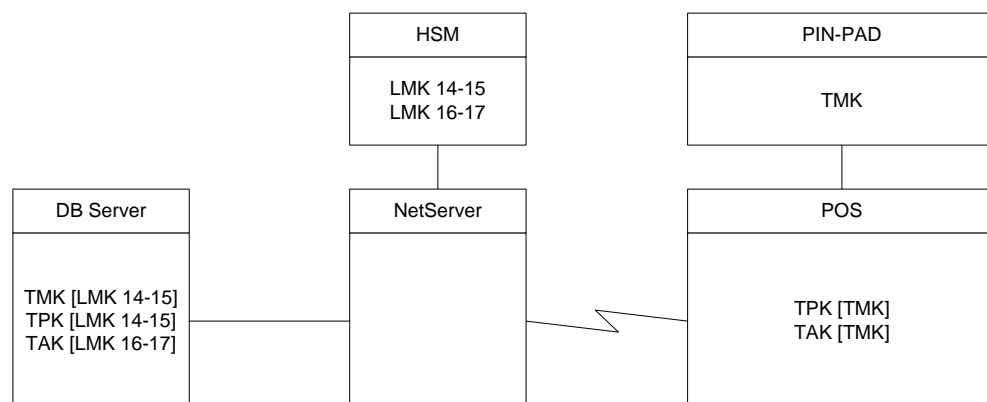


Fig. 1. Standard diagram of POS terminal key storage

The following mechanism is usually used in the system to store and generate terminal keys. Three keys must be generated for POS terminals: TMK, TPK and

TAK. All the keys encrypted under the corresponding LMK pairs are recorded in the database. The TMK in clear form is entered on the PIN pad, and the TPK and TAK encrypted under TMK are entered in the POS terminal. Terminal key storage and generation mechanisms may differ from the standard one and depend on the POS terminal type. In this case, refer to the documentation for the used POS terminal.

When a transaction is performed, the PIN pad encrypts the PIN block under TPK and signs the messages using TAK. TAK is also used to verify the signature of messages received from the system. The POS terminal sends TPK and TAK encrypted under TMK to the PIN pad, they are decrypted inside the PIN pad, and clear (non-encrypted) keys are never sent to the POS terminal.

**i** If dynamic key change is used for POS terminals, see the necessary system configurations in the POS Terminal Dynamic Key Change Setup in WAY4™ Administrator Manual.

The system processes a PIN block received from a POS terminal using the TPK key stored in the database. The PIN block and the encrypted TPK are sent to the HSM, which does the actual processing. The PIN block is processed inside the HSM entirely, and clear (non-encrypted) TPK and PIN block values are never sent to the system.

All keys encrypted under LMK and used by POS terminals are stored in the PM\_KEYS database table. The "Keys For <name of POS terminal>" form (see Fig. 2) is used for key management.

POS Management

Terminal ID: 12343652 Service Class: Unique Business Hours from: 09:09 to: 05:05

POS Type: Olivetti Default Curr: RUR Cut-Off Time: 10:10

POS Location: LOCATION2 MAC Status: None Time Offset: 4

Serial Number: SerialNumber2 PBT Status: None Device Status: OK

Ins Del Query Setup Operations Parm Enh Parm Keys

Keys for POS Hotels

Key Algorithm	Key Type	Key Name	DES Key	Key Check	Used as MK	Storage MK	Serial Number	Is Active
3DES ABA	Terminal Master Key	TMK1	U8787AD83781FF89012345FF7AC7	Yes				Active
3DES ABA	Terminal Authentication Key	TAK1	U8787AD83781FF67890123FF7AC7					Active
3DES ABA	Terminal PIN Key	TPK1	U8787AD83781FF12345678FF7AC7					Active

Ins Del Query Manage Key Options

Fig. 2. Form for entering POS terminal encryption keys

## Storing ATM Keys

Fig. 3 shows a diagram of ATM key storage.

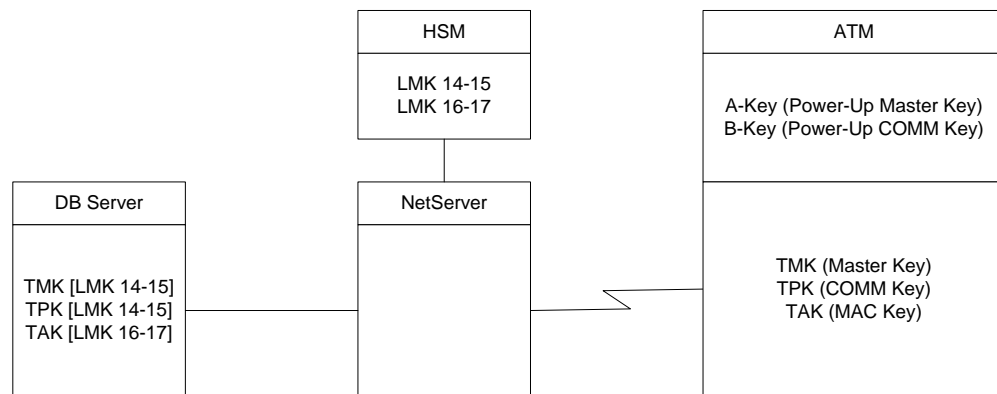


Fig. 3. Standard diagram of POS terminal key storage

For ATMs, it is necessary to manually generate and enter in the database one key only – TMK. The key is entered in the ATM cell "A-Key". The key is entered by security officers in clear (non-encrypted) form directly on the ATM's technological console. When an ATM is switched on, the ATM configuration copies the key to the ATM's master key, which is used as TMK during operation.

Each key component must be entered in the ATM cell by a different security officer. Depending on an ATM model, a key may consist of two or more components.

A security officer enters a full-length key component. For instance, when a single-length key is used, each security officer enters a component consisting of 16 hexadecimal digits.

When an ATM is switched on, it sends a "Power-Up Message" to the system. When the system receives this message, it sends TPK and TAK encrypted under TMK. The system also saves the sent TPK and TAK in the database encrypted in the HSM under the corresponding LMK pairs. The system never receives clear (non-encrypted) TPK and TAK values.

When a transaction is performed, an ATM encrypts a PIN block under TPK stored in the "COMM-Key" cell and signs the messages using TAK stored in the "MAC-Key" cell. TAK is also used to verify the signature of messages received from the system.

The system processes a PIN block received from an ATM using the TPK key stored in the database. The PIN block and the encrypted TPK are sent to the HSM, which does the actual processing. The PIN block is processed inside the HSM entirely, and clear (non-encrypted) TPK and PIN block values are never sent to the system.

If an encryption error (Response Code 88) occurs during interaction between an ATM and the system, the system must send new TPK and TAK values to the ATM. An encryption error occurs if TPK and TAK values stored in an ATM and in the system are for some reason different.

The system can also generate for an ATM default TPK and TAK. In this case, the values of the keys must be the same. A clear (non-encrypted) TPK/TAK value is entered in the ATM cell "B-Key". The key is entered by security officers in clear (non-encrypted) form directly on the ATM's technological console. The TPK/TAK value encrypted under the corresponding LMK pairs must be saved in the database in fields *TPK*, *TAK* and *Power-Up TPK*. When an ATM is



switched on, the ATM configuration copies the value of the "B-Key" cell to "COMM-Key" and "MAC-Key" cells, which are later used as TPK and MAC, respectively.

The ATM cell "VISA-Key" is not used during transaction processing.

All keys encrypted under LMK and used by ATMs are stored in the PM\_KEYS database table. The "Keys For <name of ATM>" form (see Fig. 4) is used for key management.

The screenshot shows the 'ATM Device Management' window. The top section contains various configuration fields: Terminal ID (5555555), Denominations, Online status, ATM Type (Diebold 1071ix), Global/Coin Limit, HS Service, ATM Location (NEW LOCATION), Cut-Off Time (23:59), Socket, Service Group, Time Offset, INW Address, Default Curr (EUR), MAC Status, Configuration, PIN Prevalidation (Optional), and ATM Status (OK). Below these fields is a tabbed interface with 'Query', 'Setup', 'Hardware', 'Operations', 'Messages', 'Cassettes', 'Parms', 'Enh Parms', and 'Keys' tabs. The 'Keys' tab is active, displaying a table of keys for terminal 1234567890. The table has columns: Key Algorithm, Key Type, Key Name, DES Key, Key Check, Used as MK, Storage MK, Serial Number, Is Active, and Date From. The table contains five rows of key data.

Key Algorithm	Key Type	Key Name	DES Key	Key Check	Used as MK	Storage MK	Serial Number	Is Active	Date From
3DES ABA	Terminal Master Key	TMK_test	U0123456789ABCDEF0123456789ABCDE	D5D44F	Yes				01/08/2009
3DES ABA	Terminal PIN Key	TPK_test	11111111111111111111111111111111	112233		TMK_test		Inactive	01/08/2009
3DES ABA	Terminal Authenticat	TAK_test	31111111111111111111111111111111	112233		TMK_test		Inactive	01/08/2009
3DES ABA	Terminal PIN Key	TPK_test	J22222222222222222222222222222222	112233					01/08/2009
3DES ABA	Terminal Authenticat	TAK_test	J42222222222222222222222222222222	112233					01/08/2009

Fig. 4. Form for entering ATM encryption keys

## Key Generation

In WAY4, keys are generated by the "DES Key Management" pipe. To start the key generation procedure, click the [Manage] button in the "Keys For <...>" form (see Fig. 2 or Fig. 4) and select the corresponding item from the context menu that appears.

The screenshot shows the 'DES Management Mode' dialog box. A context menu is open, listing several options: 'Generate Device Key under KLK or TMK & LMK' (selected), 'Generate Device Key under KLK or TMK & LMK', 'Generate Key & Component Print', 'Generate Key & Split Print', 'Generate Key (No Printing)', 'Generate XOR Component', and 'Verify KCV'. At the bottom of the dialog are 'Cancel' and 'Proceed' buttons.

Fig. 5. Form for selecting encryption key generation mode

The following key generation options are available:

- "Generate Key & Component Print" (see "Generate Key & Component Print");

- "Generate Key & Split Print" (see "Generate Key & Split Print");
- "Generate Key (No Printing)" (see "Generate Key (No Printing)");
- "Generate Device Key under KLK or TMK" (see "Generate Device Key under KLK or TMK & LMK");
- "Generate XOR Component" (see "Generate XOR Component");
- "Verify KCV" (see "Verify KCV");

The following mandatory key information must be entered in the form before key generation:

- Key type
- Key algorithm



It is strictly prohibited to share keys between terminals.

### "Generate Key & Component Print"

The "Generate Key & Component Print" mode is used to generate components of the same length as the key itself. Key components will be generated inside the HSM in clear form and printed out on the printer connected to the HSM. Then, the key of a specified length can be assembled from the components by executing the operation "bitwise exclusive OR". For this, the HSM assembles an open key from encrypted components and encrypts it under the corresponding LMK pair. Then, the encrypted key is saved in the database. The number of generated components is specified by the "KEY\_COMPONENTS" parameter (see ""DES Key Management" Pipe Parameters") or using the key type additional parameter "Num of XOR Components" (see "Key Printing Templates").

Components will be printed out in PIN mailers according to preconfigured templates (see "Key Printing Templates"). In this mode, a key is printed out successively: first, the first key component, then, the second key component, etc. All mailers containing key components must be kept by security officers and securely destroyed right after use.

### "Generate Key & Split Print"

The "Generate Key & Split Print" mode is used to generate single-length components of the key. Key components will be generated in clear form; then, the key of a specified length can be assembled from the components by concatenation. Components will be printed out according to preconfigured templates (see "Key Printing Templates"). Parameter "LAST\_PRN\_TEMPL\_FILE"(see ""DES Key Management" Pipe Parameters") cannot be specified in this mode since the printing template is the same for all key components.




Note that this method may only be used for obsolete terminals that do not support the XOR key assembly method. In "Generate Key & Split Print" mode, a part of a key is printed out as a key component, which does not comply with the basic key management principle of secure key generation.

## "Generate Key (No Printing)"

The "Generate Key & Component Print" mode is used to generate a key without printing it on the printer connected to HSM. To do so, HSM generates a random key of a specific type, and then encrypts it under the corresponding LMK pair. The encrypted key is then saved in the database.


## "Generate Device Key under KLK or TMK & LMK"

The "Generate Device Key under KLK or TMK & LMK" mode is used to generate a key and encrypt it under LMK and TMK. In this mode, two records are created for a key in the "Keys for <...>" form (see Fig. 2 or Fig. 4). Each of the records contains the key encrypted under the corresponding master key. Key components are not printed out in this mode.

 To encrypt keys under TMK, TMK must be generated in advance. Mark TMK as a master key; for this, select "Yes" in the *Used as MK* field of the "Keys for <...>" form (see Fig. 2 or Fig. 4). Also, to encrypt keys under TMK, select the generated master key in the *Storage MK* field.

## "Generate XOR Component"

The "Generate XOR Component" mode is used to generate components of the same length as the key itself. Key components will be generated in clear form; then the key of a specified length can be assembled from the components by executing the operation "bitwise exclusive OR". For this, the HSM assembles an open key from encrypted components and encrypts it under the corresponding LMK pair. Then the encrypted key is saved in the database. The number of generated components is specified by the "KEY\_COMPONENTS" parameter (see "'DES Key Management' Pipe Parameters") or using the key type additional parameter "Num of XOR Components" (see "Key Printing Templates"). The generated key and its check sum (KCV) will be saved in fields *DES Key* and *DES Key Check* of the "Keys for <...>" form (see Fig. 2 or Fig. 4) after the last key component is generated (see "Key Printing Templates").

 Note that for every call of the procedure only one key component is generated. Key components will be assembled after the last key component is generated and printed. The number of key components is determined by the "KEY\_COMPONENTS" parameter.

Components are printed out according to preconfigured templates (see "Key Printing Templates"). In this mode, a key is printed out componentwise: first, the first key component, then, the second key component, etc. All mailers containing key components must be kept by security officers and securely destroyed right after use.

## "Verify KCV"

The "Verify KCV" mode is used to verify the Key Check Value (KCV).

If the KCV in the *Key Check* field of the "Keys for <...>" form (see Fig. 2 or Fig. 4) differs from that calculated by HSM, the error message "Invalid Key Check Value <value> for Key <value>" will be displayed on the screen.

## "DES Key Management" Pipe Parameters

The following parameters may be specified for the "DES Key Management" pipe:

- "COMM\_PARAMS" – parameters of the network connection to the hardware encryption module (HSM) under TCP/IP
- "PRN\_TEMPL\_FILE" – path to the file containing a template for printing out a key component PIN mailer (see "Key Printing Templates")
- "LAST\_PRN\_TEMPL\_FILE" – path to the file containing a template for printing out a PIN mailer of the last key component (only used in modes "Generate Key & Component Print" and "Generate XOR Component")
- "KCV\_TEMPL\_FILE" – path to the file containing a template for printing out a key checksum PIN mailer (only used in modes "Generate Key & Component Print" and "Generate XOR Component" after the last component is generated). If the parameter is set to "NONE", a checksum is not printed out.
- "KEY\_COMPONENTS" – number of key components (only used in modes "Generate Key & Component Print" and "Generate XOR Component"). May be set to "2" or "3" (the default value is "3").

## Key Printing Templates

To print key components in PIN mailers, the corresponding templates must be configured. Key printing templates are configured in one of the following ways:

In the form "PM Key Type Options" (Full → Configuration Setup → Merchant Device Setup → Device Key Type Options), select the key type, click the [Options] button and in the "Options for <...>" form that opens (see Fig. 6), specify printing templates.

The screenshot shows two windows from a software application. The top window is titled "Device Key Type Options" and contains a table with three columns: Name, Code, and Owner Type. It lists three key types: Terminal Encryption Key (TEK), Terminal Master Key (TMK), and Terminal Offline PIN Key (TOPK). The "Terminal Master Key" row is selected. Below the table are buttons for "Ins", "Del", "Query", and "Options". The bottom window is titled "Options for Terminal Master Key" and contains a table with four columns: Key Type, Key Algorithm, Option Code, and Option Value. It lists five options for the Terminal Master Key, all using the 3DES ABA algorithm. The "Split Component Print Template" option is selected.

Name	Code	Owner Type
Terminal Encryption Key	TEK	Device
Terminal Master Key	TMK	Device
Terminal Offline PIN Key	TOPK	Device

Key Type	Key Algorithm	Option Code	Option Value
Terminal Master Key	3DES ABA	Num of XOR Components	3
Terminal Master Key	3DES ABA	KCV Print Template	Check Value : {[KCV]}-
Terminal Master Key	3DES ABA	XOR Component Final Print Template	-Clear DES Key Component {[COMPONENT_NUM]}, Key {[KEY_NAME]},
Terminal Master Key	3DES ABA	XOR Component Print Template	-Clear DES Key Component {[COMPONENT_NUM]}, Key {[KEY_NAME]},
Terminal Master Key	3DES ABA	Split Component Print Template	-Key part 1, Key {KEY_NAME}, Type {KEY_TYPE} Key Serial# {KEY_SER

Fig. 6. Setting key printing templates

In this form, select the encryption algorithm for this key type (*Key Algorithm* field), an additional parameter for the key type (*Option Code* field), and the value of the additional parameter (*Option Value* field). For key printing templates, the following additional parameters are used:

- "Num of XOR components" – number of key components (only used for "Generate Key & Component Print" and "Generate XOR Component" modes). The possible values are "2" or "3".
- "XOR Component Print Template" – template for printing a key component PIN mailer (only used for "Generate Key & Component Print" and "Generate XOR Component" modes).
- "XOR Component Final Print Template" – template for printing a PIN mailer for the last key component (only used for "Generate Key & Component Print" and "Generate XOR Component" modes).
- "KCV Print Template" – template for printing a key check value PIN mailer (only used for "Generate Key & Component Print" and "Generate XOR Component" modes after the last component has been generated).
- "Split Component Print Template" – template for printing a single-length key component (only used for the "Generate and Split Print" mode).
- A printing template must be stored in a file with the "\*.txt" extension.

Key printing template variables and examples of templates are shown in the section "Variables Used in Key Printing Templates".

During key generation, a search is made for a key printing template in the following way:

- First a search is made for the template configured in the "Options for <...>" form (see Fig. 6).
- If a key printing template is not set in the "Options for <...>" form, a check is made for the "DES Key Management" pipe parameters "PRN\_TEMPL\_FILE", "LAST\_PRN\_TEMPL\_FILE" and "KCV\_TEMPL\_FILE".
- If a template is not set in the "Options for <...>" form and pipe parameters are not set, the "Choose print template file" window will be displayed. Select a manually configured key printing template file in this window.

## Variables Used in Key Printing Templates

The following variables are used in the templates:

- "COMPONENT\_NUM" – number of key components to be printed out
- "KEY\_NAME" – key name
- "KEY\_SERIAL" – key serial number (not used for device keys by default); the field may be used to store additional key identification data
- "KEY\_TYPE" – key type
- "KCV" – key check sum
- "KEY\_OWNER\_TYPE" – key owner type
- "KEY\_OWNER\_ID" – key owner ID
- "DEVICE\_BANK" – bank to which the terminal belongs
- "DEVICE\_LOCATION" – terminal address

- "DEVICE\_CITY" – city where the terminal is located

Standard HSM fields (see HSM documentation) may also be used in templates.

An example of a template:

```
-  
Clear 3-DES Key Component [{COMPONENT_NUM}], Key [{KEY_NAME}], Type  
[{KEY_TYPE}]  
  
Key Serial# [{KEY_SERIAL}]  
  
Key Owner [{KEY_OWNER_TYPE}] , ID [{KEY_OWNER_ID}]  
  
Bank [{DEVICE_BANK}] Device City [{DEVICE_CITY}] Device Location  
[{DEVICE_LOCATION}]  
  
Component : [{^P}]  
-
```

### Printing KCV on a PIN Mailer Containing the Last Component

To print a key checksum (KCV) on a PIN mailer containing the last key component, edit the corresponding templates. It is necessary that the contents of two templates be printed on the same PIN mailer.

For this, leave all variables before "KCV" (excluding "KCV") in the template for printing out the PIN mailer of the last component and place the "KCV" variable and final indents in the template for printing out the key check sum.

Therefore, the template for printing out the last key component must not contain form feeds or line feed groups in the end:

```
-  
Clear DES Key Component [{COMPONENT_NUM}], Key [{KEY_NAME}], Type  
[{KEY_TYPE}]  
  
Key Serial# [{KEY_SERIAL}]  
  
Key Owner [{KEY_OWNER_TYPE}] , ID [{KEY_OWNER_ID}]  
  
Bank [{DEVICE_BANK}] Device City [{DEVICE_CITY}] Device Location  
[{DEVICE_LOCATION}]  
  
Component : [{^P}]
```

A key checksum printing template will be as follows:

```
Check Value : [{KCV}]  
-
```

Therefore, when the changes are made to templates, KCV will be printed on a PIN mailer together with the last key component.

## Key Distribution

Terminal keys are distributed as follows:

- Clear key components in tamper evident envelopes. Each envelope must have at least the following attributes:
  - Terminal ID
  - Key type
- Encrypted keys in a terminal configuration via third-party terminal management software
- Encrypted keys using the dynamic key exchange procedure provided by WAY4

## Key Revocation

Keys must be revoked in the following cases:

- A key is compromised or suspected of being compromised (emergency case)
- A key is expired (normal case)
- A key usage counter exceeds the key usage limit (normal case)

In any case, the key must immediately be revoked. If the key revoked emergently is a master key, all the keys encrypted using the master key must be emergently revoked, too. The revocation procedure is as follows:

Generate a new key of the same type

Distribute the key using the terminal's standard method

Delete the revoked key

For the dynamic key exchange option, keys are revoked automatically. For emergent key revocation, set its expiration date to the current date value or set the key usage counter to the maximal key usage value directly in the form.

## Key Deletion

All key material must be deleted if it is not used. Clear key components must be securely destroyed; encrypted keys must be deleted from the database using the "<Keys For...>" form.