

Configuring WAY4™ for Magnetic Stripe Card Issuing

Contents

INTRODUCTION	1
CHAPTER 1. CONFIGURING THE HARDWARE SECURITY MODULE	3
Configuring Thales HSM in WAY4	3
Configuring SafeNet ProtectServer in WAY4	3
Configuring Hardware Security Module Connection Parameters	3
CHAPTER 2. CARD PRODUCTION PARAMETERS	8
Bank Production Parameters	8
Validation Parameters	9
Production Parameters	11
Encryption Keys	15
Configuring Key Parameters for Different HSM Configurations	21
PIN Mailers	23
Printing the PIN2 Value	25
Translating Keys between Two HSMs	27
Changing the Card Production Parameters within one PAN Range	28
Automatically Resetting the PIN Tries Counter when Reissuing a Card	28
CHAPTER 3. WORKING WITH PERSO BUREAUS	29
Registering a Perso Bureau	29
Generating Transport Keys	30
Pipes in which a Perso Bureau ID is Set	30
Default Perso Bureau	30

Introduction

The PIN Management Module is used to configure parameters for card personalisation (magnetic stripe and smart cards), generate and store encryption values, and create PIN mailer templates.

This document describes procedures set up for the issuing of magnetic stripe cards. Procedures for setting up smart card issuing are described in the document "Configuring WAY4™ for Smart Card Issuing".

The PIN Management Module functions from the workstation of a bank or processing centre connected to a hardware security module (HSM) that generates the necessary data for plastic personalisation. This HSM is also connected to a printer for printing PIN mailers.



This document is intended for WAY4 system administrators (employees of banks or processing centres) responsible for card production setup.

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

- DB Manager User Manual
- Menu Editor User Manual
- Issuing Module User Manual
- Configuring WAY4™ for Smart Card Issuing
- Products and Contract Subtypes
- Importing and Exporting Card Production Tasks in XML Format
- Installing and Configuring ProtectServer Control Module in WAY4™
- Exporting Cryptographic Keys to MasterCard.

This document uses the following conventions:

- Names of screen form fields are indicated in *italics*.
- Names of screen form buttons are encased in square brackets, for example [Approve].
- Sequences for selecting items from the user menu are given using arrows, as in "Issuing → Contracts Input & Update".
- Sequences for selecting items from the system menu are given using another type of arrow, as in "Database => Change password".
- Key combinations used when working with DB Manager are displayed in angular brackets, for example <Ctrl>+<F3>.
- Values such as directory and file names, as well as file paths which vary for each local instance of the program are also shown in angular brackets, as in <OWS_HOME>.

- Warnings that there is a risk of making an incorrect action 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. Configuring the Hardware Security Module

A hardware security module (HSM) must be installed in the system for encrypting data during data preparation and card personalisation.

WAY4 supports the following types of hardware security modules:

- Thales™ HSM 8000 and payShield 9000
- SafeNet™:
 - SafeNet ProtectServer Gold (PSG)
 - SafeNet ProtectServer External (PSE)
 - SafeNet PSE Refresh (with one COM port) in the mode for manually entering LMK without using a smart card.
 - SafeNet PSI-e (with one COM port) in the mode for manually entering LMK without using a smart card.
 - SafeNet PSE 2 in the mode for manually entering LMK without using a smart card.
 - SafeNet PSI-e 2 in the mode for manually entering LMK without using a smart card.

Configuring Thales HSM in WAY4

Detailed instructions on the installation and setup of the Thales HSM are given in "HSM 8000 Security Operations Manual" or "PayShield 9000 Installation Manual".

Configuring SafeNet ProtectServer in WAY4

Detailed instructions on the installation and setup of SafeNet HSMs are given in the document "Installing and Configuring ProtectServer Control Module in WAY4™".


Configuring Hardware Security Module Connection Parameters

To set up the connection between the PIN Management workstation and the hardware security module, select the menu path "Full → Configuration Setup → Card Production Setup → Security Device". This will invoke the "Security Device" form (see Fig. 1).

Fig. 1. Form for setting up the connection with the hardware security module

In this form, fill in these fields:

- *Device Name* – device name
- *Device Type* – device type
 - "HSM" – Thales™
 - "OWSEM" – SafeNet ProtectServer
- *Device Status* – device status; this field may contain the following values:
 - "Active" – activates the device entered in the form, if the entry is active this field will contain this value.
 - "Inactive" – used to deactivate the device.
- *Realignment* – number of PIN mailers that the printer will print before it automatically stops for users to realign the paper manually.


 By default, 10 is specified in this field. If it is not necessary to stop the printer to realign the paper, 0 should be specified in this field.
- *Version* – device software version
 - "HSM 5.04 Smart OW" – for SafeNet ProtectServer.
 - "HSM 8000 Smart" – for Thales™ HSM 8000
 - "HSM 8000 Smart & Perso" – for Thales™ HSM 8000 with Smart Card Issuer Firmware
 - "HSM 9000 Smart & Perso" – for Thales™ HSM 9000 with Smart Card Issuer Firmware
 - "HSM 9000 Contactless & EMV Issuing" – for Thales™ HSM 9000 with basic firmware (HSM9-LIC001 Base Firmware version 2.2a and higher) and license set "HSM9-LIC002 RSA License", "HSM9-LIC011

Magnetic Stripe Contactless Card Data Preparation License" and "HSM9-LIC016 EMV based Card Data Preparation License".

- *Debug Level* – level for logging information about tasks; possible values:
 - "0" – only error information is logged ("Error" level).
 - "1" to "49" – informational messages and error messages are logged ("Info" level).
 - "50" to "74" – debugging information is logged ("Debug" level).
 - "75" to "98" – more detailed debugging information is logged than for the "Debug" level. Dumps of commands sent to the HSM are not saved.
 - "99" (or higher) – all messages are logged, including dumps of requests and responses from the HSM.

Information about the location of message log files will be shown in the "Process Log" form (Full → Process Log → Process Log). For each process communicating with the HSM, the log will contain the message "Security Device Interaction Logs directory: <Path>". Note that these logs are temporary, i.e. they will only be in the directory until the client application (DB Manager / WAY4 Manager) has successfully completed operation.

- *Transparent Mode* – "Yes" is recommended in this field for compatibility with smart card issuing, along with further configuration of the HSM (see section "Configuring Thales HSM in WAY4 System" in the "Configuring WAY4™ System for Smart Card Issuing")
- *Protocol* – type of protocol through which the hardware security module is connected with the PIN Management module workstation:
 - "TCP/IP" – TCP/IP protocol
 - "Serial" – connection using an RS-232 interface
- *IP Address/IP Port* – fields which should indicate the IP (or DNS) address and port number for connection with the hardware security module if TCP/IP is used
- *Comm Port* – the sequential number of the workstation's port where the device is connected if a device with an RS-232 interface is used
- *Baud Rate* – drop-down list of values for indicating the baud rate
- The *Key1*, *Key2* and *Key File Path* fields are used for backward compatibility, it is not necessary to fill them in.
- *Encrypted PIN length* – encrypted PIN length value; the value in this field is determined as the maximum length of the PIN calculated on this device, plus one. For example, if cards with a PIN length of 4 or 6 digits are issued on this device, the value "7" must be specified in this field. If the field is not filled in ("0" value), the encrypted PIN length will be equal to "5". This parameter is only used for Thales devices (the "HSM" value is specified in the *Device Type* field); the field value must correspond to the value of the "Encrypted PIN length" parameter value specified on the device.

 This field must correspond to the value of the "Encrypted PIN Length" parameter specified in Thales HSM settings.

- *Message Header Len* – message identifier length; the message identifier is added to the beginning of all messages sent or received by the HSM. The value of this field must correspond to the value of the same parameter specified on the device. By default ("0" value), the identifier length is four digits.

Clicking the [Add Funct] button opens a context menu containing the following items:

- "Add Funct" – this item remains for backward compatibility.
- "Audit Upload" – used to export the audit log from the HSM. To view the audit log, click the [Audit] button in this form. The "Audit for <...>" form will be displayed (see Fig. 2).
- "Verify Audit" – verification of all messages contained in the exported audit log; i.e. electronic signing of each message and comparison of the obtained result with the value of the *Audit Record MAC* field in the "Audit for <...>" form (see Fig. 2).
- "LMK migration for Audit" – used to generate a new MAC (Message Authentication Code) signature for each message from the audit log if the LMK for the HSM was changed.
- "Load Default Weak PIN Table" – used to import a list of predefined "weak" PINs (for example "0000", "1111") to the HSM. These PINs will not be generated by the device. This menu item is only available for Thales devices and the corresponding mode for importing "weak" PINs must be enabled for import to the HSM to be possible.
- "Load Weak PIN Table" – used to import "weak" PINs to the HSM. These PINs will not be generated by the device. To generate a list, the following global parameters must be defined (Full → Configuration Setup → Main Tables → Additional Global Parameters):
 - "PM_PIN_LENGTH=<number>" – length of PINs in the list of "weak" PINS used when defining the global parameter "PM_WEAK_PIN_TABLE".
 - "PM_WEAK_PIN_TABLE=<list of values>" – defines the list of "weak" PINs (for example "0000", "1111"). The list contains "weak" PINs in open form. These PINs must not be generated by the HSM when generating new PINs. The values in the list are not delimited by spaces or commas; the length of each PIN is determined by the global parameter "PM_PIN_LENGTH". The maximum number of "weak" PINs is specified in the HSM's documentation. This menu item is only available for Thales devices and the corresponding mode for importing "weak" PINs must be enabled for import to the HSM to be possible
- "Test HSM" – used to test the workstation connection with the HSM.

The [Functionality] button of the "Security Device" form (see Fig. 1) remains for backward compatibility.

Clicking the [Audit] button opens the "Audit for <...>" form (see Fig. 2) containing the audit log; i.e. information about the execution of commands in the HSM.

Audit for HSM Thales 9000								<< >>		1 of 463	b	x
Audit Counter	Produce Date	Upload Date	Command Code	Command Code Type	Settings	Response Error Codes	Audit Record MAC	Random MAC Key				
→ 000001D2	15/08/14 16:12:15	15/08/14 21:02:09	EC	Fraud Event	9000	01	EEA0CCFD69401CBD	F3A578AD7A0106010				
000001D1	13/08/14 10:32:37	13/08/14 14:34:39	UT	User Action	D000	00	FB CD2F2FB75C2A62	AC885F6820EB6E1A4				
000001D0	13/08/14 10:32:04	13/08/14 14:34:39	UT	User Action	D000	00	D0786FAD33F8A672	0526CE448E7B5152C5				
000001CF	13/08/14 10:31:21	13/08/14 14:34:39	UT	User Action	D000	00	2D0A2544ED11FEB4	58668EFFAD00B93FE8				
000001CE	13/08/14 10:31:08	13/08/14 14:34:39	UT	User Action	D000	00	03DC18EA31E576D8	578E4E8255170FCF16				
000001CD	13/08/14 10:30:32	13/08/14 14:34:39	UT	User Action	D000	00	9AA1812FD58A1DCE	E9AA7D663F846737C				
000001CC	13/08/14 10:28:49	13/08/14 14:34:39	UT	User Action	D000	00	F0CDC01227621BBE	046899155AA5EC2931				
000001CB	13/08/14 10:03:40	13/08/14 14:34:39	UT	User Action	D000	00	0EF60266D796E151	93CAC889FA95B6950				
000001CA	04/08/14 16:41:02	05/08/14 13:11:02	A1	User Action	D000	00	0AABD3F427A9C493	3CD8259E4A0991F331				
Inrs	Del	Query	Verify									

Fig. 2. Audit log

The form contains a message counter, console command code and the date the command was executed in the HSM, export date, log message MAC signature and the key used to generate hash functions, etc. To verify a message, click the [Verify] button in this form. A MAC signature for the message will be generated and compared with the value in the *Audit Record MAC* field. If these values don't match, an error message will be displayed.

To verify all log messages, click the [Add Funct] button in the "Security Device" form (see Fig. 1) and select the "Verify Audit" item from the context menu. Note that the audit log is only created for Thales HSMs.

Chapter 2. Card Production Parameters

This chapter describes how to set up parameters for magnetic stripe card personalisation. For a description of how to set up parameters for smart card personalisation, read the "Configuring WAY4™ System for Smart Card Issuing" manual.

Bank Production Parameters

Bank production parameters may be set up through the "Bank Production Parameters" form (see Fig. 3), which is opened through the menu path "Full → Configuration Setup → Card Production Setup → Bank Production Parameters". Other forms accessed through the "Bank Production Parameters" form are also used.

Name	Bank Code	Branch Code	Phone	Contact With	Production Details
Test Bank 1	0001	0001		Mr. Manager	
Test Bank 2	0002	0002		Mr. Manager	

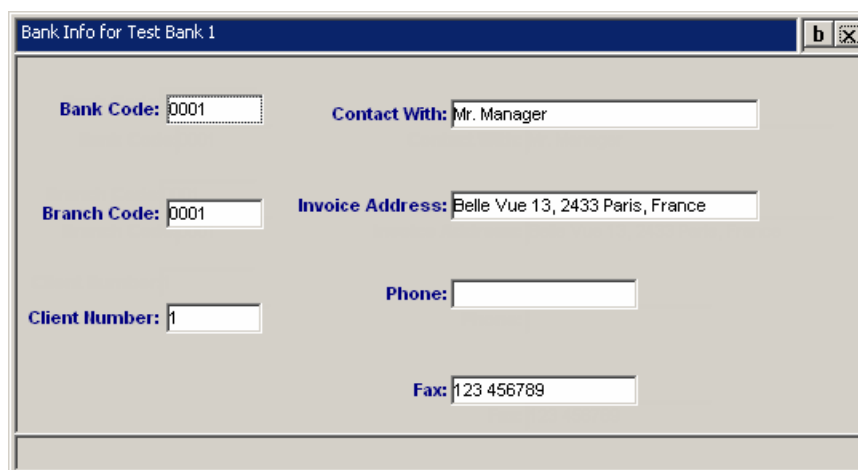
Buttons: Ins, Del, Query, Check, Parameters, Bank Info, Validation, CA Keys, MC OBKM, Certificates

Fig. 3. Form for configuring bank production parameters

This form contains the following fields:

- *Name* – name of bank for which cards are issued.
- *Bank Code* – bank code, an internal system parameter used to create production jobs, this ID may be used when creating personalisation data and its value must be the same as that in the *Bank Code* field of the "Financial Institutions" form ("Full → Configuration Setup → Main Tables → Financial Institutions").
- *Branch Code* – branch code (an internal system parameter). This ID is used by the PIN Management module and its value must be the same as that in the *Branch Code* field of the "Financial Institutions" form ("Full → Configuration Setup → Main Tables → Financial Institutions").
- *Phone* – contact phone number of the customer requesting card issuing.
- *Contact With* – contact person.
- *Production Details* – additional information.

Additional information about the customer bank may be indicated in the child form that appears after the user clicks the [Bank Info] button (see Fig. 4).



Bank Info for Test Bank 1

Bank Code: 0001 Contact With: Mr. Manager

Branch Code: 0001 Invoice Address: Belle Vue 13, 2433 Paris, France

Client Number: 1 Phone:

Fax: 123 456789

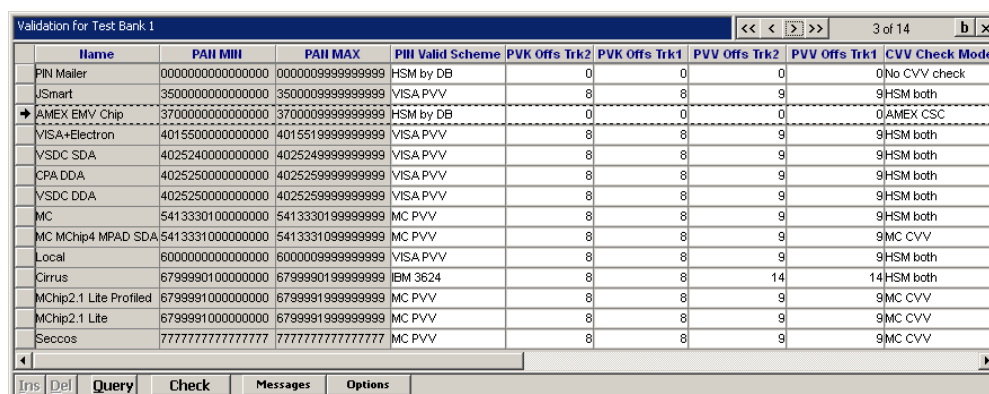
Fig. 4. Form for including additional bank information

Card production parameters are configured through child forms invoked through the "Bank Production Parameters" form. Buttons [CA Keys] and [Certificates] invoke forms used to set up smart card production parameters (see the document "Configuring WAY4™ for Smart Card Issuing").

The [MC OBKM] button is used to register transport keys when using the MasterCard On-behalf Key Management (OBKM) service. For more information, see the document "Exporting Cryptographic Keys to MasterCard".

Validation Parameters

To set up validation parameters, use the "Validation for <bank name>" form (see Fig. 5), invoked to the screen through the [Validation] button in the "Bank Production Parameters" form (see Fig. 3 in the section "Bank Production Parameters").



Name	PAN MIN	PAN MAX	PIN Valid Scheme	PVK Offs Trk2	PVK Offs Trk1	PVV Offs Trk2	PVV Offs Trk1	CVV Check Mode
PIN Mailer	0000000000000000	0000009999999999	HSM by DB	0	0	0	0	0/No CVV check
JSmar	3500000000000000	3500009999999999	VISA PVV	8	8	9	9	9/HSM both
AMEX EMV Chip	3700000000000000	3700009999999999	HSM by DB	0	0	0	0	0/AMEX CSC
VISA+Electron	4015500000000000	4015519999999999	VISA PVV	8	8	9	9	9/HSM both
VSDC SDA	4025240000000000	4025249999999999	VISA PVV	8	8	9	9	9/HSM both
CPA DDA	4025250000000000	4025259999999999	VISA PVV	8	8	9	9	9/HSM both
VSDC DDA	4025250000000000	4025259999999999	VISA PVV	8	8	9	9	9/HSM both
MC	5413330100000000	5413330199999999	MC PVV	8	8	9	9	9/HSM both
MC MChip4 MPAD SDA	5413331000000000	5413331099999999	MC PVV	8	8	9	9	9/MC CVV
Local	6000000000000000	6000009999999999	VISA PVV	8	8	9	9	9/HSM both
Cirrus	6799990100000000	6799990199999999	IBM 3624	8	8	14	14	14/HSM both
MChip2.1 Lite Profiled	6799991000000000	6799991999999999	MC PVV	8	8	9	9	9/MC CVV
MChip2.1 Lite	6799991000000000	6799991999999999	MC PVV	8	8	9	9	9/MC CVV
Secos	7111111111111111	7111111111111111	MC PVV	8	8	9	9	9/MC CVV

Fig. 5. Form for entering validation parameters

This form contains the following fields:

- *Name* – name indicating the type of issued card
- *PAN MIN*, *PAN MAX* – possible range of card numbers
- *PIN Valid Scheme* – drop-down list of PIN validation schemes:
 - "IBM 3624" – validation according to IBM3624 offset standard.

- "HSM by DB" – PIN validation based on the HSM PIN OFFSET value stored in the database.
- "VISA PVV" – PIN validation according to the PVV received in an online message from the card.
- "VISA PVV by DB" – PIN validation according to the PVV stored in the database.

If a PVV is not stored in the database, the PVV value stored on the card's magnetic stripe (Track 2) is used.

- "DEP PVV" – validation according to the DEP standard.
- "ESM PVV" – remains for backward compatibility.
- "MC PVV" – PIN validation according to the PVV received in an online message from the card. Differs from the "VISA PVV" method in the set of keys used.


If a PVV is not stored in the database, the PVV value stored on the card's magnetic stripe (Track 2) is used.

- "MC PVV by DB" – PIN validation according to the PVV stored in the database. Differs from the "VISA PVV by DB" method in the set of keys used.
- "VISA PVV PVKI by DB" – remains for backward compatibility.
- "Adaptive HSM or PVV by DB" – remains for backward compatibility.
- *PVK Offs Trk2* – position of PVKI (PIN Verification Key Index) on the second track of the magnetic stripe card
- *PVK Offs Trk1* – position of PVKI on the first track of the magnetic stripe card
- *PVV Offs Trk2* – position of PVV (PIN Verification Value) on the second track of the magnetic stripe card
- *PVV Offs Trk1* – position of PVV on the first track of the magnetic stripe card
- *CVV Check Mode* – drop-down list of CVV (Card Verification Value) check modes for VISA, CVC (Card Verification Code) for MasterCard; CSC (Card Security Code) for AMEX:
 - "HSM both" – verification of CVV1 and CVV2 on the HSM, where the expiry date for CVV1 verification is given in "YYMM" format, and for CVV2 validation in "MMYY" format
 - "HSM CVV1 only" – verification on the HSM of only CVV1 with the expiry date given in "YYMM" format
 - "By DB both" – verification of CVV1 and CVV2 by DB values
 - "HSM both, YYMM" – verification of CVV1 and CVV2 on the HSM, where the expiry date is given in "YYMM" format
 - "No CVV check" – no verification occurs

- "HSM Both, no DB CVV2" – verification of CVV1 and CVV2 on the HSM, where the expiry date for CVV1 verification is given in "YYMM" format, and for verification of CVV2 in "MMYY" format; this verification assumes that there is no CVV2 in the DB
- "HSM both, YYMM, no DB CVV2" – verification of CVV1 and CVV2 on the HSM, where the expiry date is given in "YYMM" format, this verification assumes that there is no CVV2 in the DB
- "MC CVV" – MasterCard CVV Verification
- "AMEX CSC" – AMEX CSC verification


 When selecting a value in the *CVV Check Mode* field, note that security standards prohibit the following:

- storing CVV in the DB.
- no CVV verification.

 The user is entirely responsible for the use of values like "HSM CVV1 only", "By DB both", and "No CVV check" in generating card verification parameters.

- *CVV Offs Trk2* – position of CVV1 on the second track of the magnetic stripe card
- *CVV Offs Trk1* – position of CVV1 on the first track of the magnetic stripe card
- *Encr PIN Format* – field reserved for future use
- *EMV Crypto Scheme*, *EMV MAC Scheme*, *EMV Encr Scheme* – fields used for smart card production according to recommendations in the "Configuring WAY4™ System for Smart Card Issuing" manual.

Production Parameters

 For keys and other production parameters to be defined correctly, it is recommended to set production parameters for the entire BINRange assigned to the bank or processing centre by the payment system.

To set up card production parameters, use the form "Parameters for <bank name>" (see Fig. 6), accessed by clicking the [Parameters] button in the "Bank Production Parameters" form (see Fig. 3 in the section "Bank Production Parameters").

Parameters for Test Bank 1											<< < > >>		4 of 14	b x
Name	Code	PAN MIN	PAN MAX	PIN Len	ICA	Card Type	Encoding Method	PVKI	Is Ready	Ready Till	Bank			
PIN Mailer	HH	0000000000000000	0000099999999999	4		Magnetic Card	PIN Mailer		Ready	00/00/0000	1			
JSmart		3500000000000000	3500099999999999	4	7777	JSmart	VISA	1	Ready	00/00/0000	1			
AMEX EMV Chip		3700000000000000	3700099999999999	4	2222	AMEX EMV	AMEX	1	Ready	00/00/0000	1			
VISA+Electron		4015500000000000	4015519999999999	4	3333	Magnetic Card	VISA	1	Ready	00/00/0000	1			
VSDC SDA		4025240000000000	4025249999999999	4	3333	VSDC	VISA	1	Ready	31/12/2012	1			
VSDC DDA		4025250000000000	4025259999999999	4	3333	VSDC	VISA	1	Ready	31/12/2012	1			
CPA DDA	CRA	4025250000000000	4025259999999999	4	3333	CPA	MC	1	Ready	31/12/2012	1			
MC		5413330100000000	5413330199999999	4	5555	Magnetic Card	MC	1	Ready	00/00/0000	1			
MC MChip4 MPAD SDA		5413331000000000	5413331099999999	4	2222	MCHIP	MC	1	Ready	31/12/2012	1			
Local		6000000000000000	6000099999999999	4	5555	Magnetic Card	VISA	1	Ready	00/00/0000	1			
Cirrus		6799990100000000	6799990199999999	4	5555	Magnetic Card	Local	1	Ready	00/00/0000	1			
MChip2.1 Lite		6799991000000000	6799991999999999	4	1111	MCHIP	MC	1	Ready	31/12/2012	1			
MChip2.1 Lite Profiled	PROFILED	6799991000000000	6799991999999999	4	1111	MCHIP	MC	1	Ready	31/12/2012	1			
Seccos		7171717171717171	7171717171717171	4	222	SECCOS	MC	1	Ready	00/00/0000	1			
Ins	Del	Query	Manage	PIN Mailer	EMV	IBM3624	DES Keys	3-DES Keys	RSA Keys	Certificates	Options	PIN2 Mailer	Commands	

Fig. 6. Form for configuring card production parameters

This form contains the following fields:

- *Name* – type of card issued
- *Code* – ID for the set of card production parameters, this field is the same as the *PM Code* field of the contract subtype (see "Card Contract SubTypes Form" in the "Products and Contract Subtypes" manual) and allows the set of card production parameters to be changed within the PAN range (see "Changing the Card Production Parameters within one PAN Range");
- *PAN MIN* – minimal PAN value
- *PAN MAX* – maximal PAN value
- *PIN Len* – PIN length
- *ICA* – ICA code of produced card
- *Card Type* – type of produced card:
 - "Magnetic Card" – card with magnetic stripe only
 - "VSDC" – VISA smart card
 - "MCHIP" – MasterCard smart card
 - "JSmart" – JCB smart card
 - "AMEX EMV" – AMEX smart card
 - "CPA" – CAP (Common Payment Application) smart card.
 - "SECCOS" – SECCOS (Security Chip Card Operating System) smart card.
 - "UICS" – UnionPay International (UPI) smart card.
- *Encoding Method* – field determining the set of parameters that will be considered and used when encoding the values written to the magnetic stripe and printed on the plastic or written to the smart card memory, select from a drop-down list of encoding standards.
 - "Local" – IBM3624 offset standard; card expiry date for calculating CVV1 is shown in "YYMM" format and for calculating CVV2 in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".

- "VISA" – VISA PVV standard; card expiry date for calculating CVV1 is shown in "YYMM" format and for calculating CVV2 in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".
- "VISA with iCVV" – VISA iCVV standard; card expiry date for calculating CVV1 is shown in "YYMM" format and for calculating CVV2 in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".
- "MC" – MasterCard PVV standard; card expiry date for calculating CVC1 and CVC2 is shown in "YYMM" format. The format of the date for calculating CVC2 can be redefined using the additional production parameter "MasterCard CVC2 MMYY".
- "MC PayPass" – MasterCard PayPass (contactless smart cards) standard; card expiry date for calculating CVC1 and CVC2 is shown in "YYMM" format. The format of the date for calculating CVC2 can be redefined using the additional production parameter "MasterCard CVC2 MMYY".
- "DEP VISA" – DEP standard for VISA; card expiry date for calculating CVV1 is shown in "YYMM" format and for calculating CVV2 in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".
- "DEP MC" – DEP standard for MasterCard; card expiry date for calculating CVC1 and CVC2 is shown in "YYMM" format. The format of the date for calculating CVC2 can be redefined using the additional production parameter "MasterCard CVC2 MMYY".
- "AMEX" – AMEX standard; the card expiry date for calculating CSC is shown in "YYMM" format.
- "VISA Virtual" – Visa Virtual standard (card for use in the Internet; this card contains only the card number, expiry date and CVV2); card expiry date for calculating CVV2 is shown in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".
- "MC Virtual" – MasterCard Virtual standard (card for use in the Internet; this card contains only the card number, expiry date and CVC2); card expiry date for calculating CVC2 is shown in "YYMM" format. The format of the date for calculating CVC2 can be redefined using the additional production parameter "MasterCard CVC2 MMYY".
- "UPI (CUP)" – UnionPay International standard; card expiry date for calculating CVV1 is shown in "YYMM" format and for calculating CVV2 in "MMYY" format. The format of the date for calculating CVV2 can be redefined using the additional production parameter "VISA indent CVV YYMM".
- "Custom Loyalty" – set of parameters for loyalty programme applications

- "Password List" – set of parameters for issuing a card containing a list of one-time passwords
- "PIN Mailer" – PIN mailer standard



For the values "Local", "VISA", "VISA with iCVV", "DEP VISA", "VISA Virtual" and "UPI (CUP)" it is possible to redefine the format of the date for calculating CVV2; to do so, click the [Options] button in this form and in the form that opens, add the parameter "VISA indent CVV YYMM". When the parameter value is "Y", the date will be shown in the format "YYMM", otherwise ("N", the default value) in "MMYY" format. Similarly, for the values "MC", "MC PayPass", "DEP MC" and "MC Virtual", the "MasterCard CVC2 MMYY" parameter can be defined. If the value is "Y", the date is specified in "MMYY" format, if "N" (default), in "YYMM" format.

- *PVKI* – fields for entering values necessary when using VISA PVV and MasterCard PVV standards.

Clicking the [Manage] button opens a context menu containing the following items:

- "Check" – calls a procedure to verify input data. If data was entered correctly, a window with the "Parameters Validated" message will open and the "Ready" value will be specified in the *Is Ready* field.
- "MC OBKM" – export keys to the MasterCard payment system (see the document "Exporting Cryptographic Keys to MasterCard").
- "Apply Profile" – import a card application parameter profile for a smart card (see the section "Configuring Card Applications" of the document "Configuring WAY4™ for Smart Card Issuing").
- "Translate Keys" – send keys (key translation) between various types HSM (see "Translating Keys between Two HSMs").

The [PIN Mailer] and [PIN2 Mailer] buttons are used to set parameters for printing PIN mailers and PIN2 mailers (see "PIN Mailers" and "Printing the PIN2 Value", respectively).

The [EMV] button is used to open a child form used to set up basic EMV application parameters.

The [IBM3624] button opens a child form used to set up parameters for IBM 3624 offset.

The [DES Keys] and [3-DES Keys] buttons are used to set DES key parameters (see "Encryption Keys").

The [3-DES Keys] and [RSA Keys] buttons open forms used to set up encryption key parameters used for smart cards (see the section "Encryption Keys" in the document "Configuring WAY4™ for Smart Card Issuing").

The [Options] button opens a form used to set up additional card production parameters.


The [Commands] button is used to set issuer script parameters (see the section "Configuring Issuer Scripts" of the document "Configuring WAY4™ for Smart Card Issuing").

Encryption Keys

To set up DES (Data Encryption Standard) encryption keys, use the form "DES Keys for <card product name>", or the form "3-DES Keys for <card product name>" (see Fig. 7), invoked from the "Parameters for <bank name>" form through the [DES Keys] button or the [3-DES Keys] button respectively in the "Parameters for <bank name>" form (see the "Card Production Parameters" section).

Key Algorithm	Key Type	DES Key	DES Key Check	Date From	Date To	MC OBKM Key Extra Data	Storage Form	Is Ready	Ready Till
3DES ABA	PIN Export Key	UDF1D258F4277C34B7129A0F9DEB9DCC4	30EDB4	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	PVK - 3DES	U1789DD53DC85A91EEC58576D0DBF538F	A0C111	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	CVK - 3DES	USC862FAB20EBF6217050803E85406C4F	76F4CE	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000

Fig. 7. Form for setting up DES key parameters

 Note that the HSM only exports/imports encryption keys in standard ANSI X9.17.

When producing magnetic stripe cards, the following 3-DES keys are used:

- "PVK" (PIN Verification Key) – this key is used for online generation and verification of a PVV (PIN Verification Value).
- "CVK" (Card Verification Key) – this key is used for online generation and verification of a CVV (Card Verification Value).
- "CVK2" – this key is used for online generation and verification of CVV2.
- "PEK" (PIN Export Key) – this key is used to encrypt a PIN during card personalisation, as well as when sending data from the PIN Management system to the electric personalisation subsystem.
- "ZPK" (Zone PIN Key) – this key is used to encrypt a PIN block when sending from the issuing module to PIN Management if PIN block translation is used.

It is recommended to generate DES keys using the "DES Key Management" pipe (see "Generating Keys"). While the pipe is running, the corresponding key generation commands will be sent to the HSM. The procedure for importing, exporting and generating keys for the Thales HSM 8000 hardware security module are described in the section "Host Commands" of the document "Host Security Module 8000. Host Command Reference Manual"; and for the payShield 9000 device, in the section "Host Commands" of the document "PayShield 9000 Host Command Reference Manual".

Generating Keys

Encryption keys are generated in the system using the "DES Key Management" pipe. When keys are generated this way, their parameters are automatically imported into the database and additional configuration of their parameters is not required.

Before starting key generation, in the "3-DES Keys for <name of card type >" form (see Fig. 7 in the section "Encryption Keys") select a key type from the list (*Key Type* field) and in the *Storage Form* field, select one of the following storage methods:

- "HSM / Host / Hex" – for keys generated on a Thales device.
- "HSM / Host / Keyblock Hex" – for Thales devices supporting "Keyblock" storage format. This format allows a key and all its attributes to be stored in a single block.
- "OWSeM / Host / Hex" – for keys generated on a SafeNet device.



It is strictly prohibited to use the same key for several card types.

To start the key generation procedure, click the [Manage] button in the "3-DES Keys for <name of card type>" form (see Fig. 7 in the section "Encryption Keys").

[Manage] Button

A context menu will be displayed, containing the following items:

- "Manage" – when this menu item is selected, the "PM DES Management Mode" form will be shown (see Fig. 8).

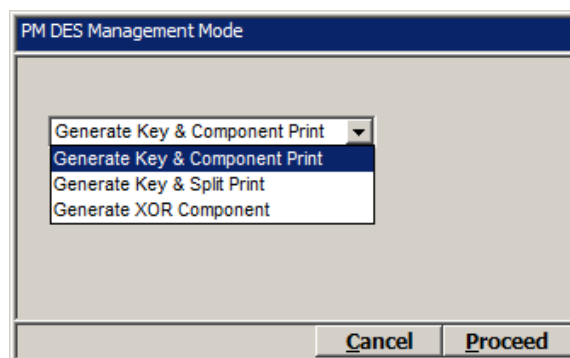


Fig. 8. Form for selecting DES key generation mode

One of the following key generation modes can be selected in this form:

- "Generate Key & Component Print" – generate a key and print components (see "Generate Key & Component Print" Option").
- "Generate Key & Split Print" – generate a key and separately print components.



It is not recommended to use this key generation mode; it has been left for backward compatibility.

- "Generate XOR Component" – generate components of the same length as the given key (see "Generate XOR Component" Option").
- "Verify KCV" – verify the key check value (KCV); see "Verify KCV" Option".
- "Generate Key (No Printing)" – generate a key without printing it (see "Generate Key (No Printing)" Option").

"Generate Key & Component Print" Option

The "Generate Key & Component Print" mode is used to generate components of the same length as the given key. Key components are generated within HSM in open form and printed on a printer connected to HSM, after which the key of the specified length can be assembled from the given components by executing the operation "exclusive OR" between them. To do so, HSM assembles a public key from encrypted components and encrypts it under the corresponding LMK pair. Then, the encrypted key is saved in the database. The number of components to be generated is set using the "KEY_COMPONENTS" pipe parameter (see "'DES Key Management' Pipe Parameters") or the "Num of XOR Components" key type additional parameter (see "Key Printing Templates").

Key components are printed in PIN mailers according to configured templates (see "Key Printing Templates"). In this mode, a key is printed component-by-component: first the first component of the key, then the second component, etc. All mailers with key components must be kept by data security officers and must be safely destroyed immediately after use.

"Generate Key (No Printing)" Option

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 XOR Component" Option

The "Generate XOR Component" mode is used to generate components of the same length as the given key. Key components are generated in open form and printed on a printer connected to HSM, after which the key of the specified length can be assembled from the given components by executing the operation "exclusive OR" between them. To do so HSM assembles a public 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 using the "KEY_COMPONENTS" pipe parameter (see "DES Key Management" Pipe Parameters") or the key type additional parameter "Num of XOR Components" (see "Key Printing Templates"). The generated key, as well as the key check value (KCV) will be entered into the fields *DES KEY* and *DES Key Check* fields, respectively, of the "3-DES Keys for <name of card type>" form (see Fig. 7 in the section "Encryption Keys") after the last component of the key is generated.



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 using the pipe parameter "KEY_COMPONENTS" or the key type additional parameter "Num of XOR Components".

Components are printed according to configured templates (see "Key Printing Templates"). In this mode, a key is printed component-by-component: first the first component of the key, then the second, etc. All mailers with key components must be kept by data security officers and must be safely destroyed immediately after use.

"Verify KCV" Option

The "Verify KCV" mode is used to verify the key check value (KCV) of the generated key. The algorithm for verifying the KCV is specified by the "KCV_ALG" parameter (see "DES Key Management" Pipe Parameters).

If the KCV in the *DES Key Check* field of the "3-DES Keys for <name of card type>" form (see Fig. 7 in the section "Encryption Keys") is different from that calculated using the HSM, an error message will be displayed.

"DES Key Management" Pipe Parameters

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

- "COMM_PARAMS" – used to specify parameters of the network connection with the HSM through the TCP/IP protocol.
- "PRN_TEMPL_FILE" – used to specify the path where the file is stored with the key component PIN mailer template file.
- "LAST_PRN_TEMPL_FILE" – used to specify the path where the file is stored with the template for printing the PIN mailer for the last component of a key (only used for the "Generate Key & Component Print" and "Generate XOR Component" modes).
- "KCV_TEMPL_FILE" – used to specify the path where the file is stored with the template for printing a PIN mailer with the key check value (used only for the "Generate Key & Component Print" and "Generate XOR Component" modes after the last component is generated). If the value of the parameter is set to "NONE", the key check value is not printed.
- "KEY_COMPONENTS" – this parameter specifies the number of key components (used only for "Generate Key & Component Print" and "Generate XOR Component" modes). The possible values are 2 or 3. The default value is 3.
- "KCV_ALG" – used to specify the algorithm for verifying the key check value (KCV) of the generated key. If the value of the parameter is "S", the algorithm for verifying the KCV for SECCOS cards will be used. If no value or any other value is specified, the standard algorithm for verifying the KCV will be used.

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 "PM Key Type Options" form (Full → Configuration Setup → Card Production Setup → PM Key Type Options), select a key type, click the [Options] button and in the "Options for <...>" form that opens (see Fig. 9), define printing templates.

The screenshot shows a two-part form. The top part is titled "PM Key Type Options" and contains a table with columns: Name, Code, and Owner Type. The bottom part is titled "Options for PVK - 3DES" and contains a table with columns: Key Type, Key Algorithm, Option Code, and Option Value.

Name	Code	Owner Type
PIN Encryption Key	PIN_KEY	Card Range
PVK 1	PVK1	Card Range
PVK 2	PVK2	Card Range
→ PVK - 3DES	PVKF	Card Range

Key Type	Key Algorithm	Option Code	Option Value
PVK - 3DES	3DES ABA	KCV Print Template	Check Value : {[KCV]}-
PVK - 3DES	3DES ABA	XOR Component Final Print Template	-Clear 3-DES Key Component {[COMPONENT_NUM]}, Key {[KEY_NAME]},
→ PVK - 3DES	3DES ABA	XOR Component Print Template	-Clear 3-DES Key Component {[COMPONENT_NUM]}, Key {[KEY_NAME]},

Fig. 9. Setting a key printing template

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

- "Num of XOR Components" – number of key components (only used for "Generate Key & Component Print" and "Generate XOR Component" modes). Possible values are "2" or "3".
- "XOR Component Print Template" – template to print a key component PIN mailer (only used for "Generate Key & Component Print" and "Generate XOR Component" modes).
- "XOR Component Final Print Template" – template to print a PIN mailer for the final component of a key (only used for "Generate Key & Component Print" and "Generate XOR Component" modes).
- "KCV Print Template" – template to print a PIN mailer for a key check value (only used for "Generate Key & Component Print" and "Generate XOR Component" modes after the last component has been generated).
- Printing templates must be stored in "*.txt" files.

Key printing template variables and sample templates are provided in the section "Key Printing Template Variables".

During key generation, a printing template is searched for as follows:

- First a search is made for the template configured in the "Options for <...>" form (see Fig. 9).
- If no key printing template is set in the "Options for <...>" form, a check is made for the "DES Key Management" pipe parameters PRN_TEMPL_FILE", "LAST_PRN_TEMPL_FILE", "KCV_TEMPL_FILE" and "KEY_COMPONENTS".
- If no template is set in the "Options for <...>" form and pipe parameters are not set, the "Choose print template file" window will be displayed, in which a manually created key printing template should be selected.

Key Printing Template Variables

The following variables are used in key printing templates:

- "COMPONENT_NUM" – the number of key components to be printed.
- "KEY_NAME" – key name.
- "KEY_SERIAL" – the serial number of the key (by default, this is not used for device keys); the field can be used to store additional identifying information about the key.
- "KEY_TYPE" – key type.
- "KCV" – key check value.
- "KEY_OWNER_TYPE" – key owner type.
- "KEY_OWNER_ID" – key owner ID number

Moreover, standard HSM fields can be used in templates (see HSM documentation).

Sample 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}]  
  
Component : [{^P}]  
-
```

Printing the Key Check Value (KCV) in a PIN Mailer with the Last Component

To print the key check value (KCV) in a PIN mailer with the last component of the key, the corresponding templates must be modified. Moreover, it must be possible for the contents of two templates to be printed in one PIN mailer.

To do so, in the template for printing the PIN mailer of a key's last component, leave all variables up to "KCV" (not including the "KCV" variable), and put the "KCV" variable and final indents in the template for printing the key check value,

Therefore, the template for printing the last component of a key must not contain a form feed or group of line feeds at the end:

```
-  
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}]
```

```
Component : [{^P}]
```

The template for printing the key check value will appear as follows:

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

```
-
```

Therefore, after making changes to the template files, the key check value (KCV) will be printed in a PIN mailer together with the last component of the key.

Configuring Key Parameters for Different HSM Configurations

To allow for functioning of the data preparation system and the online processing system, two independent HSMs can be used.

In the event that two or more Thales encryption devices are used in the system, it is recommended that the same set of Local Master Keys (LMK) be used for all devices.

In the event that devices of different vendors (e.g. Thales HSM and SafeNet ProtectServer) are used in the system, different sets of LMK are always used for these devices. While configuring the system, it is necessary to follow these recommendations:

- It is recommended that keys be generated on the HSMe of the data preparation and key management system; a key may also be received from the payment system (see the "Generating Keys" section).
- Key used to validate transaction information must be imported into the HSM of the online processing system (see the document "Transferring DES Keys between Thales™ HSM and SafeNet ProtectServer").
- For every key encrypted with LMKs of different encryption devices, two records in the "DES Keys for <...>" or "3-DES Keys for <...>" form must be manually entered:
 - A record for the key encrypted with the LMK of the data preparation and key management system HSM (if this record is not created automatically).
 - A record for the key encrypted with the LMK of the online processing system HSM.



If a key is imported into a Thales HSM with the Variant method (the "U" value is assigned to the "Key Scheme" parameter when importing the key), the "U" prefix must be added to the encrypted key value in the *DES Key* field of the "DES Keys for <...>" or "3-DES Keys for <...>" form.

- For each record, one of the following values must be specified in the *Storage Form* field:
 - "HSM / Host / Hex" – for a key encrypted with the Variant LMK of a Thales HSM.

- "HSM / Host / Keyblock Hex" – for a key encrypted with the Keyblock LMK of a Thales HSM.
- "OWSeM / Host / Hex" – for a key encrypted with the LMK of a SafeNet HSM.
- The "HH" value must be assigned to the AUTH_KEY_STORAGE_FORM global parameter.
- To re-encrypt the PIN under ZPK to LMK, specify the "Y" value for the "PM_PIN_TRANSLATE" global parameter. Moreover, in the "Options for <...>" form opened by clicking the [Options] button in the "Parameters for <name of financial institution>" form (see Fig. 6 in the section "Bank Production Parameters"), set the "Issuer PIN Format" parameter value to "UNDER_ZPK".
- In the "Produce Cards & PINs" pipe parameters (see the "Processing Jobs" section of the document WAY4™ Magnetic Stripe Card Issuing), it is necessary to specify, using the "STORAGE_FORM" parameter, what HSM is used by the data preparation and key management system:
 - "HH" – a Thales HSM.
 - "WH" – a SafeNet HSM.

As an alternative, the name of the HSM used in the system (the value of the *Device Name* field in the "Security Device" form – see the section "Configuring Hardware Security Module Connection Parameters") can be specified using the "SM_ID" parameter.



Note that the "Produce Cards & PINs" menu item definition consists of two sub-items. The "STORAGE_FORM" ("SM_ID") parameter value must be specified for both sub-items.

The system allows card issuing tasks to be processed simultaneously on several HSMs. This may be required when a large number of cards must be issued. For simultaneous processing on several devices, follow the instructions below:

- Use the same type of HSMs (for example, Thales).
- Use the same set of local master keys (LMK) for all devices.
- For the "Produce Cards & PINs Multithread" pipe that simultaneously processes card issuing tasks, specify the following device IDs:
 - For the first menu sub-item, use the "SM_ID" parameter to specify the IDs, separated by commas, of those HSMs that will be used to calculate encryption values.
 - For the second menu sub-item, use the "SM_ID" parameter to specify the ID of the HSMs to which the PIN mailer printer is connected.



Note that PIN mailers can only be printed on one device.

To start the process of simultaneously processing card issuing tasks, select the user menu item "Card Production on HSM pool → Produce Cards & PINs Multithread". Simultaneous processing of tasks is performed in the same way

as task processing for magnetic stripe card issuing (see the "Processing Jobs" section of the document WAY4™ Magnetic Stripe Card Issuing).

PIN Mailers

To set up PIN mailer parameters, use the "PIN mailer for <card product name>" form (see Fig. 10), invoked by clicking on the [PIN Mailer] button in the "Parameters for <bank name>" form (see the "Card Production Parameters" section).

Fig. 10. Form for setting up PIN mailer parameters

This form shows the type of information to be printed on the PIN mailer, and the curly brackets indicate the variables that will be replaced with values when printing the PIN mailer. Location of the information will correspond to the way it is displayed in the form.

When parallel printing mode is used (two PIN mailers are printed simultaneously), the "PIN mailer for <name of card product>" form must contain the data of both PIN mailers (see Fig. 11).

Fig. 11. Form for specifying printing parameters for parallel printing of two PIN mailers

In this case, variables whose values will be used when PIN mailers are printed are numbered successively (^0, ^1, etc.), and variables of the second PIN mailer have postfix "#2".

When setting up the PIN mailer format, the following variables may be used:

- "ICA_NUM" – ICA code of the issued card
- "SHORT_PAN" – short PAN (the last four digits of the full number)
- "EXP_DATE" – card expiry date
- "SERVICE_CODE" – card service code according to payment system

- "CARD_NAME" – cardholder name to be embossed on the card, for example, MR JOHN BROWN; this value is taken from the *Name* field of the "Plastics for <...>" form, opened from the card contract parameter form
- "COMPANY" – name of company shown in the corresponding client record field
- "COUNTRY" – country name specified in the corresponding client record field
- "CITY" – city specified in the corresponding client record field
- "ZIP" – postal code specified in the corresponding client record field
- "ADDRESS1", "ADDRESS2", "ADDRESS3", "ADDRESS4" – information about the address for delivering the PIN mailer. Information from the database will be used as variable values. These values can be redefined using the pipe parameters ("PINM_ADDR_LINE1_FMT", "PINM_ADDR_LINE2_FMT", "PINM_ADDR_LINE3_FMT", "PINM_ADDR_LINE4_FMT") exporting card production tasks to PIN Management and started using the menu item "Full → Issuing → Send / Receive Production Batches → PIN Management File Export". When specifying parameter data, variables whose list is provided in the section "List of Variables" of the document "Client Messages" can be used.
- "BRANCH_CODE", "BANK_CODE", "BANK_NAME" – parameters from the "Bank Production Parameters" table (see Fig. 3)
- "ADD_INFO_01", "ADD_INFO_02", "ADD_INFO_03", "ADD_INFO_04" – additional information, these are the values of parameters for the export pipe that sends production jobs to the PIN Management module and is run through the menu path "Full → Issuing → Send / Receive Production Batches → PIN Management File Export". It should be kept in mind that corresponding pipe parameters are indicated in the following format: ADD_INFO_1, ADD_INFO_2, etc. These parameters are set up when the menu item is edited (see the section "Pipe Type" in the document "Menu Editor")
- "PAN" – bankcard number
- "BIN_6D" – first 6 digits of the card number
- "CVV2" – CVV2 value of the issued card
- "JOB_NUM" – number of the job in which this card production task is located
- "SEQ_NUM" – sequence number of the card with the same PAN
- "ADD_FLD1", "ADD_FLD2", "ADD_FLD3", "ADD_FLD4" – additional information; these parameters are the same as the "ADD_INFO_01", "ADD_INFO_02", "ADD_INFO_03", "ADD_INFO_04" parameters and are values of the pipe exporting card production tasks to the PIN Management module.
- "PIN_S_FORM" – PIN Selection Form
- "^P" – PIN code value in four-digit format, for example, "1234"

- "^V" –PIN code value in text format for example, "ONE TWO THREE FOUR"
- "^Q" – PIN code value for the second PIN mailer in four-digit format, for example "1234", or the PIN2 value (see "Printing the PIN2 Value").
- "^W" –PIN code value for the second PIN mailer in text format, for example "ONE TWO THREE FOUR"
- "^T" – for Thales HSMs, the last six digits of the card number without a check position (without the last digit); for SafeNet ProtectServer – the last 12 digits of the card number without a check position.

The form "PIN mailer for <card product name>" may also indicate the escape sequence for the printer in the following format "|<L><hh hh hh...>", where:

- "|" – symbol with code 0x6a for ASCII or 0x7c for EBCDIC;
- "L" – hexadecimal value of the length of data that follows in bytes, the possible range of values is 0 – F
- hh – hexadecimal byte code

For example, a sequence of "|<A><01 02 03 04 05 06 07 08 09 0A>" will initiate sending 10 bytes of data to the printer with codes 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A.

Printing the PIN2 Value

The PIN2 cryptographic value can be printed in one of the following ways:

- Together with the PIN in one PIN mailer.
- In a separate PIN mailer within a separate Production Event for a card issued earlier.

To print the PIN2 value together with the PIN in one PIN mailer, do as follows:

- For the Production Event specified in the "Production Events" dictionary (Full → Configuration Setup → Transaction Types → Production Events), specify the tag "PTPIN2=Y;" in the *Add Prod Params* field.



Note that for joint printing of the PIN2 value, the "PTPIN2=Y;" tag must be specified for Production Events that involve printing of a PIN mailer; i.e. for which the value "Replace All", "Replace PIN" or "Reorder PIN" is specified in the *Production Type* field of the "Production Events" form.

- In the PIN mailer template (see "PIN Mailers") to print the PIN2 value, specify the "^Q" variable. An example of a template is shown in Fig. 12.

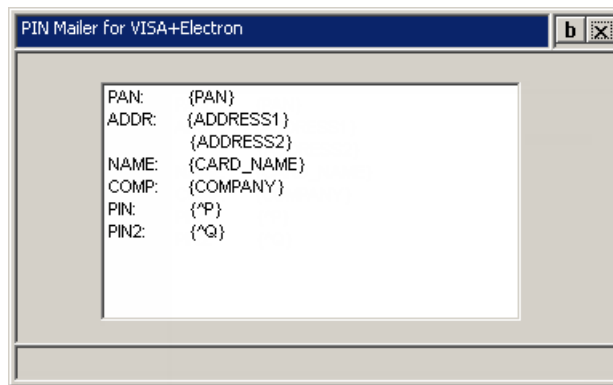


Fig. 12. Example of PIN mailer for printing PIN2 value



If it is necessary to disable printing the PIN2 value together with the PIN in one PIN mailer, not only should the "PTPIN2=Y;" tag be deleted from "Production Events" dictionary, but the "^Q" variable should also be deleted from the PIN mailer template. If only the "PTPIN2=Y;" tag is deleted without deleting the "^Q" variable, the mode will be enabled for parallel printing of two PIN mailers in one printer run and the value of the PIN for the second PIN mailer will be placed in this variable.

To print the PIN2 value in a separate PIN mailer within one Production Event, it is necessary to do the following:

- In the "Production Events" dictionary (Full → Configuration Setup → Transaction Types → Production Events) create a new Production Event, specifying the following parameters:
 - In the *Event* field, specify the "Replace Card" value.
 - In the *Production Type* field, specify the "Replace Add Parms" value.
 - In the *Add Prod Parms* field, specify the tag "PTPIN2=Y;".
- In the form "Parameters for <name of financial institution>" (see Fig. 6 in the section "Card Production Parameters"), click the [PIN2 Mailer] button and specify the "^P" variable in the PIN2 mailer template. An example of the PIN2 mailer template is shown in Fig. 13.

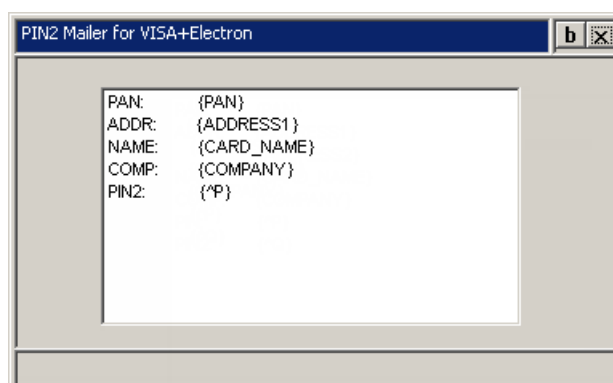


Fig. 13. Example of PIN2 mailer for printing PIN2 value



The same variables used to print a PIN mailer (see "PIN Mailers") can be used to print a PIN2 mailer, with the exception of "^Q".

Translating Keys between Two HSMs


In WAY4, automatic translation of 3-DES keys set for a certain card number range is possible between two different hardware security modules (from under the LMK of one device to under the LMK of another). Keys can be translated, for example, if a Thales device is used to process transactions online and a SafeNet device for card production.

To do so, click the [Manage] button in the "Parameters for <...>" form (see Fig. 5 in the section "Card Production Parameters") and select the "Translate Keys" context menu item.

To set up key translation, follow the instructions below (for a description of pipe parameters, see the section "KM DES Key Management" Pipe Parameters" of the document "Importing and Exporting Card Production Tasks in XML Format"):

- Ensure that the value "TRANSLATE_CARD_RANGE_KEYS" is specified for the "MODE" parameter of the "KM DES Key Management" key translation pipe.
- The identifiers of the first HSM (under the LMK of which encryption keys are encrypted) and the second HSM (under the LMK of which keys must be re-encrypted) must be specified for the "KM DES Key Management" key translation pipe. The identifiers are set, using the "SRC_SM_ID" and "DEST_SM_ID" parameters, respectively.
- For the "KM DES Key Management" pipe, using the "SRC_ZMK" and "DEST_ZMK" parameters, the ZMK (Zone Master Key) must be specified, encrypted, \under the LMK of the first and second HSM, respectively.
- For the "KM DES Key Management" pipe, using the "SRC_STORAGE_FORM" and "DEST_STORAGE_FORM" parameters, specify the key storage method for the first and second HSM, respectively. Note that parameter values for the first and second HSM must differ. For translated keys, the value of the parameter "DEST_STORAGE_FORM" will be specified in the *Storage Form* field of the "3-DES Keys for <...>" form (see Fig. 6 in the section "Encryption Keys").
- During translation of keys for the same range of card numbers records will be created corresponding to keys encrypted under the LMK of the second device (the identifier of which is specified using the pipe parameter "DEST_SM_ID"). Therefore, it is not recommended to translate keys between two devices of the same type since these keys (a key encrypted under the LMK of the first device and the same key encrypted under the LMK of the second device) will have the same *Storage Form* field value.
- Note that in addition to translation of double-length keys, single-length keys can also be translated: for two single-length keys "CVK A" and "CVK B", one double-length "CVK" key will be generated as the result of translation, which will be placed in the "3-DES Keys for <...>" form (see Fig. 6 in the section "Encryption Keys"); for two single-length keys "PVK 1" and "PVK 2" a double-length "PVK" key will be generated. The mode for translating single-length keys is defined by the pipe parameter "TRANSLATE_SINGLE_CVK_PVK".

Changing the Card Production Parameters within one PAN Range

 The settings described in this section should first be made in a test system. These settings can only be used in a production system if there are no errors.

To change the set of card production parameters within one PAN range (for example when issuing DDA (Dynamic DataAuthentication) standard cards instead of SDA (Static DataAuthentication) standard cards or when migrating to new verification parameters) the following settings are required:

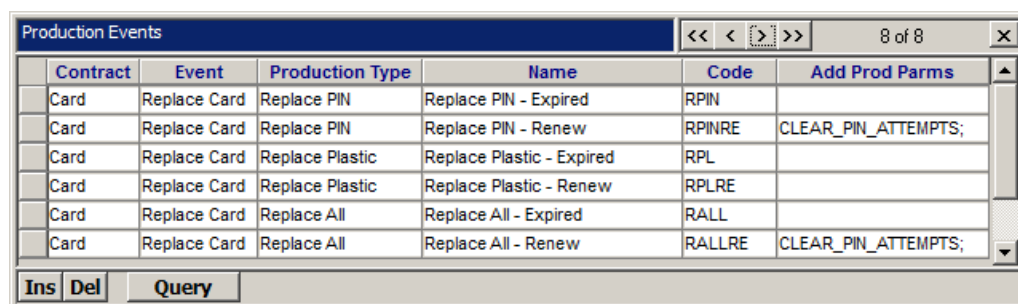
- In the "Parameters for <name of financial institution>" form (see Fig. 6 in the section "Production Parameters") create a new record, in the *PAN MIN* and *PAN MAX* fields of which the same values must be specified as for "old" production parameters, and in the *Code* field, specify the unique identifier of the parameter set.
- In the *PM Code* field of the "SubTypes for <card contract type name>" form (Full → Configuration Setup → Contract Types → Card Contract Types → [SubTypes]) specify the identifier of the new set of production parameters (value of the *Code* field from the previous step) for the subtype of those card contracts whose production parameters must be changed.

After these settings have been made, "old" cards (marked and issued before subtype settings were changed) during authorisation will use old card production parameters and "new" and reissued "old" cards will use the new card production parameters.

Automatically Resetting the PIN Tries Counter when Reissuing a Card

In WAY4, the PIN tries counter can automatically be reset when reissuing a card. The counter is reset when the response received from the PIN Management module is loaded into the issuing module.

For the counter to be automatically reset, in the "Production Events" handbook (Full → Configuration Setup → Transaction Types → Production Events) specify the "CLEAR_PIN_ATTEMPTS;" tag in the *Add Prod Parms* field for the Production Event. This tag should be specified for Production Events that involve printing a PIN mailer, i.e. for which the "Replace All", "Replace PIN" or "Reorder PIN" value is specified in the *Production Type* field of the "Production Events" form. An example of setup is shown in Fig. 14.




Contract	Event	Production Type	Name	Code	Add Prod Parms
Card	Replace Card	Replace PIN	Replace PIN - Expired	RPIN	
Card	Replace Card	Replace PIN	Replace PIN - Renew	RPINRE	CLEAR_PIN_ATTEMPTS;
Card	Replace Card	Replace Plastic	Replace Plastic - Expired	RPL	
Card	Replace Card	Replace Plastic	Replace Plastic - Renew	RPLRE	
Card	Replace Card	Replace All	Replace All - Expired	RALL	
Card	Replace Card	Replace All	Replace All - Renew	RALLRE	CLEAR_PIN_ATTEMPTS;

Fig. 14. Setup for automatic PIN counter reset

Chapter 3. Working with Perso Bureaus

A personalization bureau (perso bureau) is a hardware and software system used to personalize plastic. Cards are personalized based on parameters prepared in WAY4 (see "Card Production Parameters") and sent to the perso bureau. A client can personalize his or her cards in several perso bureaus. Data sent to a perso bureau are encrypted with transport keys:

- PEK (PIN Export Key) – key for PIN code encryption.
- KEK – (Key Encryption Key) – key for encrypting cryptographic values.

 Note that KEK is only used for smart card issuing.

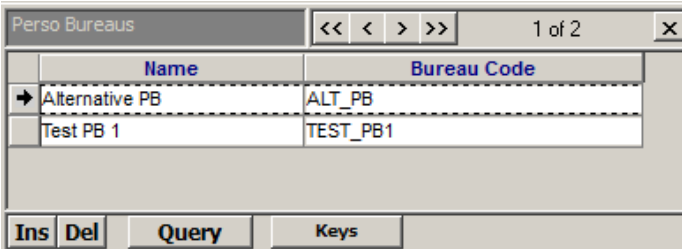
Each perso bureau has its own transport keys. Using one set of card production parameters (PM ParmS) and a specific perso bureau's transport keys, the process of personalizing cards in several perso bureaus at the same time is optimized.

The perso bureau used by default to personalize cards is defined for a financial institution's corresponding set of parameters (PM ParmS) (see the section "Default Perso Bureau").

Selection of a perso bureau when calculating cryptographic values, exporting a personalization file, etc., is based on the PBID pipe parameter. The perso bureau's code must be specified in the PBID parameter (see the section "Pipes in which a Perso Bureau ID is Set"). If the PBID parameter is not set in the pipe, the default perso bureau for PM ParmS is used.

Registering a Perso Bureau

The "Perso Bureaus" form contains a list of perso bureaus, menu item Full → Configuration Setup → Card Production Setup → Perso Bureaus (see Fig. 15).



Name	Bureau Code
Alternative PB	ALT_PB
Test PB 1	TEST_PB1

Fig. 15. List of perso bureaus

Fill in the fields:

- *Name*- perso bureau name.
- *Bureau Code* – perso bureau code.

The list of perso bureaus is stored in the PM_KEY_OWNER (OWNER_TYPE="PERSO_BUREAU") table.

Generating Transport Keys

Transport keys are generated in the standard way, using a hardware security module (see the section "Encryption Keys").

Transport keys are generated in the "Keys for < >" form (see Fig. 16) in the standard way (see the section "Generating Keys"). The "Keys for < >" form is opened by clicking on the "Keys" button in the "Perso Bureaus" form.

Keys for Test PB 1					<< < > >>		1 of 2		b x		
	Perso Bureau	Key Algorithym	Key Type	DES Key	DES Key Check	Storage Form					
→	1	3DES ABA	PIN Export Key	U7568FA7C8EB1C8A84A5290AA90ADCB7C	E2F243	HSM / Host / Hex					
	1	3DES ABA	Key Encryption Key	UA940CC330472671D0CDA49CCF19924DD	EE21F1	HSM / Host / Hex					
Ins		Del	Query		Manage		Options				

Fig. 16. PEK transport key

Pipes in which a Perso Bureau ID is Set

List of pipes in which a PBID is set:

- PM File Response Export – export of response files from the PIN Management module.
- PM Personalization File Export – generation of a personalization file (perso file) for cards.
- PM Security Calc&Mailer Printing – single-thread calculation of cryptographic values and PIN mailer printing.
- PM Security Calc (Multithread) – multithread calculation of cryptographic values.

For more information about pipes and their parameters, see the document "Importing and Exporting Card Production Tasks in XML Format".



The pipes listed below are only used for issuing smart cards:

- PM RSA ICC Keys Pre Generator – generation of RSA keys.
- PM RSA ICC Keys Pre Generator (Multithread) – multithread generation of RSA keys.

Default Perso Bureau

The default perso bureau is specified in card production additional parameters, menu item "Full → Configuration Setup → Card Production Setup → Bank Production Parameters → [Parameters] → [Options]" (see Fig. 17).

Bank Production Parameters												<< < > >>		1 of 1	
Name	Bank Code	Branch Code	Phone	Contact With	Production Details										
Test Bank 1	0001	0001		Mr. Manager	Test										

Ins	Del	Query	Check	Parameters	Bank Info	Validation	CA Keys	MC OBKM	Certificates		
Parameters for Test Bank 1											
<< < > >>											
Name	Code	PAN MIN	PAN MAX	PIN Len	ICA	Card Type	Encoding Method	PVKI	Is Ready	Ready Till	Bank
[Test]Main PayPass OW	TEST_MAIN_PP_OW	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Main PayPass Dc	TEST_MAIN_PP_ZPSM_O	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Main PayPass Dc	TEST_MAIN_PP_ZPSM_TH	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Sub PayPass OW	TEST_SUB_PP_OW	5555550000000000	5555559999999999	4	2222	MCHIP	MC PayPass	1	Ready	00/00/0000	1

Ins	Del	Query	Manage	PIN Mailer	EMV	IBM3624	DES Keys	3-DES Keys	RSA Keys	Certificates	Options	PIN2 Mailer	Commands	Bureau Keys
Options for [Test]Main PayPass OW														
<< < > >>														
Option	Value													
MC OBKM Key Set Ref. M	0077													
EMV Appl Priority Ind (tag 87)	01													
5F28 - Issuer Country Code	0643													
MC OBKM Member ID	1234567890													
ICC Keys To Gen	7													
MC OBKM KMC ID	77													
Validation Errors As Warnings	DDF1_NOT_0_CHAR,DDF2_NOT_0_CHAR													
Dynamic CVC/CVV Scheme	M													
ICC Key Format	PQ													
Track 2 Discr. Data Format	PV/KI+PV/V+*0*+*0000*+CVC1													
Track 1 Discr. Data Format	PV/KI+PV/V+*0*+*0000000*+CVC1													
Default Perso Bureau ID	TEST_PB1													
SYNC_ALLOWED	true													
Issuer PIN Format	UNDER_ZPK													
Chip CVC Present	Y													

Ins	Del	Query	Long Value
-----	-----	-------	------------

Fig. 17. Default personalization bureau for the Test Bank financial institution

Specify the following in the "Options" form for the required set of PM Params:

- *Option* – additional parameter "Default Perso Bureau Id".
- *Value* – code of the default perso bureau for the corresponding set of card production parameters.

Access to perso bureau transport keys is through the "Bureau Keys for < >" form (see Fig. 18) opened by clicking on the [Bureau Keys] button (see Fig. 17).

Bureau Keys for [Test]Main PayPass OW						<< < > >>		1 of 2	
Perso Bureau	Key Algorithm	Key Type	DES Key	DES Key Check	Storage Form				
253DES ABA		Key Encryption Key	C6351A596166E48CA687D56BB8D50796	EE21F1	OWSeM / Host / Hex				
253DES ABA		PIN Export Key	0B7DF6F9886A8C05053E65214C0342CD	E2F243	OWSeM / Host / Hex				

Query	Manage	Options
-------	--------	---------

Fig. 18. Personalization bureau transport keys

The [Manage] button is used for standard actions with keys (see the section "[Manage] Button").