Exporting Cryptographic Keys to Mastercard

Contents

Introduction

This document is intended for bank and processing centre employees responsible for exporting cryptographic keys to Mastercard, and for interaction with Mastercard On-behalf Key Management (OBKM).

When working with this document, it is recommended to refer to the following resources:

- "Configuring WAY4™ for Magnetic Stripe Card Issuing"
- "Configuring WAY4™ for Smart Card Issuing"
- "On-behalf Key Management (OBKM) Document Set"

The following notation is used in the document:

- Field labels in screen forms are shown in *italics*.
- Labels for screen form buttons are shown in square brackets, such as [Approve].
- Sequences for selecting user menu items are given using arrows, as in "Full → Issuing → Contracts Input & Update".
- Sequences for selecting system menu items are given using arrows in the following way: "Database => Change password";
- Key combinations in DB Manager are shown in angular brackets, for example <Ctrl>+<F3>.
- Variables that differ for each local computer, such as directory names, file names, and file paths are shown in angular brackets, for example <OWS_HOME>.
- Warnings about potentially hazardous situations or actions are marked with the ⚠ sign.
- Messages marked with the ℹ sign contain information about important features, additional options, or the best use of certain system functions.

Chapter 1. General Principles of Working with OBKM

Mastercard offers issuers a service (Mastercard On-behalf Key Management, OBKM), for checking the cryptographic values of cards and performing authorisation on behalf of the issuer. This service can be used, for example, if the production database (DB) is temporarily unavailable (due to failure or routine maintenance).

WAY4 supports a two-level mechanism for sending the issuer's keys to the payment system (Two-Level Key Hierarchy). This means that all the issuer's keys are encrypted by transport keys received from Mastercard, and then sent to the payment system.

To export keys to the payment system, the following setup is required:

- From open key components received from Mastercard, compile "BKAM" (Transport Key for Message Authentication) and "BKEM" (Transport Key for Encryption) transport keys.
- Generate an "OKEN" key (Network Key). This key will be used for PIN block or session key encryption/decryption. The value of this key should be entered in the NetServer configuration and in the interchange channel with Mastercard.
- For magnetic stripe keys ("CVK1", "CVK2" and "PVK") and smart card keys ("IMK_{ac}") specify additional parameters according to Mastercard requirements.
- Specify additional export parameters: the unique identifier of the issuer in Mastercard, the Key Management Centre (KMC) identifier, etc.
- Generate files with cryptographic keys and send them to the payment system.

Chapter 2. Exporting Cryptographic Keys

The "MC OBKM Export" pipe is used to export encryption keys (see ""MC OBKM Export" Pipe Parameters"). The appropriate settings must have been made in the WAY4 DB before export.

Registering Mastercard Transport Keys

Mastercard sends the issuer open components of the following transport keys:

- "BKEM" (Transport Key for Encryption) – this key is used to encrypt/decrypt keys.
- "BKAM" (Transport Key for Message Authentication) – this key is used for electronic signature of keys sent, i.e. message authentication with MAC (Message Authentication Code).

From the open key components the following keys must be compiled using the "FK" command of the cryptographic device (HSM) management console:

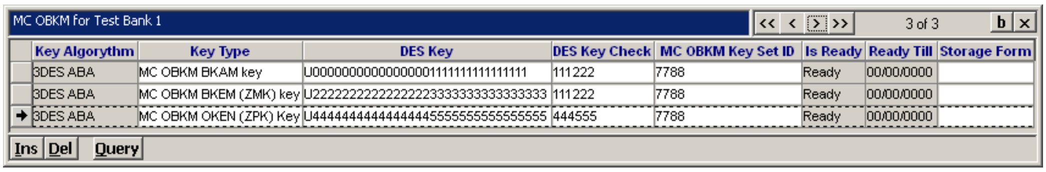
- "BKEM" – double-length "ZMK" (Zone Master Key). Specify "U" as the key scheme.
- "BKAM" – double-length "TAK" (Terminal Authentication Key). Specify "U" as the key scheme.

Moreover, for PIN block encryption/decryption, the "KG" command must be used to generate an "OKEN" key (Network Key) on the cryptographic device with. This is a double-length "ZPK" (Zone Pin Key). Specify "U" as the key scheme.

After the "BKEM", "BKAM" and "OKEN" keys encrypted under LMK of the cryptographic device are obtained, they must be registered in the database. To do so, click the [MC OBKM] button in the "Bank Production Parameters" form (Full → Configuration Setup → Card Production Setup → Bank Production Parameters).

As a result, the "MC OBKM for <…>" form will be displayed, to which three records should be added, specifying the values "MC OBKM BKAM key", "MC OBKM BKEM (ZMK) key" and "MC OBKM OKEN (ZPK) key" in the *Key Type* field. In the *DES Key* and *DES Key Check* fields, specify the value and checksum, respectively of the "BKAM", "BKEM" and "OKEN" keys. Moreover, in the *MC OBKM Key Set Id* field specify the unique identifier (four-digit number) received from Mastercard for these keys.

An example of registered transport keys is shown in Fig. 1.



	Key Algorythm	Key Type	DES Key	DES Key Check	MC OBKM Key Set ID	Is Ready	Ready Till	Storage Form
	3DES ABA	MC OBKM BKAM key	U00000000000000001111111111111111	111222	7788	Ready	00/00/0000	
	3DES ABA	MC OBKM BKEM (ZMK) key	U22222222222222223333333333333333	111222	7788	Ready	00/00/0000	
➔	3DES ABA	MC OBKM OKEN (ZPK) Key	U44444444444444445555555555555555	444555	7788	Ready	00/00/0000	

Fig. 1. Transport keys

Exporting Smart Card and Magnetic Stripe Card Keys

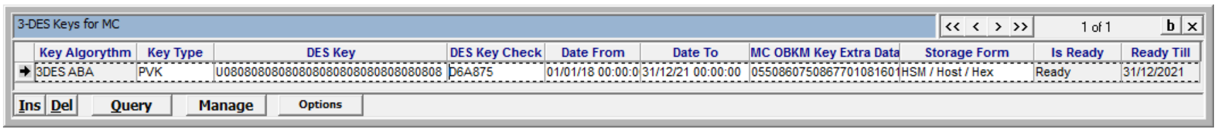
The following keys are exported to Mastercard:

- For magnetic stripe cards:
  - "PVK" (PIN Verification Key) – this key is used for online generation and verification of the PVV (PIN Verification Value).
  - "CVK1" (Card Verification Key) – this key is used for online generation and verification of CVC1 (Card Verification Code).
  - "CVK2" (Card Verification Key) – this key is used for online generation and verification of CVC2 (Card Verification Code). Note that this key is exported if the "Y" value is specified for the "EXPORT_CVK2" parameter of the "MC OBKM Export" pipe (see. ""MC OBKM Export").
- For smart cards the "IMK$_{ac}$" (Issuer Master Key for Application Cryptogram) is exported. This key is used for generation and verification of ARQC, ARPC and TC cryptograms. In WAY4 this key is registered as a "TC Master Key".
- The key for online verification of AAV (Mastercard SecureCode™ Accountholder Authentication Value) used in e-commerce systems for data exchange on the 3-D Secure protocol.
- For contactless cards "IMK$_{CVC3}$" (Issuer Master Key for CVC3) is exported. This key is used for online generation and verification of CVC3 (Dynamic CVC).

For each of the keys listed, additional parameters must be specified according to Mastercard requirements. To do so, in the "Parameters for <…>" form, opened by clicking the [Parameters] button in the "Bank Production Parameters" form (Full → Configuration Setup → Card Production Setup → Bank Production Parameters), select the required row and click the [3-DES Keys] button. In the "3-DES Keys for <…>" form that opens, specify additional parameters for each key being exported in the *MC OBKM Key Extra Data* field. The format of parameters depending on key type is described in the document "On-behalf Key Management (OBKM) Document Set". For example, for a "PVK" key, this field will contain 40 bytes of information: the response code if a PIN is entered incorrectly, PIN verification method, etc. Additional parameters can also be defined using the following "MC OBKM Export" pipe parameters (see ""MC OBKM Export" Pipe Parameters"); in this case, pipe parameter values have a higher priority:

- "EXTRA_PVK_DATA" – for "PVK" keys
- "EXTRA_CVK1_DATA" – for "CVK1" keys
- "EXTRA_CVK2_DATA" – for "CVK2" keys
- "EXTRA_CVK3_DATA" – for "IMK$_{CVC3}$" keys
- "EXTRA_TCMK_DATA" – for "IMK$_{ac}$" keys
- "EXTRA_CAVV_DATA" – for "AAVK" keys.

An example of filling in "3-DES Keys for <…>" form fields is shown in Fig. 2.



	Key Algorythm	Key Type	DES Key	DES Key Check	Date From	Date To	MC OBKM Key Extra Data	Storage Form	Is Ready	Ready Till
➔	3DES ABA	PVK	U08080808080808080808080808080808	D6A875	01/01/18 00:00:0	31/12/21 00:00:00	0550860750867701081601	HSM / Host / Hex	Ready	31/12/2021

Fig. 2. Additional key parameters

The *Date From* field of the "3-DES Keys for <…>" form must contain a value that is described in the "Floor Expiry Date" section of the document "On-behalf Key Management (OBKM) Document Set". The same value must be specified in this field for all exported keys.

The *Date To* field must contain the key expiry date that is used to generate an export file name according to the recommendations of the "Communication Requirements" section of the document "On-behalf Key Management (OBKM) Document Set". The same value must be specified in this field for all exported keys. The "AAVK" key is exported on the basis of parameters set in the "3-DES Keys for <…>" form (see Fig. 2). If parameters for this key are not set in the form, parameters set in the "DES Keys for <…>" form will be used to export the key. The "DES Keys for <…>" form is opened by clicking on the [DES] button in the "Bank Production Parameters" form. Parameters for the "AAVK_A" and "AAVK_B" DES keys must be set in the "DES Keys for <…>" form for export of the "AAVK" to be possible. On export, these components will be used to generate an "AAVK" 3-DES key.

For the 3-DES keys "PVK", "CVK1", "CVK2", "IMK_{ac}", "IMK_{CVC3}" and "AAVK", additional export parameters must be specified. These are set in the "Options for <…>" form, opened by clicking the [Options] button in the "Parameters for <…>" form, which in turn is opened by clicking the [Parameters] button in the "Bank Production Parameters" form (Full → Configuration Setup → Card Production Setup → Bank Production Parameters). In the "Options for <…>" form, specify the following parameters (select the parameter name in the *Option* field, and specify the value in the *Value* field):

- "MC OBKM KMC ID" – Key Management Centre (KMC) identifier received from the payment system. This is a two-digit number. The value can also be defined using the "MC_KMC_ID" pipe parameter (see ""MC OBKM Export" Pipe Parameters"); in this case, the value specified in the "Options for <…>" form will have a higher priority.
- "MC OBKM Member ID" – unique identifier of the issuer in the Mastercard key management centre. This is a 10-digit number. The value can also be defined using the "MC_KMC_MEM_ID" pipe parameter (see ""MC OBKM Export" Pipe Parameters"); in this case, the value specified in the "Options for <…>" form will have a higher priority.
- "MC OBKM Key Set Ref. M" – unique identifier of the magnetic stripe card key set ("PVK", "CVK1", and "CVK2") and contactless card "IMK_{CVC3}". This is a 4-digit number. This identifier must be changed each time a new key set is exported. The value can also be defined using the "KEY_SET_REF" pipe parameter (see ""MC OBKM Export" Pipe Parameters"); in this case, the value specified in the "Options for <…>" form will have a higher priority.
- "MC OBKM Key Set Ref. E" – unique identifier of the smart card key ("AAVK"). This is a four-digit number. This identifier must be changed each

time a new key is exported. If the parameter "MC OBKM Key Set Ref. E" is not specified, the parameter "MC OBKM Key Set Ref. M" will be used to export smart card keys.

- "MC OBKM Key Set Ref. P" – unique identifier of the smart card key ("IMK$_{\mathrm{CVC3}}$"). This is a four-digit number. This identifier must be changed each time a new key is exported. If the parameter "MC OBKM Key Set Ref. P" is not specified, the parameter "MC OBKM Key Set Ref. M" will be used to export smart card keys.

- "MC OBKM Key Set Ref. S" – unique identifier of the smart card key ("IMK$_{\mathrm{ac}}$"). This is a four-digit number. This identifier must be changed each time a new key is exported. If the "MC OBKM Key Set Ref. S" parameter is not specified, the parameter "MC OBKM Key Set Ref. M" will be used to export smart card keys.

- "MC OBKM AAVK Index" – "AAVK" key's unique six-digit identification number. A value can also be defined using the "AAVK_INDEX" pipe parameter (see ""MC OBKM Export" Pipe Parameters") however the value defined in the “Options for <…>” form will have a higher priority.

To export keys to Mastercard, click the [Parameters] button in the "Bank Production Parameters" form (Full → Configuration Setup → Card Production Setup → Bank Production Parameters). In the "Parameters for <…>" form that opens, select the required production parameters containing the keys being exported, click the [Manage] button and then select the "MC OBKM" item from the context menu. The "MC OBKM Mode" will be displayed (see Fig. 3).

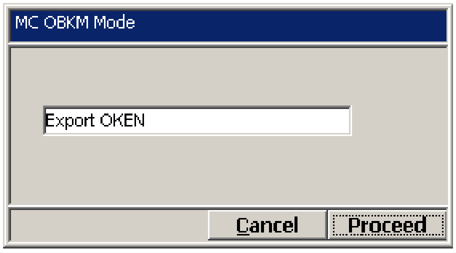


Fig. 3. Selecting key export mode

Key export modes are as follows:

- "Export OKEN" – export the "OKEN" (Network Key) used for PIN block encryption.

- "Export Mag Stripe Keys (MC PVV)" – export magnetic stripe card keys ("CVK1", "CVK2" and "PVK").

- "Export Chip Keys" – export a smart card key ("IMK$_{\mathrm{ac}}$").

- "Export PayPass MagStripe CVC3 Validation Key" – export a contactless card key ("IMK$_{\mathrm{CVC3}}$").

- "Export SecureCode AAV Validation Key" – export the "AAVK" key used for data exchange on the 3-D Secure protocol.

Export must be performed sequentially: first the item "Export OKEN" must be selected, next "Export Mag Stripe Keys (MC PVV)", and then"Export Chip Keys". The parameter "OUTPUT_DIRECTORY" can be used to specify the outgoing file directory. If the parameter is not specified, each time the pipe is run (export mode is selected), the user will be asked to select the directory for the corresponding file.

Keys are exported by the "MC OBKM Export" pipe. This pipe's parameters are shown in the section "MC OBKM Export".

⚠ Before exporting cryptographic keys ensure that a connection with the cryptographic device (HSM) is established for this workstation. The process for registering a cryptographic device in WAY4 is described in the section "Configuring Security Device Connection Parameters" of the document "Configuring WAY4™ for Magnetic Stripe Card Issuing".

The three files generated as a result of export must be sent to Mastercard.

"MC OBKM Export" Pipe Parameters

"MC OBKM Export" pipe parameters are shown in Table 1.

Table 1. "MC OBKM Export" pipe parameters

Parameter	**Value**	**Parameter description**
AAVK_INDEX	Six-digit number	"AAVK" key's unique identification number. The identifier’s format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set". The parameter's default value is "008001".
OUTPUT_DIRECTORY		Outgoing file directory. If the parameter is not set, when the pipe is started the user will be asked to select the directory in which the file will be put.
STORAGE_FORM		Method for saving keys. Determined by the HSM type. "HH" – Thales cryptographic device is used. "WH" – SafeNey cryptographic device is used.
MC_KMC_MEM_ID	Ten-digit number	Unique identifier of the issuer in the Mastercard KMC. The value may be redefined using the additional parameter "MC OBKM Member ID" (see "Exporting Smart Card and Magnetic Stripe Card Keys").
MC_KMC_ID	Two-digit number	The KMC identifier received from the payment system. The value may be redefined using the additional parameter "MC OBKM KMC ID" (see "Exporting Smart Card and Magnetic Stripe Card Keys").
MODE		This parameter determines the key export mode. Possible values: C – export a smart card key ("IMK_{ac}") D – export the "IMK_{CVC3}" key used for contactless cards M – export keys for magnetic stripe cards ("CVK1", "CVK2" и "PVK") O – export the "OKEN" key (Network Key) used for PIN block encryption S – export the "AAVK" key used for 3-D Secure data exchange @COMMAND_TEXT@ – export the key that was selected using the "MC OBKM Mode" form.

Parameter	Value	Parameter description
KEY_SET_REF	Four-digit number	Unique identification number of the set of keys for magnetic stripe or smart cards. This identifier must be changed each time a new set of keys is exported. The value may be redefined using the additional parameters "MC OBKM Key Set Ref. M", "MC OBKM Key Set Ref. E", "MC OBKM Key Set Ref. P", or "MC OBKM Key Set Ref. S" (see "Exporting Smart Card and Magnetic Stripe Card Keys").
EXTRA_CAVV_DATA	7 characters	Additional parameters for the "AAVK" key. Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK1_DATA	11 characters	Additional parameters for the "CVK1" key. Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK2_DATA	7 characters	Additional parameters for the "CVK2" key. Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
EXTRA_TCMK_DATA	104 characters	Additional parameters for the "IMK_{ac}" (TC Master Key). Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
EXTRA_PVK_DATA	40 characters	Additional parameters for the "PVK" key. Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK3_DATA	82 characters	Additional parameters for the "IMK_{CVC3}" key. Parameter format is determined by the payment system and described in the document "On-behalf Key Management (OBKM) Document Set".
OKEN_ROLE	"D" / "I"	The parameter determines how the "OKEN" key (Network Key) will be used. "D" – the key will be used for PIN block encryption/decryption. "I" – the key will be used for session key encryption/decryption. The default value is "D".
SM_ID		Name of the cryptographic device (HSM) registered in WAY4 that is used to export keys. The list of registered devices is available in the "Security Device" form (Full → Configuration Setup → Card Production Setup → Security Device).
EXPORT_PVK	Y/N	When this flag is set ("N" value) the "CVK2" key will not be exported to the payment system. The default value is "Y" ("PVK" will be exported).
EXPORT_CVK1	Y/N	When this flag is set ("N" value) the "CVK2" key will not be exported to the payment system. The default value is "Y" ("CVK1" will be exported).

Parameter	**Value**	**Parameter description**
EXPORT_CVK2	Y/N	When this flag is set ("Y" value) the "CVK2" key will be exported to the payment system. The default value is "N" ("CVK2" is not exported). Note that the Mastercard OBKM service does not verify "CVC2"; "CVK2" is only required if the issuer uses the Mastercard Emergency Card Replacement (ECR) service.