Installation and Configuration Manual

Configuring WAY4 for Smart Card Issuing

03.49.30

16.03.2020

Contents

This document is intended for WAY4™ users, bank and processing centre employees responsible for configuring the data preparation system for smart card personalisation and key management.

WAY4 manages RSA Visa, MasterCard, JCB and AMEX keys as described in the following documents:

- Visa Certificate Authority User's Guide. VSDC and Visa Cash CEPS. Version 1.2.
- Registration Authority (RA) Interface Specification. Version: 2.1 – November 2000.
- JCB CA Interface Guide. Version 2.2 – February 2006.
- Amex CA Interface Specification. Amex AEIPS Chipcard Certificate Authority. August 2006.

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

- Risk Management
- ProtectServer Encryption Device Control Module: Description of Console Commands
- Electric Personalisation of Smart Cards Module: a User's Manual
- WAY4™ Data Preparation and Key Management Subsystem Main Technical Requirements.
- WAY4™ Magnetic Stripe Card Issuing
- Configuring WAY4™ System for Magnetic Stripe Card Issuing
- WAY4™ Products: Service Packages
- Products and Contract Sub-types
- DB Manager Manual
- Installing and Configuring ProtectServer Control Module in WAY4™
- Importing and Exporting Card Production Tasks in XML Format

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 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 about potentially hazardous situations or actions.

Messages with information about important features, additional options, or the best use of certain system functions.

1. Hardware Security Module Setup

To perform cryptographic operations while preparing data for personalising smart cards, a hardware security module (HSM) must be installed in the system. A detailed description of device types used as encryption hardware is provided in the document "WAY4™ Data Preparation and Key Management Subsystem Main Technical Requirements".

1.1 Configuring Thales HSM in WAY4 (Hardware Security Module Setup)

A detailed description of Thales devices using is provided in the "Encryption Hardware" section of the "WAY4™ Data Preparation and Key Management Subsystem Main Technical Requirements" document.

In WAY4, the form found at "Full → Configuration Setup → Card Production Setup → Security Device" is used to configure the Thales HSM. A detailed description of configuring parameters with the use of this form may be found in the "Configuring Connection between Workstation and Encryption Device" section of the Configuring WAY4™ System for Magnetic Stripe Cards Issuing Administrator Manual.

> ⚠ Note that "Yes" should be selected as the value of the *Transparent Mode* field of this form.

1.2 Configuring SafeNet ProtectServer Gold in WAY4

Detailed instructions for installing and configuring SafeNet ProtectServer Gold, ProtectServer External, PSE-Refresh and PSI-e devices may be found in the document "Installing and Configuring ProtectServer Control Module in WAY4™".

1.3 Configuring Gemalto Luna HSM

Detailed instructions on the installation and setup of Gemalto Luna HSMs are given in the documents package "SafeNet Payment HSM 2.2.0".

2. Stages of WAY4 Parameter Configuration for Smart Card Issuing

This chapter covers the rules for using parameter categories in card applications and the sequence for configuring card production parameters.

2.1 Card Production Parameter Categories

A card production parameter category is an indicator that allows the same set of parameters (tags) to be used in card applications for different interfaces (see the section "Card Applications"). Use of categories for cards with several applications makes it possible to simplify setup of a Product for production of these cards.

For example, two EMV applications are used to issue a card with a contact and contactless interface. Tag 82 (Application Interchange Profile (AIP)) is present in both applications. When a parameter belongs to a specific category, this makes it possible to set the required values for this parameter according to the interface.

Moreover, pursuant to the EMV specification, some parameters (for example, 9F50, 9F51, etc.) are configured according to payment system rules. Categories make it possible to use such tags according to these rules.

The following parameter categories are supported in the current version:

- EMVT – smart card production parameters. This category is used by default. If mandatory parameters for production are not set when preparing the data of other categories, this category's parameters are used by default.
- EMVC – contactless application (EMV contactless) parameters.
- MSDC – contactless application parameters for magnetic stripe cards.
- UISS – contactless application parameters for UnionPay International cards.

> The values of EMVC, MSDC, and UICC category parameters have a higher priority and redefine the values of EMVT category parameters.

> The WAY4 vender registers parameters and assigns them to categories.

An example of registering the ESDD parameter (Extended SDA DOL) for use in EMVC and MSDC categories is shown in Fig. 1.

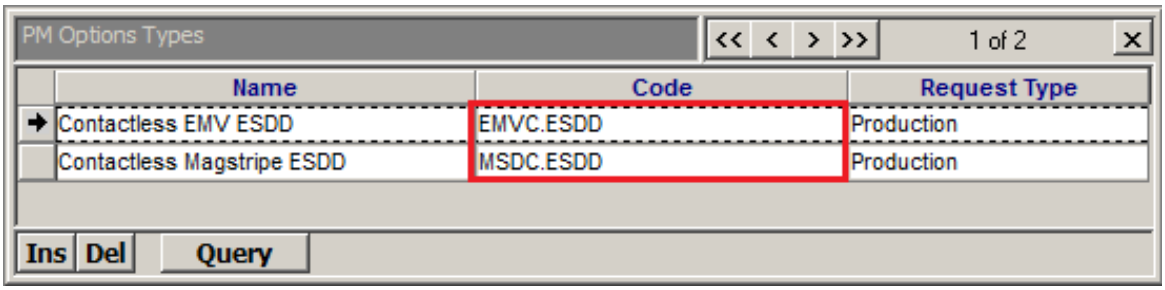


Fig. 1. Example of registration, making it possible to use the ESDD tag for applications with the EMVC and MSDC parameter categories

A specific category's set of parameters with which the EMV application will work is determined when creating a Risk Scheme. The parameter category is shown in the *Category* field of the "ParmType for Parms for <Risk Scheme name>" form (see Fig. 10). An example of Risk Scheme setup is shown below (see the section "Example of Configuring a Risk Scheme for EMVC Category Parameters").

The values of parameters used as additional card verification parameters, for example, ESDD (Extended SDA DOL) shown in Fig. 1 are set in the "Options for <parameter name>" form (see Fig. 16).

2.2 Parameter Configuration Sequence

Configuration of WAY4 parameters for smart card issuing includes the following stages:

- Creating smart card Risk Schemes based on an existing template (see "Smart Card Risk Schemes).
- Assigning a Risk Scheme to a contract (see "Defining Smart Card Risk Schemes").
- Setting smart card production parameters and validation parameters for a financial institution (see "Configuring Smart Card Issuing for Financial Institutions").
- Defining card application parameters and, when necessary, configuring several card applications (see "Card Applications").
- Generating and configuring encryption key parameters: 3-DES keys (see "3-DES Keys") and RSA keys (see "RSA Keys").
- After parameters have been configured, issue smart cards. The smart card issuing process is identical to the process for issuing magnetic stripe cards (see the document "WAY4™ Magnetic Stripe Card Issuing").

3. Smart Card Risk Schemes

Smart card Risk Schemes are sets of transactional restrictions, that is, parameters written into the microchip memory while a card is being personalised. These parameters may also be written into microchip memory with the use of issuer scripts (see "Issuer Scripts"). The restrictions in question may include the allowable number of PIN entry attempts, the maximal allowable transaction amount, etc.

3.1 Defining Smart Card Risk Schemes

When smart cards are being issued, a Risk Scheme must be assigned to each card contract. A Risk Scheme may be assigned at the following levels:

- At the Service Package level – in the *Chip Scheme* field (see the "Additional Parameters of Service Packages" section of the document "WAY4™ Service Packages"). In this case, one scheme will be shared by all contracts using the same Service Package.
- At the card contract level – in the *Chip Scheme* field of the "Risk / Chip for <contract name>" form invoked by clicking the [Risk / Chip] button in any of the forms used to configure contracts (see the Issuing Module User Manual).

If a contract is assigned Risk Schemes at both the Service Package and Contract levels, the scheme assigned at the Contract level prevails.

3.2 Creating Smart Card Risk Schemes

Risk Schemes are created on the basis of their templates. A Risk Scheme template is a set of parameters allowed for use when creating Risk Schemes.

The use of any parameters other than those included in the template used to create a Risk Scheme is inadmissible.

Risk Scheme templates are created by the system vendor.

Risk Scheme templates are accessed through the "Chip Schemes Templates View" grid form (see Fig. 2) invoked by selecting the "EMV Smart Cards → Configuration → Chip Schemes Templates View" user menu item.

Chip Schemes Templates View << < > >> 1 of 30

Name
VSDC 1.3.2 Generic Easy Setup
Proprietary
VSDC 1.4.0 Generic Easy Setup
MCHIP 4 MPAD
MCHIP 2 Lite Generic Easy Setup
NonChip
Custom Preauthorized
Custom Loyalty
VSDC 1.3.2 Generic
VSDC 1.4.0 Generic
MCHIP 2 Lite Generic
MCHIP 4 Generic with PayPass
AEIPS Generic Easy Setup
JSmart Generic
VSDC 1.4.0 VPA full for Native
VSDC 1.4.0 VPA for GP applet
CPA OnLine Generic
SECCOS 6 Generic
URPS Biometric Verification
MCHIP 4 URPS BPAD

Ins Del Query Parameters

Fig. 2. Smart card Risk Scheme templates

The *Name* field of this form specifies the name of the Risk Scheme template.

Parameters included in a Risk Scheme template may be viewed in the "Parameters for <template name>" grid form (see Fig. 3), which is invoked by selecting a row in the "Chip Schemes Templates View" grid form and then clicking the [Parameters] button in it.

Parameters for MCHIP 4 MPAD << < > >> 1 of 40

Parm Type	Parm Value	Parm Status
CATE00	000000080000	Optional
TOPUP_AMOUNT_BAL_TYPE		Optional Changeable
AUTO_TOPUP_MODE	LAST_OK	Optional Changeable
CAPN00	000000200000	Optional
APPROVE_ONLINE_TRANS	0010	Optional
DECLINE_ONLINE_TRANS	0000	Optional
9F42	000	Mandatory Changeable
9F44	0	Optional Changeable
C7	00	Mandatory Changeable
C8	000	Optional Changeable
PTLM	0	Mandatory Changeable

Ins Del Query

Fig. 3. Set of parameters in a smart card Risk Scheme template.

The form contains the following fields:

- *Parm Type* is the parameter type.
- *Parm Value* is the parameter default value.
- *Parm Status* is the parameter status. The statuses are as follows:
- "Mandatory" means that the parameter must be included in the Risk Scheme and its value must not be edited.
- "Mandatory Changeable" means that the parameter must be included in the Risk Scheme, while its value may be edited.
- "Optional" means that the parameter may be optionally included in the Risk Scheme, yet its value must not be edited.
- "Optional Changeable" means that the parameter may be optionally included in the Risk Scheme, and its value may be edited.

3.3 Configuring Smart Card Risk Schemes

The "Chip Schemes" form (see Fig. 4) is used to configuring smart card Risk Schemes. It opens when the "EMV Smart Cards → Configuration → Chip Schemes" menu item is selected.

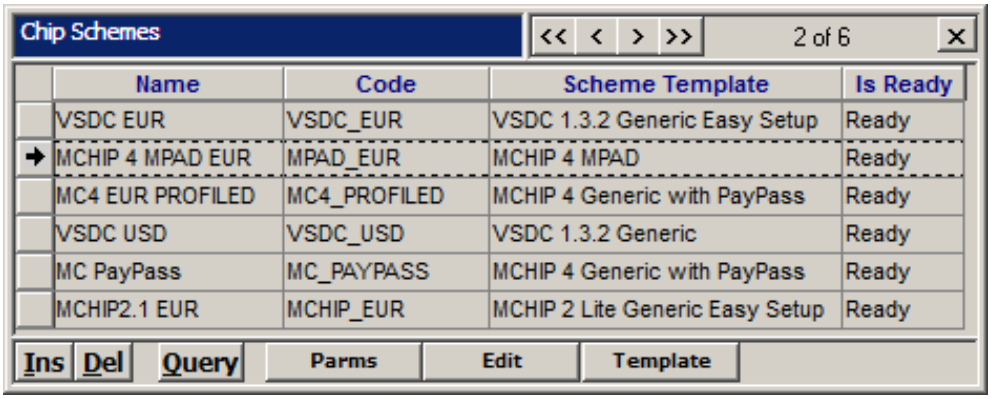


Fig. 4. Form for defining smart card Risk Schemes

The form contains the following fields:

- *Name* – the name of the Risk Scheme.
- *Code* – a user-assigned code that, further on, is used to identify the Risk Scheme.
- *Scheme Template* is the template on whose basis the Risk Scheme has been created.
- *Is Ready* – specifies whether the Risk Scheme has been approved.

To create a new Risk Scheme, add a new entry to the "Chip Schemes" form by clicking the [Ins] button in it. After that, select the new entry and click the [Edit] button. The "Edit for <Risk Scheme name>" form will open (see Fig. 5).

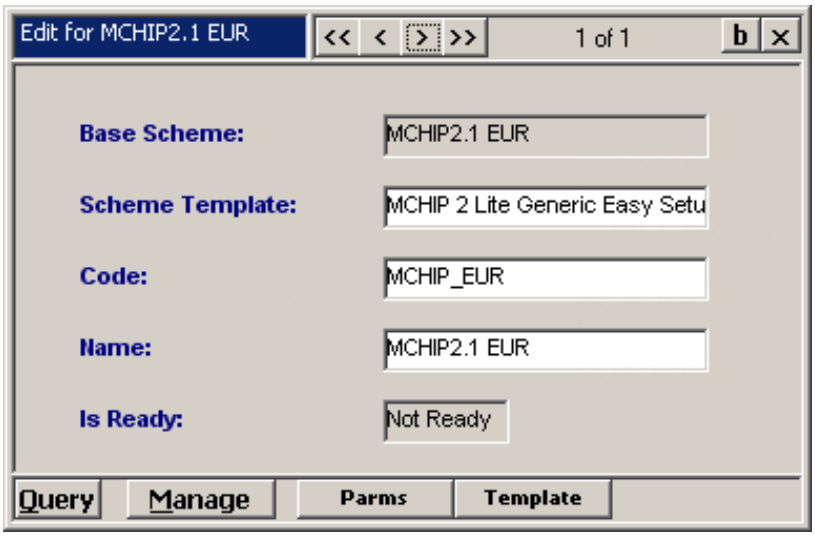


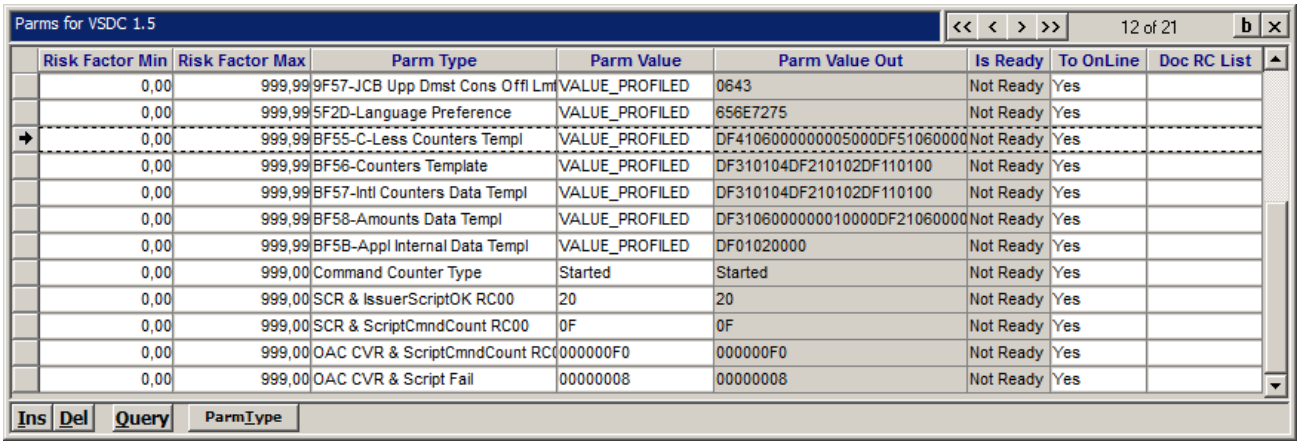
Fig. 5. Form for editing Risk Schemes properties

The fields of this form, which are the same as the fields of the "Chip Schemes" form (see Fig. 4) must be filled in.

After the fields of this form have been filled in, the Risk Scheme must be configured.

Parameters can be configured automatically by importing a card product parameter profile (see "Importing a Risk Scheme Parameter Profile from a File").

To enter Risk Scheme parameters manually, use the "Parms for <Risk Scheme name>" form (see Fig. 6), which opens when the [Parms] button in the "Edit for <Risk Scheme name>" form is clicked.



Risk Factor Min	Risk Factor Max	Parm Type	Parm Value	Parm Value Out	Is Ready	To OnLine	Doc RC List
0,00	999,99	9F57-JCB Upp Dmst Cons Offl Lmt	VALUE_PROFILED	0643	Not Ready	Yes	
0,00	999,99	5F2D-Language Preference	VALUE_PROFILED	656E7275	Not Ready	Yes	
0,00	999,99	BF55-C-Less Counters Templ	VALUE_PROFILED	DF41060000000005000DF51060000	Not Ready	Yes	
0,00	999,99	BF56-Counters Template	VALUE_PROFILED	DF310104DF210102DF110100	Not Ready	Yes	
0,00	999,99	BF57-Intl Counters Data Templ	VALUE_PROFILED	DF310104DF210102DF110100	Not Ready	Yes	
0,00	999,99	BF58-Amounts Data Templ	VALUE_PROFILED	DF31060000000010000DF21060000	Not Ready	Yes	
0,00	999,99	BF5B-Appl Internal Data Templ	VALUE_PROFILED	DF01020000	Not Ready	Yes	
0,00	999,00	Command Counter Type	Started	Started	Not Ready	Yes	
0,00	999,00	SCR & IssuerScriptOK RC00	20	20	Not Ready	Yes	
0,00	999,00	SCR & ScriptCmndCount RC00	0F	0F	Not Ready	Yes	
0,00	999,00	OAC CVR & ScriptCmndCount RC0	000000F0	000000F0	Not Ready	Yes	
0,00	999,00	OAC CVR & Script Fail	00000008	00000008	Not Ready	Yes	

Fig. 6. Form for configuring smart card Risk Schemes

The following fields of this form need to be filled in:

- *Risk Factor Max* and *Risk Factor Min* – the maximum and minimum limits of the "Risk Factor" special parameter.
  The current values of Risk Scheme parameters depend on the range into which the value of the "Risk Factor" parameter falls (see "Example of Defining Smart Card Risk Scheme Parameter Values for a Contract").
- *Parm Type* – the parameter name. A smart card Risk Scheme must include several mandatory parameters (these parameters have the "Mandatory" status in Risk Scheme templates).

- *Parm Value* is the parameter numeric value. A parameter will have this value if the value of the "Risk Factor" parameter of a contract lies within the range between the values entered into the *Risk Factor Min* and *Risk Factor Max* fields. This field cannot be edited if the parameter has the "BER-TLV Container" type (see "Types of Smart Card Risk Scheme Parameters"); i.e., the parameter consists of several parameters. In this case, it is necessary to click the [SubParms] button to define the values of subordinate parameters.
  If this field contains the "VALUE_PROFILED" value, the corresponding output value of the parameter, cast to its type (the value of the *Parm Value Out* field) was taken from the imported parameter profile file (see "Importing a Risk Scheme Parameter Profile from a File").

  > If the *Parm Value* parameter is used to determine the amount of an operation, its value must be presented in minimal currency units (cents, pennies, etc.).

- *Parm Value Out* is the output value of a parameter cast to its type (see the section "Types of Smart Card Risk Scheme Parameters").
- *To OnLine* – if the value of this field is "Yes", the parameter will be sent online as an issuer script; if the "No" value is set, the parameter will not be sent online.
- *Doc RC List* – comma-delimited list of response codes from the "Response Codes" system dictionary ("Full → Main Tables → Response Code (Customise)"). When creating issuer scripts, the parameter value will be selected that corresponds to the response code received. If no parameter value is found that corresponds to the response code, a parameter value with an empty response code will be selected.

If the parameter has the "BER-TLV Container" type (see "Types of Smart Card Risk Scheme Parameters") the [SubParms] button will be available in the "Parms for <...>" form (see Fig. 6). Clicking this button opens the "SubParms for Parms for <...>" form; in this form, the name of a subordinate parameter can be selected in the *Parm Type* field, and the parameter value specified in the *Parm Value* field.

The [ParmType] button of the "Parms for <...>" form (see Fig. 6) is used to view information about the parameter type (see "Types of Smart Card Risk Scheme Parameters").

After a Risk Scheme has been configured, it must be approved. For this, click the [Manage] button in the "Edit for <Risk Scheme name>" form (see Fig. 5) and select "Approve" from the menu that appears.

This will invoke the procedure checking whether the parameters of the Risk Scheme comply with the template and whether their values comply with their types. Also, the *Parm Value Out* field will be filled in. Its value is a formatted value of the *Parm Value* field.

If all the input data concerning the Risk Scheme parameters are correct, the Risk Scheme is approved, and a window with the "Issuer Production Scheme approved" message appears on the screen.

If any of the input data concerning the Risk Scheme parameters is incorrect or any compulsory parameters have been omitted, a window with an error message will appear, and the Risk Scheme will not be approved.

Information detailing the error is found in the *Parm Value Out* field of the "Parms for <Risk Scheme name>" form (see Fig. 7 for an example).

Parms for VSDC 1.5 << < > >> 2 of 21

Risk Factor Min	Risk Factor Max	Parm Type	Parm Value	Parm Value Out	Is Ready	To OnLine	Doc RC List
0,00	999,99	BF56-Counters Template	123	DF310104DF210102DF110100; Error: Length of	Not Ready	Yes	
0,00	999,99	9F6C-qVSDC PW Crd Trn Qualif	885	3A00; Error: Invalid value length	Not Ready	Yes	
0,00	999,00	SCR & ScriptCmndCount RC00	0F	0F; Error: Parameter value can not be changed	Not Ready	Yes	
0,00	999,99	9F52-VSDC Appl Default Action	VALUE_PROFILED	C3382800	Ready	Yes	
0,00	999,99	9F69-PW Card Auth Related Data	VALUE_PROFILED	01000000000000	Ready	Yes	

Ins Del Query ParmType

Fig. 7. Example of messages regarding errors in configuration of a Risk Scheme

3.3.1 Importing a Risk Scheme Parameter Profile from a File

Smart card Risk Scheme parameters can be configured automatically by importing a card product's parameter profile.

> For VSDC, this profile can be obtained on the Visa website. For M/Chip, this profile can be obtained from MasterCard.

To import the profile, click the [Manage] button in the "Edit for <name of Risk Scheme>" form (see Fig. 5) and in the context menu that opens, select an item.

- "Load Profile" – to import a VSDC template.
- "Load CPV Profile" – to import an M/Chip template.
  Import of a CPV/VPA profile using the com.openwaygroup.pipe.cpv_import_chip_scheme.jar and com.openwaygroup.pipe.vpa_import_pm.jar pipes can be performed with consideration of parameter categories (see the section "Card Production Parameter Categories"). This mechanism is supported by the EMVCATEGORIES pipe parameter. EMVCATEGORIES parameter values:
- "Y" – parameters are imported with consideration of category.
- "N" (default value) – parameters are imported without consideration of category.

Next, in the "Select files" window that opens, select the required profile file. Note that files with the "*.xml" extension located in the "<OWS_WORK>/data/card_prd/profiles/source" directory will be displayed in the dialog window.

As a result, the parameters will be loaded according to the selected Risk Scheme profile.

> Note that for parameters loaded from the file, the value "VALUE_PROFILED" will be specified in the *Parm Value* field of the "Parms for <name of Risk Scheme>" form (see Fig. 6").

If the file contains parameters that are absent in the Risk Scheme, a file is created containing these parameters. The file name will be "<name of original profile file>.remainder.xml". This file must be imported into the form containing the smart card issuing parameters (see "Configuring Card Applications").

3.3.2 Example of Defining Smart Card Risk Scheme Parameter Values for a Contract

The current values of Risk Scheme parameters assigned to a contract depend on the range into which the value of the "Risk Factor" parameter falls.

The value of this parameter is entered into the *Offline Limit Factor* field of the "Risk Scheme for <contract name>" form (see Fig. 8). The form invoked by clicking the [Risk Scheme] button in any of the forms used to configure contracts (see the Issuing Module User Manual).

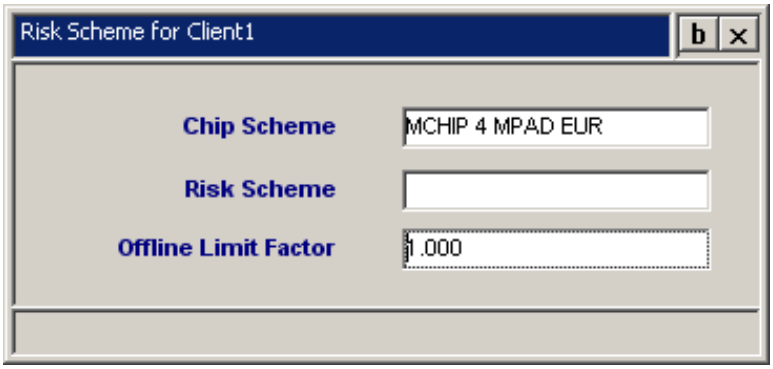


Fig. 8. Form for defining the value of the "Risk Factor" parameter of the Risk Scheme assigned to a contract

Thus, if the "Risk Factor" parameter is assigned the value of 200, the current value of the "9F54-VSDC Tot Cumul Amount Limit" will be "1000" (see Fig. 9).

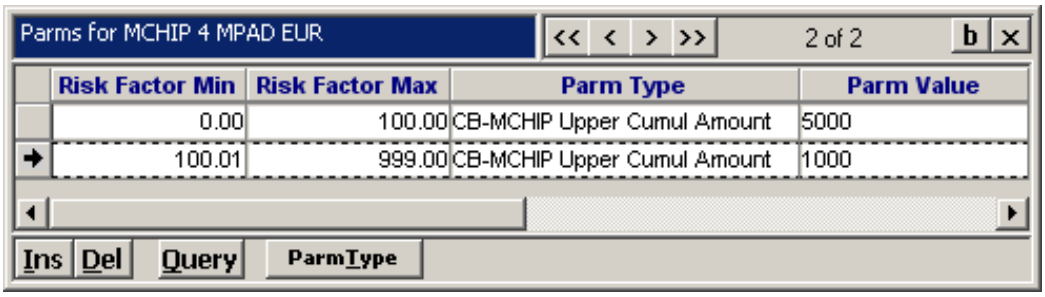


Fig. 9. Dependence of a Risk Scheme parameter value on the value of the "Risk Factor" parameter

3.3.3 Types of Smart Card Risk Scheme Parameters

Descriptions of Risk Scheme parameter types are provided in the "ParmType for Parms for <parameter name>" form (see Fig. 10) opened by clicking the [ParmType] button in the "Parms for <Risk Scheme name>" form (see Fig. 6) or in the "SubParms for Parms for <...>" form.

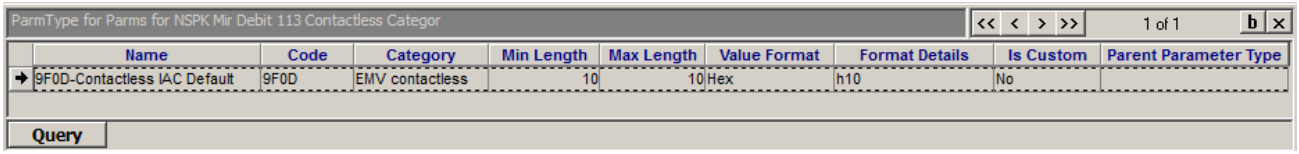


Fig. 10. Form containing the definitions of Risk Scheme parameter types

There are the following fields in this form:

- *Name* is the name of a parameter.
- *Code* is the code of a parameter.

- *Category* – parameter category (see the section "Card Production Parameter Categories").
- *Min Length* is the minimum number of symbols in the value of a parameter indicated by the user in the *Parm Value* field of the "Parms for <Risk Scheme name>" form (see Fig. 6).
- *Max Length* is the maximum number of symbols in the value of a parameter indicated by the user in the *Parm Value* field of the "Parms for <Risk Scheme name>" form.
- *Value Format* is the format of a value indicated by the user in the *Parm Value* field of the "Parms for <Risk Scheme name>" form:
- "Numeric" is a decimal number
- "String" is a string of symbols
- "Hex" is a hexadecimal number
- "BER-TLV Container" – BER TLV type (Basic Encoding Rules Tag Length Value), this type is a "container"; i.e. a composite parameter containing other (subordinate) parameters.
- *Format Details* is the description of the format of an output value:
- "h<Number>" is a hexadecimal numeric value of the indicated length padded with zeroes on the left
- "h?" is a hexadecimal numeric value whose length is within the range *Min Length – Max Length*
- "h" is a hexadecimal numeric value of the same length as that of the parameter in the template
- "h<Number>P<Symbol>" is a hexadecimal numeric value padded with the indicated symbols on the right
- "n<Number>" is a decimal numeric value of the indicated symbols padded with zeroes on the left
- "tag" is a letter
- *Is Custom* is the field determining whether or not a parameter type is a standard type of the system or a type individually configured for a certain client.
- *Parent Parameter Type* – name of the parent parameter; this field will be filled in if this parameter is included in the composite parameter with the "BER-TLV Container" type.

3.3.4 Example of Configuring a Risk Scheme for EMVC Category Parameters

The set of parameters with which the EMV application will work is determined in the Risk Scheme template.

An example of configuring 9F0F, 9F0E, and 9F0D parameters for the EMVC category and BFxx tags specific for the MIR payment system is shown below (see Fig. 11).

Chip Schemes

Name	Code	Scheme Template	Is Ready
NSPK Mir Debit 113 Contactless Categor	NSPK_MIR_DEBIT_113_CAT	NSPC MIR Generic	Ready

Ins Del Query Parms Edit Template

Parms for NSPK Mir Debit 113 Contactless Categor

sk Factor M	sk Factor Ma	Parm Type	Parm Value	Parm Value Out	Is Ready	To OnLine
0,00	999,99	C5-MIR Key Usage Counters	0064006400640064	0064006400640064	Ready	Yes
0,00	999,99	9F0F-Contactless IAC Online	F270448000	F270448000	Ready	Yes
0,00	999,99	9F0E-Contactless IAC Denial	0000800000	0000800000	Ready	Yes
0,00	999,99	9F0D-Contactless IAC Default	F270448000	F270448000	Ready	Yes
0,00	999,99	BF04-NSPK Accum Conf	D103064340	D103064340	Ready	Yes
0,00	999,99	C3-NSPK Offline Days	0	0000	Ready	Yes
0,00	999,99	BF12-MIR Profile Parameters	DF01081112F2FFFFFF0000DF0308333FFFFFFFFF0(	DF01081112F2FFFFFF0000DF0308333FFFFFF	Ready	Yes
0,00	999,99	BF0F-MIR Limits Rec Template	D206000000100000	D206000000100000	Ready	Yes
0,00	999,99	BF0B-MIR Curr Conv Table	D10C06430840679682097877138 2	D10C06430840679682097877138 2	Ready	Yes
0,00	999,99	BF0A-MIR Count Conf Template	D10130	D10130	Ready	Yes
0,00	999,99	BF09-MIR Count Parms Template	D1010ED20106	D1010ED20106	Ready	Yes
0,00	999,99	BF08-MIR Count Limits Template	D10400000000	D10400000000	Ready	Yes
0,00	999,99	BF06-MIR CIACs Template	D112000000000000000000000000100000000001D:	D112000000000000000000000000100000000	Ready	Yes
0,00	999,99	BF02-MIR Amnt Limits Template	D118000000100000000000100000000000000000(	D118000000100000000000100000000000000	Ready	Yes
0,00	999,00	Command Counter Auto Reset	N	N	Ready	Yes
0,00	999,00	CPA CSU Card Block	00400000	00400000	Ready	Yes

Ins Del Query ParmType

Fig. 11. Configuration of EMVC category parameters

4. Smart Card Issuing Parameters

Smart card issuing parameters include those used in the issuing of both magnetic and smart cards as well as smart cards exclusively. This chapter deals with actions involved in setting parameters used in smart card issuing.

Actions involving magnetic stripe cards are described in detail in the "Card Production Parameters" chapter of the Configuring WAY4™ System for Magnetic Stripe Card Issuing Administrator Manual.

4.1 Configuring Smart Card Issuing for Financial Institutions

Smart card issuing parameters for financial institutions are configured in the "Bank Production Parameters" form (see Fig. 12), which is opened by selecting the "Full → Configuration Setup → Card Production Setup → Bank Production Parameters" user menu item. This process also uses the forms subordinate to the "Bank Production Parameters" form.

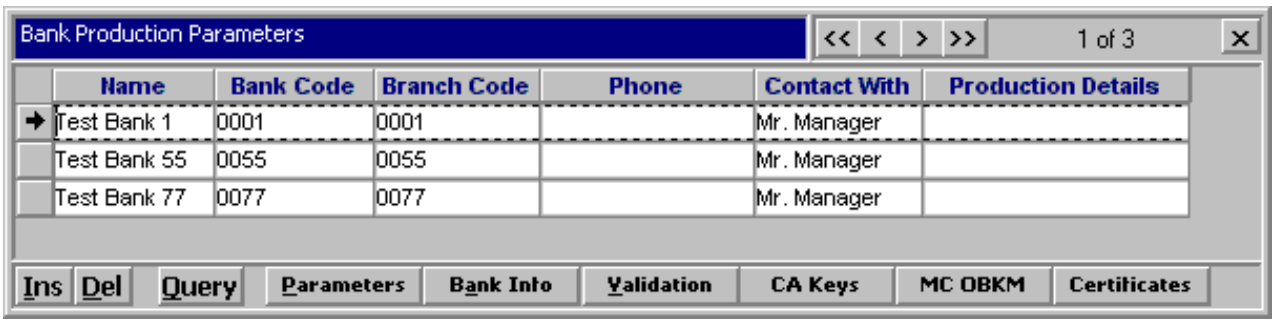


Fig. 12. Form for configuring smart cart issuing parameters

> When configuring parameters for MasterCard, in the *Production Details* field of this form it is necessary to specify the name under which the financial institution is registered in the payment system. This value will later be used in the names of files participating in key and certificate exchange with certification bureaux.

4.1.1 Smart Card Issuing Parameters

Card issuing parameters are set in the "Parameters for <name of financial institution>" form (see Fig. 13). It is opened by clicking the [Parameters] button in the "Bank Production Parameters" form (see Fig. 12).

Parameters for Test Bank 1 — << < > >> 9 of 14

Name	Code	PAN MIN	PAN MAX	PIN Len	ICA	Card Type	Encoding Method	PVKI	Is Ready	Ready Till	Bank
AMEX EMV Chip		3400000000000000	3400009999999999	4	2222	AMEX EMV	AMEX	1	Ready	00/00/0000	1
Cirrus		6799990100000000	6799990199999999	4	5555	Magnetic Card	Local	1	Ready	00/00/0000	1
CPA DDA	CPA	4025250000000000	4025259999999999	4	3333	CPA	MC	1	Ready	31/12/2012	1
JSmart		3500000000000000	3500009999999999	4	7777	JSmart	VISA	1	Ready	00/00/0000	1
Local		6000000000000000	6000009999999999	4	5555	Magnetic Card	VISA	1	Ready	00/00/0000	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	00/00/0000	1
MChip2.1 Lite		6799991000000000	6799991999999999	4	1111	MCHIP	MC	1	Not Ready	31/12/2012	1
MChip2.1 Lite Profiled	PROFILED	6799991000000000	6799991999999999	4	1111	MCHIP	MC	1	Ready	31/12/2012	1
PIN Mailer	HH	0000000000000000	0000009999999999	4		Magnetic Card	PIN Mailer		Ready	00/00/0000	1
Seccos		7777777777777777	7777777777777777	4	222	SECCOS	MC	1	Ready	00/00/0000	1
VISA+Electron		4015500000000000	4015519999999999	4	3333	Magnetic Card	VISA	1	Ready	00/00/0000	1
VSDC DDA		4025250000000000	4025259999999999	4	3333	VSDC	VISA	1	Ready	31/12/2030	1
VSDC SDA		4025240000000000	4025249999999999	4	3333	VSDC	VISA	1	Not Ready	31/12/2012	1

Ins Del Query Manage PIN Mailer EMV IBM3624 DES Keys 3-DES Keys RSA Keys Add Keys Certificates Options PIN2 Mailer Commands Bureau Keys

Fig. 13. Form for setting smart card issuing parameters

The fields of this form are filled in the same way as for issuing magnetic cards, with the exception of the Card Type field where "VSDC" must be entered for Visa, "MCHIP" for MasterCard, "AMEX EMV" for American Express, and "JSmart" for JCB, "UICS" for UnionPay International (UPI).

> For the MPAD card product based on the M/Chip4 specification, it is necessary to set up an additional parameter "OAC CVR & MC4 Go Online Bit RC00" to contain "0000000008". This should be done in the "Options for <card product name>" form opened by clicking on the [Options] button.

4.1.2 Validation Parameters

Bank card validity control parameters are entered in the "Validation for <name of financial institution>" form (see Fig. 14). The form is invoked by clicking the [Validation] button in the "Bank Production Parameters" form (see Fig. 12).

Validation for Test bank 1 — << < > >> 26 of 58

Name	PAN MIN	PAN MAX	PIN Valid Scheme	PVK Offs Trk2	PVK Offs Trk1	PVV Offs Trk2	PVV Offs Trk1
MC_SLIDING	5151510000000000	5151519999999999	VISA PVV	8	8	9	9
MC_Distribution	5151510000000000	5151519999999999	VISA PVV	8	8	9	9
MC Magn Auto	5152530000000000	5152539999999999	VISA PVV	8	8	9	9
MC EMV Auto	515254000000000	515254999999999	MC PVV	8	8	9	9
MCHIP4 OFFLINE CUF	5252520000000000	5252529999999999	MC PVV	8	8	9	9
MCHIP4 MPAD RUR	5255240000000000	5255249999999999	MC PVV	8	8	9	9

Ins Del Query Check Messages Options

Fig. 14. Form for setting cryptographic values verification parameters

The fields of this form are filled in the same way as for issuing magnetic cards, with the exception of the values of the EMV Crypto Scheme, EMV MAC Scheme and EMV Encr Scheme fields, where:

- "VSDC" is entered for VSDC (VISA Smart Debit Credit) cards.
- "VSDC+" is entered for VSDC++ cards.
- "MCHIP2" is entered for M/Chip2 cards.
- "MCHIP4" is entered for M/Chip4 cards.
- "JSmart" is entered for JCB products.
- "AMEX" is entered for American Express products.

- "EMV 2000 CPA V.4" is entered for CPA v.4 cards.
- "CPA V.5" is entered for CPA v.5 cards.
- "CUP" is entered for UnionPay International (UPI) products.
- "SECCOS" is entered for SECCOS cards.

Additional parameters for smart card verification are generated in the "Options for <parameter name>" form (see Fig. 15) opened by clicking on the [Options] button in the "Validation for <financial institution name>" form (see Fig. 14).

Options for MC << < > >> 3 of 3

Option	Value
Track 2 Discr. Data Format	PVKI+PVV+"0"+"0000"+CVC1
Track 1 Discr. Data Format	PVKI+PVV+"0"+"0000"+CVC1
ICVV Skip	Y

Ins Del Query Long Value

Fig. 15. Additional parameters for smart card verification

When generating card verification parameters, note that security standards prohibit the following:

- Storing CVV in the database.
- No CVV verification.

The user is entirely responsible for the use of card verification parameters that violate security standards. For example, the "ICVV Skip = Y" tab makes it possible to skip checking CVV for a specific pool of card numbers.

The parameter "Trust to Prevalid. Rslt Sec.Val." is used to set a list of security values that do not have to be checked in WAY4 if these values have already been checked in an external system; for example, in an IPS. A list of security value codes that are separated by commas is specified in the parameter: CVC1,CVC2,CAVV,PIN,CRYPT or the constant ALL. If these values were not checked by an external system, they will be checked in WAY4. If the external system's preliminary check failed, these transactions will be rejected in WAY4.

An example of EMVC.ESDD parameter configuration is shown below (see Fig. 16).

Options for NSPK Mir Debit Classic Profile 313 Contactless Categorized << < > >> 1 of 14

Option	Value
NSPK Card Indicator	0
Expr. Pay / Contactless CVM List	000000000000000042031F00
qVSDC AIP / Expr. Pay EMV AIP	1980
ICC Keys To Gen	3
Contactless EMV ESDD	5F245F255A5F349F078C9F0D9F0E9F0F5F289F429F088E9F4A;82
9F4F - Log Format	9F02065F2A029A039F52059F36029F2701CA01
Contactless CDOL1	9F02069F03069F1A0295055F2A029A039C019F37049F35019F3403
ICC Key Format	CRTM
BF03-NSPK Accums Parm Set	D102E001
qVSDC AUC / Expr. Pay AUC	FF00
Track 2 Discr. Data Format	PVKI+PVV+CVC1+"00"
Track 1 Discr. Data Format	PVKI+PVV+CVC1+"0000000000000000000000000000000000"
Issuer PIN Format	UNDER_ZPK
Chip CVC Present	Y

Ins Del Query Long Value

Fig. 16. Example of ESDD EMVC category parameter configuration

4.2 Card Applications

According to the EMV standard, a card application is a set of parameters used to establish interaction between a terminal and a smart card.

4.2.1 Configuring Card Applications

Card application parameters can be configured automatically by importing a card product parameter profile.

Profiles are imported in the "Parameters for <name of financial institution>" form (see Fig. 13 in the section "Smart Card Issuing Parameters"). To do so, click the [Manage] button in this form and select "Apply Profile" from the context menu that appears. In the "Select Files" window that opens, select the corresponding card application profile file.

> ⓘ If the parameters of the card application are only used by the PIN Management subsystem, it is necessary to import these parameters from the file of the card product parameter profile. In configuration of smart card Risk Scheme parameters, card application parameters are imported from the file <name of original profile>.remainder.xml" that was created after importing Risk Scheme parameters (see "Importing a Risk Scheme Parameter Profile from a File").

The parameters of a smart card application are manually set in the "EMV for <...>" form (see Fig. 17). The form is invoked by clicking the [EMV] button in the "Parameters for <name of financial institution>" form (see Fig. 13 in the section "Smart Card Issuing Parameters"). The [VISA Parms] and [MC Parms] buttons open the forms used to configure parameters that are specific for each payment system.

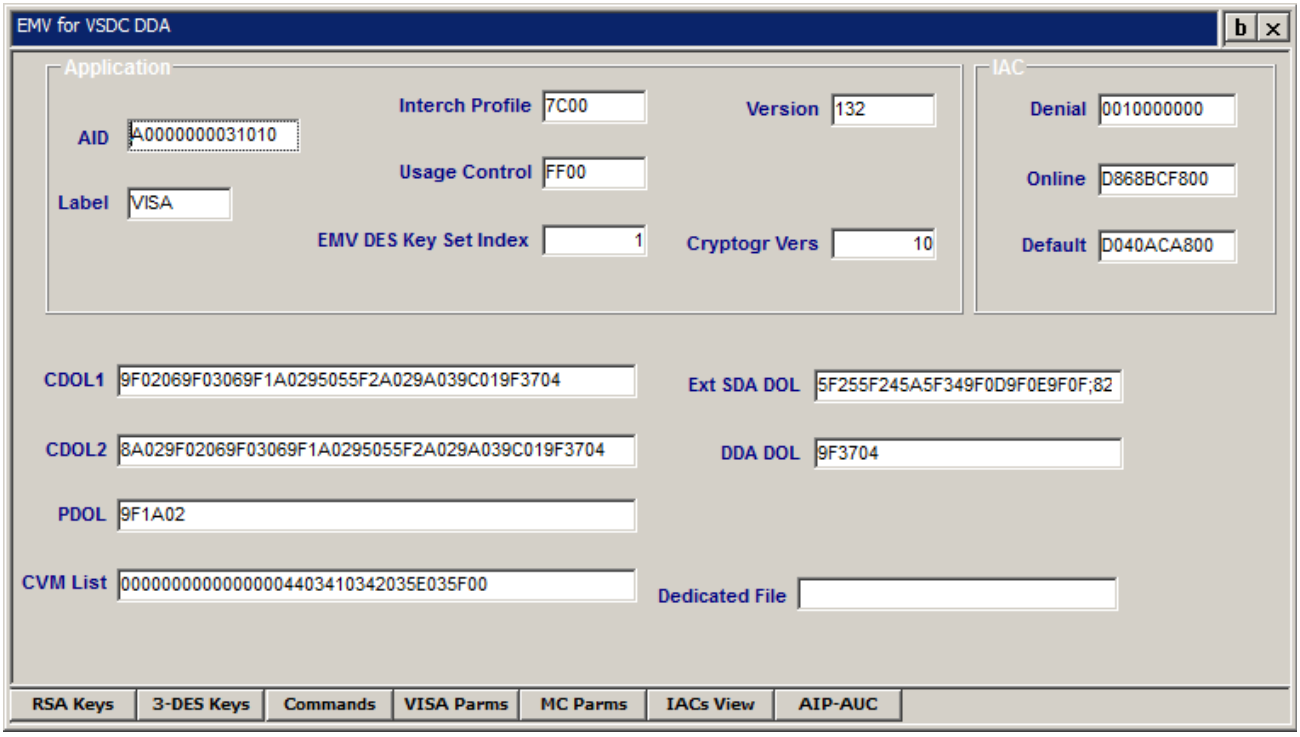


Fig. 17. Form for configuring smart card applications

> Values should be entered in the fields of the "EMV for <parameter name>" form according to the application template. For M/Chip cards, parameters are entered as required by the "*M/Chip 4 Issuer Guide to Debit and Credit Parameter Management*" and "*M/Chip Functional Architecture for Debit and Credit*" documents. The fields of this form are filled in with the values found in the "CARD DATA ELEMENTS" tables of corresponding templates.

The *Ext SDA Dol* field is an exception. This field determines the data that will be used for SDA/DDA/CDA and their order. The field value must correspond to the electric personalisation system installed at the bank.

If the parameter profile file contains additional parameters for which there is no corresponding field in the "EMV for <parameter name>" form, these parameters will be saved as tags. The parameters and their values can be viewed in the "Options for <parameter name>" form (see Fig. 18), opened by clicking the [Options] button in the "Parameters for <name of financial institution>" form (see Fig. 13 in the section "Smart Card Issuing Parameters").

Options for Test VSDC << < > >> 7 of 7 b ×

Option	Value
EMV Appl Priority Ind (tag 87)	01
9F17	03
9F10	08000A030000000F04
9F4D - Log Entry	0B0A
5F2D	7275656E6465
9F4A	82
9F4F - Log Format	9F27019F02065F2A029A039F3602

Ins Del Query Long Value

Fig. 18. Additional parameters of a smart card application

4.2.2 Configuring Several Applications for a Card

In accordance with the EMV standard, several applications, including financial ones, may be loaded onto a smart card (multi-application card).

In WAY4, several applications may be configured for one card by configuring a hierarchy of products in the issuing module and setting card application parameters in the data preparation and key management module.

In both the issuing module and the data preparation and key management module, an individual range of card numbers is configured for each card application. The application to whose range the number embossed on the plastic belongs is primary and the rest are additional.

4.2.2.1 Configuring a Hierarchy of Products

In order to configure several applications for one card in the issuing system, a product hierarchy with the Main/Sub type of relationship must be set up (see the "Creating a Product" section of the Products and Contract Subtypes Administrator Manual). This involves the following actions:

- A card contract subtype must be configured for each range of card numbers (card applications) (see the "Contract Types and Subtypes" section of the Products and Contract Subtypes Administrator Manual).
- A product hierarchy must be configured (see the "Creating a Product" section of the Products and Contract Subtypes Administrator Manual) where a contract subtype is indicated for the primary Product and subtypes of additional card applications for subordinate products. Also, for subordinate products the "Applet" value must be selected from the list opening in the *Relation Tag* field and the "1" value entered into the *# of Contracts* field of the "Full Info for <product name>" form that is invoked by clicking the [Full Info] button in the form for configuring subordinate products (see Fig. 19).

> For applications using the CAP (Chip Authentication Program) authentication standard, specify the "CAP Applet" value in the *Relation Type* field of the "Full Info for <product name>" form.

An example of a hierarchy of products configured for a card with a debiting application and a loyalty programme application is shown in Fig. 19.

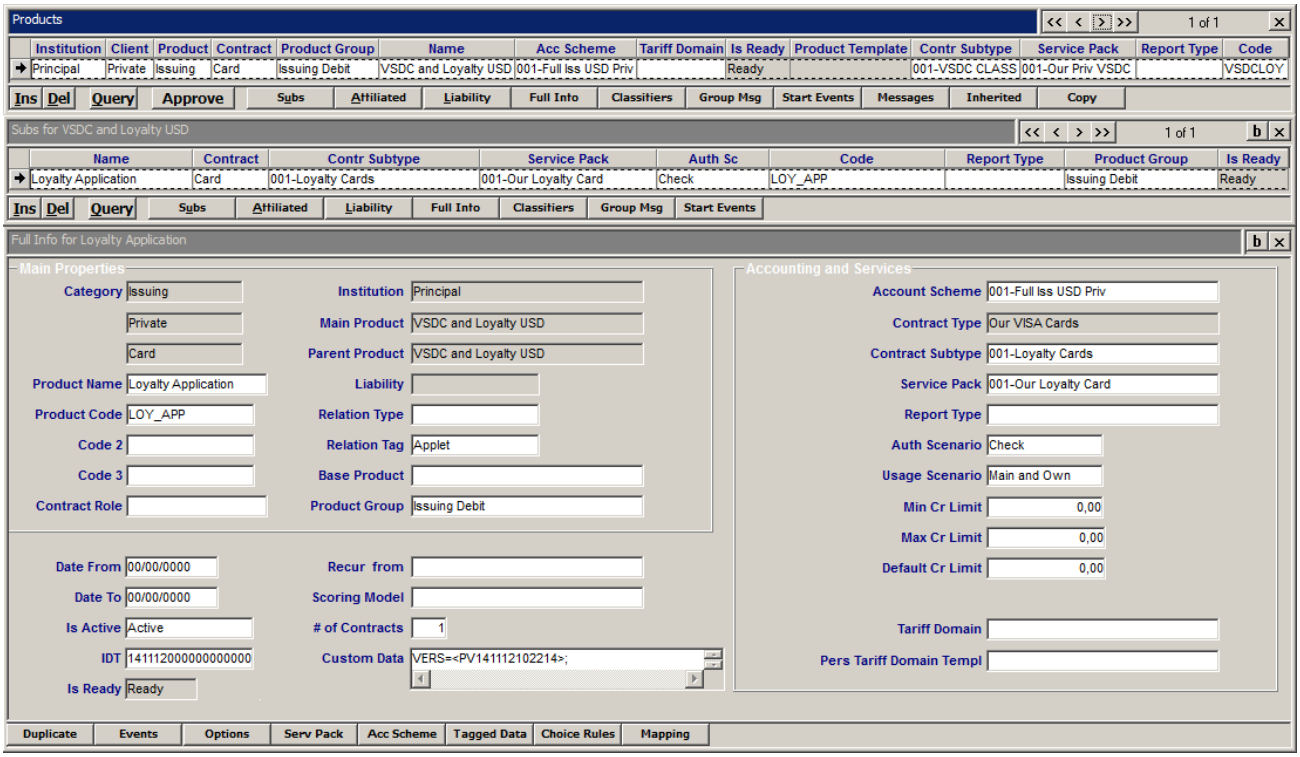


Fig. 19. Hierarchy of products for a smart card with two applications

> It should be kept in mind that only one accounting scheme is used for a product hierarchy with the Main/Sub type of relationship.

After a product hierarchy is configured, its primary product must be indicated when registering a card contract (see the "Creating Individual Card Contracts" and "Entering New Corporate Contracts" sections of the Issuing Module User Manual).

4.2.3 Configuring an Additional Card Application without Creating a Product Hierarchy

In WAY4 it is possible to create an additional card application without creating a product hierarchy. This is only possible if documents are not created and processed in WAY4 using the application (for which a contract is not created). Biometric authentication or an applet for the contactless part of MasterCard PayPass are examples of such applications.

To create an additional card application, it is necessary to do the following:

- For each range of card numbers it is necessary to configure a hierarchical structure of card contract subtypes (see the section "Contract Types and Subtypes" in the document "Products and Contract Subtypes"). To do so, in the "SubTypes for <name of card contract type>" form, select the subtype and click the [Applets] button. As a result, the "Applets for <name of subtype>" form will open (see Fig. 20).

SubTypes for Our VISA Cards

Institution	Client	Name	Is Active	BIN	Min #	Max #	Channel	BIN Record	Exp For New	Exp For Renew
Principal	Private	001-VISA Cards with Applet	Yes	402527	0100000000	0199999999	Our VISA Cards	402527:Visa Gold:Credit	12	12

Ins Del Query Validate Contracts Preferred Mapping Applets

Applets for 001-VISA Cards with Applet

Name	Prefix	Min Number	Max Number	PM Code	Fee Algorithm	Service Code	Validation Type	Add Parms	Chip Scheme	Is Active
Test Applet	12345	0000000000	9999999999	TST_APPL		101		CARD_PARMS_LIST=ARQC_MK,AIP;PAN=MAIN;	VSDC 1.5	Yes

Ins Del Query

Fig. 20. Configuring the hierarchy of a card contract's subtypes

In the "Applets for <name of subtype>" form, add a record of the subordinate subtype, and in the *Chip Scheme* field list, select a Risk Scheme for the card application The following tags can be specified in the *Add Parms* field:

- "CARD_PARMS_PREFIX=<string>;" – the prefix that will be used to identify this applet's parameters during processing of requests on the card's main financial application.
- "CARD_PARMS_LIST=<value>; - this tag is to specify parameter codes necessary for checking. Codes are comma-delimited. For example, for a biometric authentication application, specify "CARD_PARMS_LIST=ARQC_MK,AIP;".
- "PAN=MAIN" – tag indicating that the card number for the applet is inherited from the card's main financial application.
- Create a Product, specifying as the subtype the contract subtype created in the previous step that is the main one in the hierarchy. Note that on the level of the Service Package set for the Product, the Risk Scheme (see Smart Card Risk Schemes") created earlier must be defined in the *Chip Scheme* field.
  For more information about creating Products, see the section "Entering Product Data" of the document "Products and Contract Subtypes".
- Create a card contract; as the contract subtype, specify the main subtype in the hierarchy. As a result, when marking cards for issue, a record will be created about an additional card application. This record is accessible by clicking [Applet] in the card contract's "Plastics for <...>" form opened by clicking the [Plastics] button (see Fig. 21).

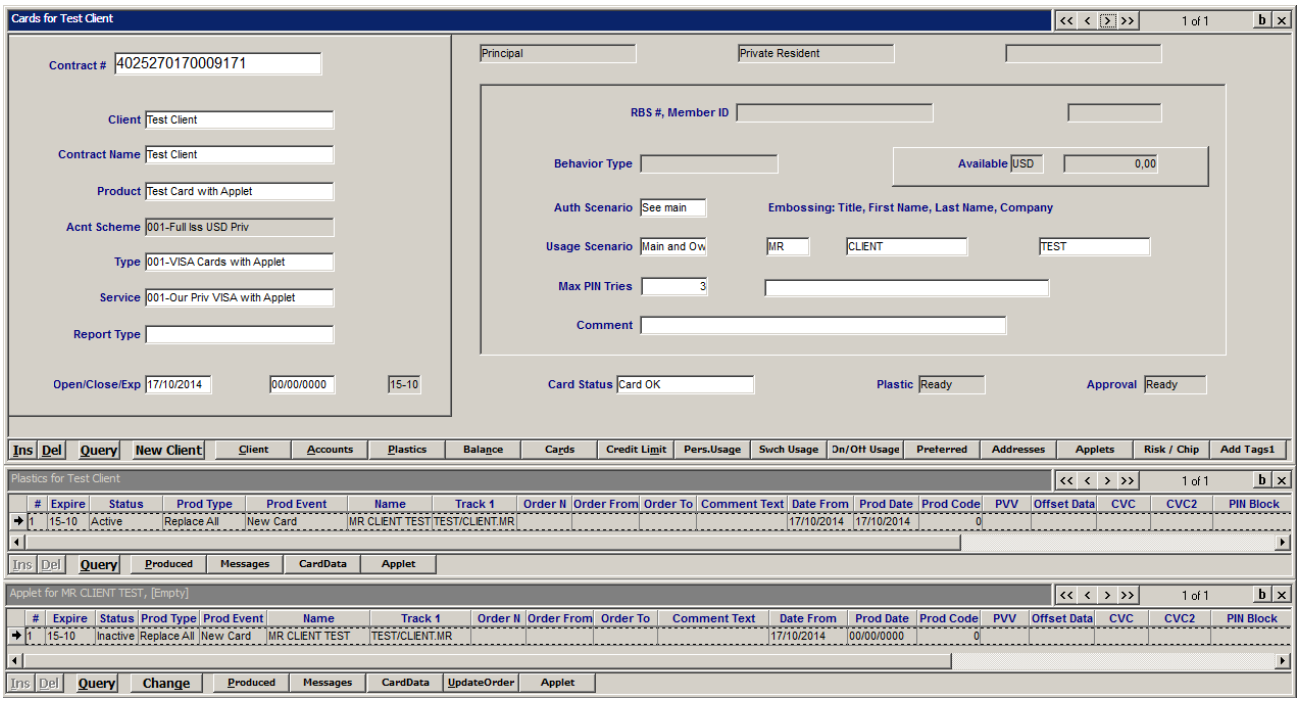


Fig. 21. A card contract and additional card application

4.3 Encryption Keys

This section describes the procedure of generating and configuring encryption keys.

This section also provides information on specific system configurations that should be set up in the event that differently configured HSMs (different vendors) are used by the data preparation and online processing systems (see "Configuring 3-DES Key Parameters for Different ").

Encryption keys required for smart card production can be generated on HSMs that differ both in purpose and type of configuration (see Fig. 22).

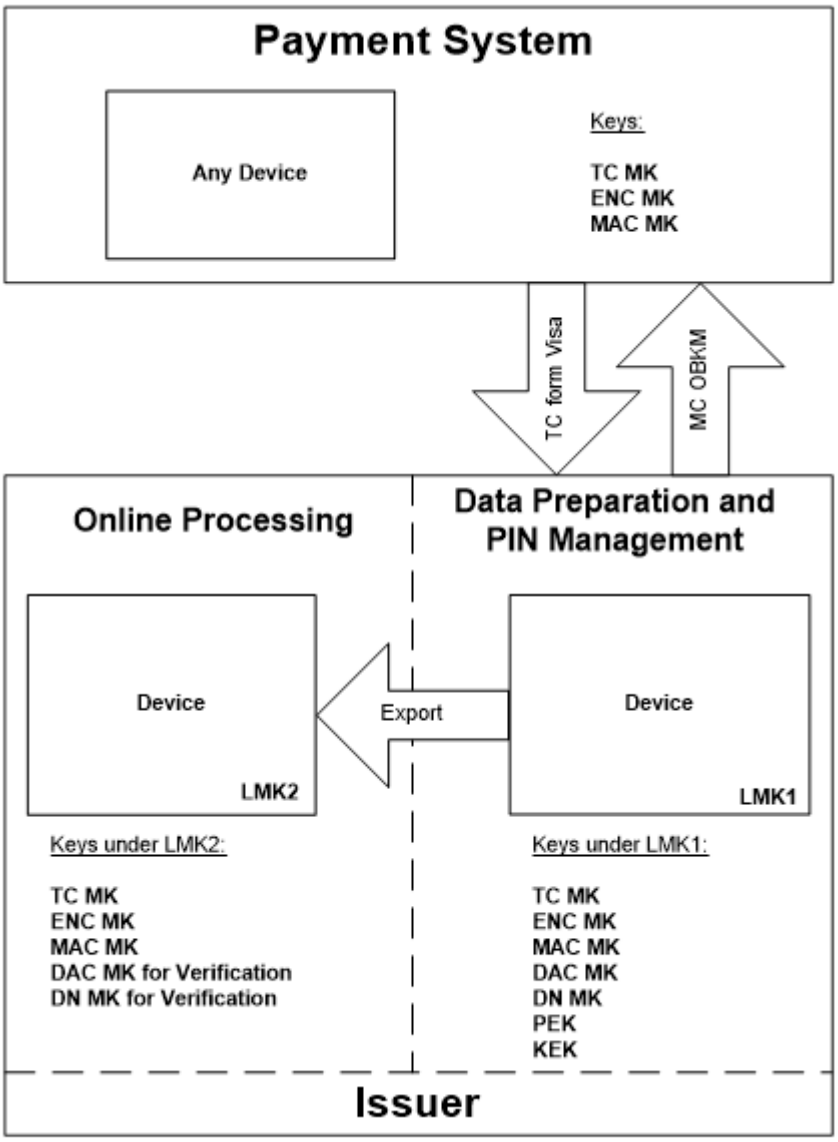


Fig. 22. Encryption keys for smart card production in WAY4

WAY4 provides for the following ways of generating encryption keys:

- Generation of keys on a Data Preparation and PIN Management module.
- Obtaining keys from a payment system.

Note that when generating as well as importing and exporting encryption keys on devices of differing configurations, different commands are used. Refer to the following documentation corresponding to the HSM used:

- For Thales payShield 9000 – "payShield 9000 Security Operations Manual".
- For SafeNet devices – "ProtectServer Encryption Device Control Module. Description of Console Commands".

> It is recommended to generate encryption keys for SafeNet OWSeM or Thales devices using the "DES Key Management" pipe (see "Key Generation").

4.3.1 3-DES Keys

The following 3-DES encryption keys are used in producing smart cards:

- "TC Master Key" – used to generate and verify ARQC, ARPC and TC cryptograms.
- "MAC Master Key" – used to generate and verify issuer script electronic signatures.
- "Encryption Master Key" – used to encrypt and decrypt data contained in issuer scripts; for example, offline pin.
- "DAC Master Key" – used to generate a Data Authentication Code value for M/Chip SDA (Static Data Authentication) cards.
- "DAC Master Key for Verification" – used for online verification of the Data Authentication Code value for M/Chip SDA (Static Data Authentication) cards.
- "DN Master Key for Production" – used to generate a DN value for DDA (Dynamic Data Authentication) cards.
- "DN Master Key for Production & Verification" – used for online verification of the DN value for DDA (Dynamic Data Authentication) cards.
- "Key Encryption Key" – used to encrypt and decrypt keys when sending data from PIN Management to an electric personalisation subsystem.
- "PIN Export Key" – used to encrypt the PIN block for card personalisation and when sending data from PIN Management to an electric personalisation subsystem.
- "PayPass Dynamic CVC3 Master Key" – used for generation and online verification of a Dynamic CVC value for MasterCard PayPass cards.
- "PayPass Dynamic CVC3 Master Key for Production" – used to generate a Dynamic CVC value for MasterCard PayPass cards. This key type is only used for Thales payShield 9000 devices (without basic firmware).
- "PayWave Dynamic CVV Master Key" – used to generate a Dynamic CVV value for Visa PayWave cards.
- "AMEX CSC Key" – used for generation and online verification of a CSC (Card Security Code) value for AMEX cards.
- "Bioverification TC Master Key" – used to generate and verify biometric verification application cryptograms.
- "PVK" (PIN Verification Key) – used for generation and online verification of a PVV (PIN Verification Value).
- "CVK" (Card Verification Key) – used for generation and online verification of a CVV (Card Verification Value).
- "CVK2" – used for generation and online verification of a CVV2.
- "ZPK (Zone PIN Key) – used to encrypt a PIN block when sending from the issuing module to PIN Management if PIN block translation mode is used.

> If a Thales HSM payShield 9000 device is used in the system, the key "DN Master Key for Production & Verification" must be used instead of the key "DN Master Key for Production".

These are master keys, meaning they are keys used to diversify a card's unique keys.

3-DES parameters are configured in the "3-DES Keys for <issued card type name>" form (see Fig. 23) opened by clicking the [3-DES Keys] button in the "EMV for <parameter name>" form.

3-DES Keys for VSDC DDA 5 of 5

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	TC Master Key	U5D44B4F3D5ACA848ABD75E22164E13F5	858E55	00/00/00 00:	00/00/00 00:		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	MAC Master Key	UF49BCF23DDD76D005B244C4A4E42B2AE	EC2078	00/00/00 00:	00/00/00 00:		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	Key Encryption Key	UCC0C86C2103F467EEC809519A48631C6	A6D39D	00/00/00 00:	00/00/00 00:		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	Encryption Master Key	U2118C04E4A2E5E291BB9CAC94A4125F9	5336B4	00/00/00 00:	00/00/00 00:		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	DN Master Key for Production	UC8E668962C9C93D71F19B5D7FF6CD957	1D689E	00/00/00 00:	00/00/00 00:		HSM / Host / Hex	Ready	00/00/0000

Ins Del Query Manage Options

Fig. 23. Form for configuring DES keys

If the data preparation system and online processing system use HSMs with different configurations, follow the instructions provided in the section "Configuring 3-DES Key Parameters for Different ".

The method for generating 3-DES keys depends on the type of HSM device used in WAY4 (see "Hardware Security Module Setup").

It is recommended to generate 3-DES keys using the "DES Key Management" pipe (see "Key Generation"). The pipe is started in the "DES Management Mode" form, opened by clicking the [Manage] button in the "3-DES Keys for <issued card type name>" form. When keys are generated this way, their parameters are automatically imported to the database and no additional configuration of their parameters is required.

This method of generation is supported for all types of devices used in WAY4 (see "Hardware Security Module Setup").

4.3.1.1 Key Generation

3-DES keys are generated in the system using the "DES Key Management" pipe. When a key is generated in this way, its parameters are automatically imported into the database, and no additional configuration of its parameters is required.

> This method is supported for all types of HSM devices used in the system (see "Hardware Security Module Setup").

Before starting key generation, in the "3-DES Keys for <issued card type name>" form (see Fig. 23 in the section "3-DES Keys"), select the key type from the list (*Key Type* field) and in the *Storage Form* field select one of the following key storage methods:

- "HSM / Host / Hex" – for keys generated on a Thales device.
- "OWSeM / Host / Hex" for keys generated on a SafeNet device.
- "GL / Host / HEX" – for keys generated on a Gemalto device.

> ⚠ Use of the same key for several card types is strictly prohibited.

To start the key generation procedure, click the [Manage] button in the "3-DES Keys for <name of card type>" form (see Fig. 23 in the section "3-DES Keys").

4.3.1.1.1 (Manage) Button

The screen will display a context menu containing the following items:

- "Manage" – when this menu item is selected, the "PM DES Management Mode" form will open (see Fig. 24).

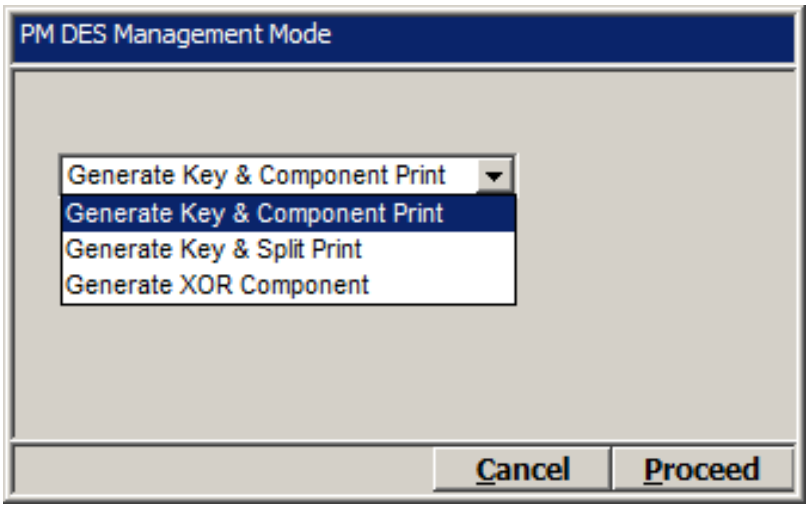


Fig. 24. Form for selecting encryption key generation mode

One of the following key generation modes canbe 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 key and separately print components.

> ⚠ It is not recommended to use this key generation mode; the mode exists in the system to ensure compatibility with previous versions.

- "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 components (see "Generate Key (No Printing)" Option").

4.3.1.1.2 "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 by the pipe parameter "KEY_COMPONENTS" (see "DES Key Management" Pipe Parameters") or the key type additional parameter "Num of XOR Components" (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.

4.3.1.1.3 "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 by the pipe parameter "KEY_COMPONENTS" (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 "DES Keys for <name of card type>" form (see Fig. 23 of the section "3-DES 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.

4.3.1.1.4 "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. 23 in the section "3-DES Keys") is different from that calculated using the HSM, an error message will be displayed.

4.3.1.1.5 "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 an 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.

4.3.1.1.6 "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.
- SRC_CODEPAGE - this parameter specifies encoding that is used in the template file for printing PIN mailers. US-ASCII encoding is used by default (Codepage 437).
- DST_CODEPAGE - this parameter specifies encoding in which generated text will be sent to a printer that is connected to HSM.

4.3.1.2 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. 25), define printing templates.

PM Key Type Options << < > >> 37 of 44

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

Ins Del Query Options

Options for PVK - 3DES << < > >> 3 of 3

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}],

Ins Del Query

Fig. 25. Setting key printing templates

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. 25).
- 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.

4.3.1.2.1 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}]
-
```

4.3.1.2.2 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 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 templates, the key check value (KCV) will be printed in a PIN mailer together with the last component of the key.

4.3.2 Configuring 3-DES Key Parameters for Different HSM Configurations

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

In the event that two or more Thales 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 PSG) 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 device of the data preparation and key management system; keys may also be received from the payment system (see the "Encryption Keys" section).
- Key used to validate transaction information must be imported into the device of the online processing system (see the document Transferring DES Keys between Thales™ HSM and SafeNet PSO").
- For every key encrypted with LMKs of different devices, two records in the "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 device (in case this record is not created automatically)
- A record for the key encrypted with the LMK of the online processing system device

> In the event that 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 "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 the key encrypted with the LMK of a Thales device
- "OWSeM / Host / Hex" – for the key encrypted with the LMK of a encryption device
- "GL / Host / HEX" – for the key encrypted with the LMK of a Gemalto device.
- The "HH" value must be assigned to the AUTH_KEY_STORAGE_FORM global parameter.
- In the "Produce Cards & PINs" pipe parameters (see the "Processing Jobs" section of the WAY4™ Magnetic Stripe Card Issuing User Manual), it is necessary to specify, through the

"STORAGE_FORM" parameter, what device is used by the data preparation and key management system:

- "HH" – a Thales device
- "WH" – a SafeNet device
- "LH" – a Gemalto device

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" in the document "Configuring WAY4™ for Magnetic Stripe Card Issuing") can be specified using the "SM_ID" parameter.

> It should be kept in mind that the "Produce Cards & PINs" menu item definition consists of two subitems. The "STORAGE_FORM" ("SM_ID") parameter value must be specified for both subitems.

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 devices (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 subitem, use the "SM_ID" parameter to specify the IDs, separated by commas, of those devices that will be used to calculate cryptographic values.
- For the second menu subitem, use the "SM_ID" parameter to specify the ID of the device 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 section "Processing Jobs" of the document "WAY4™ Magnetic Stripe Card Issuing").

4.3.3 RSA Keys

There are two types of RSA keys used while issuing smart cards:

- The Issuer Public Key used as a certificate for signing data while issuing all types of smart cards (see "Issuer Public Key"), which, in turn, is signed by the public key of a certification authority (see "Certification Authority Public Key").

> Certification authorities are organisations that issue certificates for public keys of third parties such as issuing banks. In the case of the public keys used by banks while issuing smart cards, the certification authorities are divisions of the corresponding payment systems.

- The Integrated Circuit Card Private Key (ICC Key) used as an additional card authentication tool (see "Integrated Circuit Card Private Key"). This key is only used for DDA (Dynamic Data Authentication) and CDA (Combined Data Authentication) cards.

4.3.3.1 Issuer Public Key

Issuer Public Keys are generated by issuers with the use of HSMs installed in their systems (see "Hardware Security Module Setup"). Once generated, a public key must be sent as a special-format file to a certification authority to be endorsed. The formats of such files are dictated by payment systems. The endorsement of an issuer public key by the private key of a certification authority results in an issuer public key certificate. These certificates are sent back to issuers by certification authorities along with their public keys. After this, the public key received from a certification authority and the issuer's key certificate must be loaded into WAY4. Then the certificate can be used to authenticate cards.

> Keep in mind that CA public keys must be loaded into WAY4 before the issuer public keys (see "Certification Authority Public Key").

Fig. 26 shows a diagram of key and certificate exchange with a certification authority.

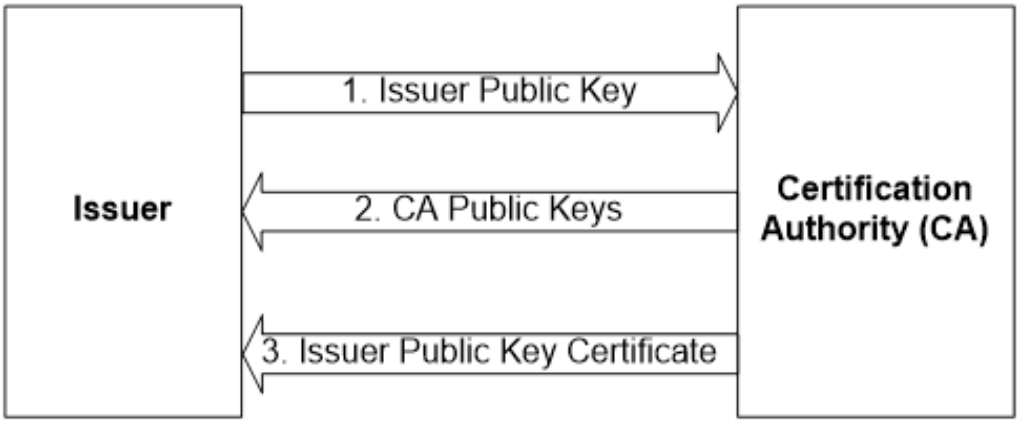


Fig. 26. Public key and certificate exchange with a certification authority

In WAY4, issuer public keys are configured in the following way:

- Open the "RSA Keys for <parameter name>" form used to configure RSA keys (see Fig. 27). The form is invoked by clicking the [RSA Keys] button in the "EMV for <parameter name>" form (seeFig. 17 in the section "Card Applications").

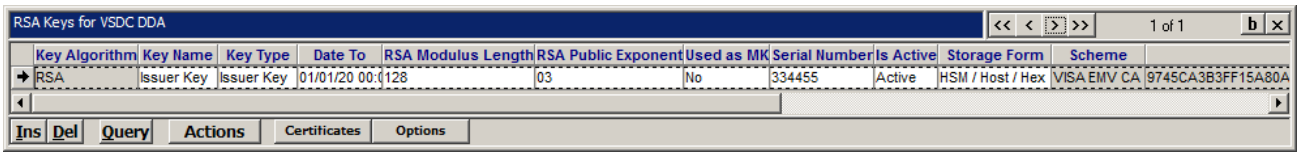


Fig. 27. Form for configuring RSA keys

- In the form, fill in the following fields:
- *Key Name* – the name of the key.
- *Key Type* – the type of the key. For the issuer public key, select the "Issuer Key" value in this field.
- *Date To* – the expiration date of the key.
- *RSA Modulus Len* – the length of the key in bytes.
- *RSA Public Exponent* – public exponent used in RSA encryption. This field may have one of the two following values: "03" or "010001".
- *Serial Number* – six-digit key number. This number is used in the name of the file with the issuer's public key sent to a certification authority for endorsement. For the VISA payment system, the value of the key number is provided by the payment system; for MasterCard, it is filled in automatically during key generation.
- *Storage Form* – key storage method.
- After filling in the form fields, click the [Actions] button and select [Manage] from the context menu that appears. This will bring the "RSA Management Mode" form (see Fig. 28) to the screen. In this form, select the "Generate Key Pair" procedure from the drop-down list and click the [Proceed] button.

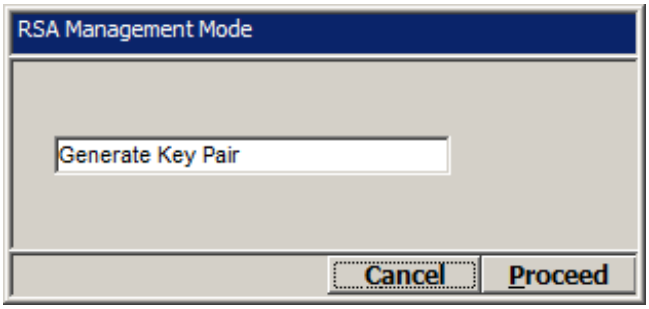


Fig. 28. Form for selecting RSA key generation procedure

If the Issuer Public Key is generated successfully, the file for this key will be put into the directory specified in the SOURCE_DIR parameter (or in the DEFAULT_PATH parameter) of the "RSA EMV Key Management" pipe. If SOURCE_DIR and DEFAULT_PATH parameters are not set, an error message will be generated.
Along with the Issuer Public Key file, the following two certificates are generated:

- Self Signed type certificate used by the certification authority for authenticating the Issuer Public Key
- Public Key MAC type certificate used for storing the Issuer Public Key in the database

The parameters of these certificates will be reflected in the "Certificates for <key name>" form (see Fig. 30) opened by clicking the [Certificates] button in the "RSA Keys for <parameter name>" form (see Fig. 27).

After the Issuer Public Key has been generated, it must be sent for signing to the certification authority according to the requirements of the payment system.

After Issuer Public Key is signed by the private key of a certification authority and received by the issuer as a certificate (along with the public key of the certification authority), the key and the certificate must be loaded into WAY4.

> In accordance with payment system regulations, all files (exported and imported) participating in the exchange of public keys and certificates have a set structure of file names. It is not recommended to manually change the names of these files.

> It should be kept in mind that CA public keys must be loaded into WAY4 before the Issuer Public Key certificate. The steps involved in this procedure are described in "Certification Authority Public Key".

To load the certificate, proceed as follows:

- Create a new entry in the "Certificates for <key name>" form that is opened by clicking the [Certificates] button in the "RSA Keys for <parameter name>" form. In the *Type* field, select the "EMV CA" value. In the *Master Key* field, select the name of the previously loaded public key of the certification authority used to sign this certificate.
- In the "RSA Keys for <parameter name>" form, click the [Actions] button and select [Manage] from the context menu that appears. This will bring the "RSA Management Mode" form to the screen. In this form, select the "Load Issuer PK Certificate" procedure and click the [Proceed] button (see Fig. 29).

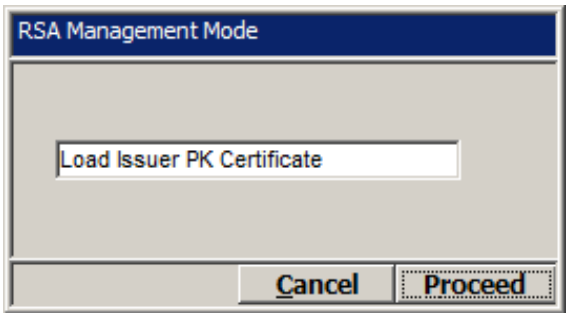


Fig. 29. Procedure of loading Issuer Public Key

Select the required file from the directory specified in the SOURCE_DIR parameter of the "RSA EMV Key Management" pipe. If the SOURCE_DIR parameter is not set, the first suitable file will be selected from the directory set in the DEFAULT_PATH parameter (if DEFAULT_PATH is set and SOURCE_DIR is not). If the SOURCE_DIR and DEFAULT_PATH parameters are not set, an error message will be generated.

If the Issuer Public Key certificate is successfully loaded, information about it can be obtained in the "Certificates for <key name>" form, which is invoked by clicking the [Certificates] button in the "RSA Keys for <parameter name>" form (see Fig. 30).

Certificates for Issuer Key

Type	Format	Hash Alg	Signature Alg	Master Key	Serial #	Authentication Data	Certificate Body	Certificate Remainder	Hash Data	Is Ready	Ready Till
Public Key MAC							26CB115C			Ready	00/00/0000
Self Signed	VSDC Iss	SHA-1	RSA		000008		22809745CA3B3FF15A8		D5D3EA6923	Ready	00/00/0000
EMV CA		SHA-1	RSA	Test CA VISA 22	334455		606AA18F05832DA1CC	0362F56A5666259E2F6144		Ready	00/00/0000

Ins Del Query

Fig. 30. Issuer Public Key certificates

4.3.3.2 Certification Authority Public Key

To configure the public key of a certification authority in WAY4, proceed as follows:

- In the "CA Keys for <bank name>" form (see Fig. 31), which is opened by clicking the [CA Keys] button in the "Bank Production Parameters" form (seeFig. 12 in the section "Configuring Smart Card Issuing for Financial Institutions"). Create a new record and fill in its mandatory fields as follows:
- In the *Scheme Code* field, the payment system the card belongs to must be indicated.
- The *Scheme Add Data* field must be filled in with the application identifier (RID+PIX), which, according to either VSDC Personalization Template standard or MasterCard Minimum Card Requirements, is a concatenation of the following two values:
- The first ten symbols are the RID (Registered Application ID) value, that is the card's application ID. It identifies the owner of the application: either VISA or MC.
- The second part of the value is the PIX (Proprietary Extension), that is, the application type.
- The *Key IDT in Scheme* field must be filled in with the index of the public key of a certification authority. The value falls within the range between"00" and "FF".
- *Key Type*

CA Keys for Test bank 1

Key Type	Date To	RSA Modulus Length	RSA Public Exponent	Key Name	Scheme Code	Key IDT in Scheme	Scheme Add Data	Is Active
CA Public Key	01/01/2030	128	03	VSDC OW test2	VISA EMV CA	23	A0000000031010	Active

Ins Del Query Manage Certificates

Fig. 31. Form for entering and configuring Public Keys of certification authorities

- After this, click the [Manage] button in the "CA Keys for <bank name>" form to open the "RSA Management Mode" form (see Fig. 32). In this form, select the "Import CA Public Key" procedure and click the [Proceed] button.

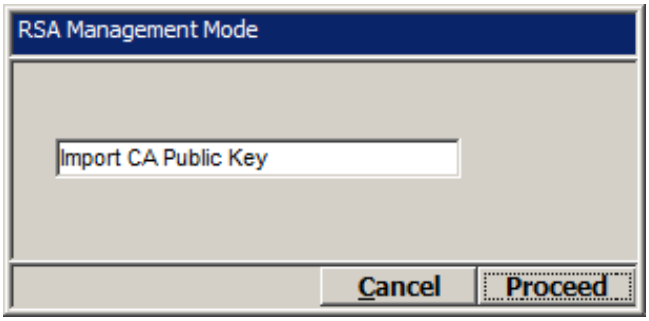


Fig. 32. Form for calling the key import procedure

- If the public key of a certification authority is successfully loaded, its encrypted value appears in the *RSA Modulus* field of the "CA Keys for <bank name>" form. The representations of two certificates of the "Public Key MAC" and "Self Signed" types also appear in the "Certificates for <key name>" form (see Fig. 33), which is opened by clicking the [Certificates] button in the "CA Keys for <bank name>" form.

Certificates for Test CA VISA 22 — << < > >> 2 of 2

Type	Format	Hash Alg	Signature Alg	Master Key	Serial #	Authentication Data	Certificate Body
Public Key MAC							D6FE3B79
Self Signed		SHA-1	RSA	5430			20101000000800101A00000000322AFDF88D93

Ins Del Query

Fig. 33. Certification authority public key certificates

4.3.3.3 Integrated Circuit Card Private Key

The Integrated Circuit Card Private Key is used as an additional card authentication tool in DDA (Dynamic Data Authentication).

This key is generated by the HSM when issuing a card. This value is unique for every card.

Integrated Circuit Card Private Key parameters are configured in the "RSA Keys for <parameter name>" form (see Fig. 34).

RSA Keys for VSDC DDA — << < > >> 1 of 1

Key Algorithm	Key Name	Key Type	Date To	RSA Modulus Length	RSA Public Exponent	Used as MK	Serial Number	Is Active	Storage Form
RSA	ICC Key	ICC Key	01/01/20 00:0	128	03			Active	HSM / Host / Hex

Ins Del Query Actions Certificates Options

Fig. 34. Form for configuring the Integrated Circuit Card Private Key of a card

In this form, the following fields must be filled in for each Integrated Circuit Card Private Key: *Key Type* (select the "ICC Key" value in this field), *RSA Modulus Len*, *RSA Public Exponent.*

> ⚠ Do not generate the key by selecting the "Manage" context menu item accessed by clicking the [Actions] button in this form.

4.3.3.4 Mode for pre-generation of Integrated Circuit Card Private Keys

If it is necessary to generate a large number of Integrated Circuit Card Private Keys, which can require a significant amount of time, it is recommended to use the key pre-generation mode.

The pool of pre-generated ICC keys is stored in a separate table, PM_PREGENED_KEYS. The algorithm for generating ICC keys depends on the type of HSM (for more information, see the section "Generating RSA ICC Key Pool").

To do so, use the following settings:

- Add a new record to the "RSA Keys for <parameter name> form (see Fig. 35), filling in the *Key Type*, *RSA Modulus Len*, *RSA Public Exponent* fields. In addition, specify the value "Active for Pre-Generation" value in the *Is Active* field.

RSA Keys for VSDC DDA

Key Algorithm	Key Name	Key Type	Date To	RSA Modulus Length	RSA Public Exponent	Used as MK	Serial Number	Is Active	Storage Form
RSA	ICC Key	ICC Key	01/01/20 00:0	128	03			Active for Pre-Generation	HSM / Host / Hex

Ins Del Query Actions Certificates Options

Fig. 35. Configuring the mode for pre-generation of Integrated Circuit Card Private Keys

- Specify the number of keys to be generated. To do so, in the "Parameters for <name of financial institution>" form (see Fig. 13 in the section "Smart Card Issuing Parameters", click the [Options] button, and in the "Options for <name of card product>" form (see Fig. 36) add the parameter "ICC Keys To Gen", specifying the required number of keys in the *Value* field.

Options for VSDC DDA

Option	Value
ICC Keys To Gen	20
ICC Key Format	03

Ins Del Query Long Value

Fig. 36. Number of keys to be generated

> In this form it is recommended to also specify the key format using the "ICC Key Format" parameter. Key formats are described in the section "ICC RSA Key Format" of the document "Importing and Exporting Card Production Tasks in XML Format".

Keys are generated in one of the following ways:

- In the "RSA Keys for <name of parameter>" form (see Fig. 35), select the record with the value "Active for Pre-Generation" in the *Is Active* field and click the [Actions] button. In the context menu that opens, select the item "PRE-generate ICC Keys". Records of generated keys are accessible in this form, and the value "Pre-Generated" will be specified in the *Is Active* field of each record.
- Select the user menu item "EMV Smart Cards → Card Production → RSA ICC Keys PRE-Generation → RSA ICC Keys PRE-Generation". The "RSA ICC Keys PRE-Generation" form will open (see Fig. 37) containing a list of all the records from the "RSA Keys for <parameter name>" form (see Fig. 35) for which it is necessary to generate Integrated Circuit Card Private keys.

RSA ICC keys PRE-generation

Key Length	Public Exponent	Storage Form	ICCF	ICGM	ICC Keys to Gen	ICC Keys	Template Code
120	03	HSM / Host / Hex	CRTM	DEF	150	26	120/03/HH/CRTM_DEF
120	03	HSM / Host / Hex	PQ	DEF	180	58	120/03/HH/PQ_DEF
128	03	OWSeM / Host / Hex	PQ	DEF	64	55	128/03/WH/PQ_DEF
64	03	OWSeM / Host / Hex	13	DEF	25	18	64/03/WH/13_DEF
64	03	HSM / Host / Hex	PQ	DEF	170	79	64/03/HH/PQ_DEF

Ins Del Query Proceed Parameters

Fig. 37. List of keys for pre-generation

To generate keys, click on the [Proceed] button in this form, and select the one of the context menu items:

- "Generate keys for current row" – generate keys for the current record.
- "Generate keys for all" – generate keys for all records in the table.
- "Wipe ICC keys" – delete pre-generated private keys for the selected row (card). This functionality can be used, for example, if the key length or format has changed.

> For more information about pre-generation of RSA ICC keys, see the section "Generating RSA ICC Key Pool").

4.4 Issuer Scripts

During the entire validity period of a card, it may receive the following issuer scripts from its issuer:

- Change PIN
- Unblock PIN
- Block card
- Block application
- Unblock application
- Reconfigure Risk Scheme
- Send a response cryptogram to the card (ARPC – Authorization Response Cryptogram)

4.4.1 Configuring Issuer Scripts

Issuer scripts are configured in the "Commands for <parameter name>" form (see Fig. 38). The form is opened by clicking the [Commands] button in the "EMV for <parameter name>" form (see "Card Applications").

> Note that the parameters of issuer scripts are set in the corresponding Risk Scheme templates (see "Viewing the list of issuer scripts"). In order to ensure compatibility with previous versions, the system allows issuer script parameters to be configured in the "Commands for <parameter name>" form.

The complement and parameters of issuer scripts must be defined in compliance with the requirements, on the card microchip used by the issuer, of the appropriate payment system. This section's figures show the forms containing the sets of issuer script parameters that must be defined for the respective card types.

Commands for MChip2.1 Lite — 1 of 13

Script Command	EMV Command Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
MCHIP2 Upd LCOL	84	DC	02	AC	0	9	2	Numeric	No
MCHIP2 Upd UCOL	84	DC	03	AC	0	9	2	Numeric	No
MCHIP2 Upd Non Domest Ctr Facto	84	DC	04	AC	0	9	2	Numeric	No
MCHIP2 Application Block	84	1E	00	00	0	8	0		No
MCHIP2 Application Unblock	84	18	00	00	0	8	0		No
MCHIP2 Offline PIN Unblock	84	24	00	00	0	8	0		No
MCHIP2 Upd Lower Cumul Amount	84	DC	05	AC	0	14	12	Numeric	No
MCHIP2 Upd Upper Cumul Amount	84	DC	06	AC	0	14	12	Numeric	No
MCHIP2 Upd Card TVR Action Code	84	DC	07	AC	0	14	12	Numeric	No
MCHIP2 Upd CIAC Offline	84	DC	08	AC	0	14	8	Numeric	No
MCHIP2 Upd CIAC Online	84	DC	09	AC	0	14	8	Numeric	No
MCHIP2 Upd CIAC Denial	84	DC	0A	AC	0	14	8	Numeric	No
MCHIP2 Offline PIN Change	84	24	00	02	0	16	8	Binary	Yes

Ins Del Query

Fig. 38. Parameters of M/Chip2 card application issuer scripts

Commands for MC MChip4 MPAD SDA — 1 of 16

Script Command	EMV Command Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
MCHIP4 MPAD Limit Set	84	DA	00	CB	0	14	12	Numeric	No
MCHIP4 Offline PIN Unblock	84	24	00	00	0	8	0		No
MCHIP4 MPAD Lower Limit Set	84	DA	00	CA	0	14	12	Numeric	No
MCHIP4 ARPCRC bit					0	0	4		No
MCHIP4 Application Block	84	1E	00	00	0	8	0		No
MCHIP4 Application Unblock	84	18	00	00	0	8	0		No
MCHIP4 Upd CIAC Denial	84	DA	00	C3	0	11	3	Binary	No
MCHIP4 Upd CIAC Offline	84	DA	00	C4	0	11	3	Binary	No
MCHIP4 Upd CIAC Online	84	DA	00	C5	0	11	3	Binary	No
MCHIP4 Upd LCOL	84	DA	9F	14	0	9	1	Binary	No
MCHIP4 Upd UCOL	84	DA	9F	23	0	9	1	Binary	No
MCHIP4 Upd Cur Table	84	DA	00	D1	0	33	25	Binary	No
MCHIP4 Upd Appl Crtl	84	DA	00	D5	0	10	2	Binary	No
MCHIP4 Upd Add Check Table	84	DA	00	D3	0	26	18	Binary	No
MCHIP4 Offline PIN Change	84	24	00	02	0	16	8	Binary	Yes
MCHIP4 Card Block	84	16	00	00	0	8	0		No

Ins Del Query

Fig. 39. Parameters of M/Chip4 card application issuer scripts

Commands for VSDC SDA << < > >> 13 of 13

Script Command	EMV Command Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
Card Block	84	16	00	00	0	8	0		No
Application Block	84	1E	00	00	0	8	0		No
Application Unblock	84	18	00	00	0	8	0		No
Offline PIN Unblock	84	24	00	00	0	8	0		No
Upd Tot. Cons Intl Limit-CURR	04	DA	9F	53	0	9	1	Binary	No
Upd Tot Cumul Amount Limit	04	DA	9F	54	0	14	12	Numeric	No
Upd VSDC LCOL	04	DA	9F	58	0	9	1	Binary	No
Upd VSDC UCOL	04	DA	9F	59	0	9	1	Binary	No
Upd Cum Tot Trans Amt Upper Lim	04	DA	9F	5C	0	14	12	Numeric	No
Upd Tot Cumul Amt Limit-Dual Cur	04	DA	9F	75	0	14	12	Numeric	No
Upd Curr Conversion Factor	04	DA	9F	73	0	12	8	Numeric	No
Upd Tot. Cons Intl Limit-CN	04	DA	9F	72	0	9	1	Binary	No
Offline PIN Change	84	24	00	02	0	24	16	Binary	Yes

Ins Del Query

Fig. 40. Parameters of VSDC card application issuer scripts

Commands for JSmart << < > >> 1 of 14

Script Command	EMV Command Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
JCB Application Unblock	84	18	00	00	0	0	0		No
JCB Application Block	84	1E	00	00	0	0	0		No
JCB PIN Unblock	84	24	00	00	0	0	0		No
JCB PIN Change	84	24	00	02	0	16	8	Binary	Yes
JCB Upd 9F56-CTTAL	04	DA	9F	56	0	14	12	Numeric	No
JCB Upd 9F57-UDCOL	04	DA	9F	57	0	9	1	Binary	No
JCB Upd 9F58-LCDOL	04	DA	9F	58	0	9	1	Binary	No
JCB Upd 9F59-UCIOL	04	DA	9F	59	0	9	1	Binary	No
JCB Upd 9F5A-LCIOL	04	DA	9F	5A	0	9	1	Binary	No
JCB Upd 9F5B-MDOTA	04	DA	9F	5B	0	14	12	Numeric	No
JCB Upd 9F64-CTTAUL	04	DA	9F	64	0	14	12	Numeric	No
JCB Upd 9F65-Curr Conv	04	DA	9F	65	0	32	48	Numeric	No
JCB Upd 9F66-CAC	04	DA	9F	66	0	13	5	Binary	No
JCB Card Block	84	16	00	00	0	0	0		No

Ins Del Query

Fig. 41. Parameters of JSmart card application issuer scripts

Commands for AMEX EMV Chip << < > >> 1 of 9

Script Command	EMV Command Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
AMEX Card Block	84	1E	00	00	0	8	0		No
AMEX Appl Block	84	1E	00	00	0	8	0		No
AMEX Appl Unblock	84	18	00	00	0	8	0		No
AMEX PIN Unblock	84	24	00	00	0	8	0		No
AMEX PIN Change	84	24	00	02	0	16	8	Binary	Yes
AMEX Upd 9F53	04	DA	9F	53	0	9	1	Binary	No
AMEX Upd 9F54	04	DA	9F	54	0	14	12	Numeric	No
AMEX Upd 9F58	04	DA	9F	58	0	9	1	Binary	No
AMEX Upd 9F59	04	DA	9F	59	0	9	1	Binary	No

Ins Del Query

Fig. 42. Parameters of AMEX EMV card application issuer scripts

4.4.2 Viewing the list of issuer scripts

It is possible to view the list of issuer scripts. To do so, in the "Chip Schemes" form (see Fig. 4 in the section "Configuring Smart Card Risk Schemes") click the [Template] button. In the "Template for <name of Risk Scheme>" form that opens, click the [Scr.Cmnd] button. The "Scr.Cmnd for <name of Risk Scheme template>" form will open (see Fig. 43).

Scr.Cmnd for MCHIP 2 Lite Generic Easy Setup << < > >> 1 of 10

Card Type	Script Command	EMV Cmnd Class	Instruction	Parm 1	Parm 2	LE	LC	Data Length	Data Format	Encrypt Data
MCHIP	MCHIP2 Upd LCOL	84	DC	02	AC	0	9	2	Numeric	0
MCHIP	MCHIP2 Upd UCOL	84	DC	03	AC	0	9	2	Numeric	0
MCHIP	MCHIP2 Upd Non Domest Ctr Factor	84	DC	04	AC	0	9	2	Numeric	0
MCHIP	MCHIP2 Upd Lower Cumul Amount	84	DC	05	AC	0	14	12	Numeric	0
MCHIP	MCHIP2 Upd Upper Cumul Amount	84	DC	06	AC	0	14	12	Numeric	0
MCHIP	MCHIP2 Upd Card TVR Action Code	84	DC	07	AC	0	14	12	Numeric	0

Ins Del Query

Fig. 43. List of issuer scripts

4.4.3 Generating an issuer response cryptogram

When a contactless transaction is made with a smart card, WAY4 can send the payment application special control bits together with the issuer response cryptogram - Authorisation Response Cryptogram (ARPC).

Two technologies are supported for sending control bits:

- ARPC Response Code (ARPC RC)
- Card Status Update (CSU).

A card's payment application parameters determine which technology is used.

To generate ARPC RC, the parameters(*Parm Type*) "APPROVE_ONLINE_TRANS" and "DECLINE_ONLINE_TRANS" must be defined in the risk scheme. To generate CSU - the parameters (*Par m Type*) "CPA CSU *".

Only one of the two parameter groups can be defined per risk scheme.

4.4.4 Blocking cards with several card applications

For smart cards, a special type of command is used to block ("APPLICATION BLOCK") and unblock ("APPLICATION UNBLOCK") card applications, which makes it possible to temporarily block one or several card applications.

This allows use of a card on which one of the applications may be blocked up to a certain time.

If a card is lost or stolen, all the card's applications can be blocked simultaneously.

When attempting authorization, to prevent further use of the card, a special "CARD BLOCK" command must be sent to the blocked number of one of the smart card's applications.

To to so, in the *Chip card action type field of the* "Contract Statuses" handbook, menu item Full → Configuration Setup → Contract Types → Contract Statuses, set "CARD BLOCK" for cards with the corresponding statuses ("card lost", "card stolen").

Contract Statuses

<< < > >> 1 of 1

Category	Name	Code	Is Valid	External Code	Code Parms	Chip Card Action Type
Card	PickUp L 41	41	Decline	41		Block Card

Ins Del Query

Setting up the "CARD BLOCK" action for a card that has been lost

5. Limiting the Number of Offline PIN Unblock Attempts

In WAY4 it is possible to limit the number of offline PIN unblock attempts.

To use this functionality, the following settings must be made:

1. To the list of Additional Online Services, add a new type with the code "OFFLINE_PIN_UNBLOCK". To do so, select the user menu item "Full → Configuration Setup → Merchant Device Setup → Additional Online Services" and add the new type of online service in the "Additional Online Services" form (see Fig. 44).

Additional Online Services

Contract Cat	Group Code	Code	Is Active	Name	Is Personal	Use Contract Quota	Relation	Extra Doc Tags	Usage Operation
Card		OFFLINE_PIN_UNBLOCK	Yes	OFFLINE_PIN_UNBLOCK	Card Service				

Ins Del Query Services Full Info Quota

Fig. 44. Adding an additional online service

1. Register a new transaction type in the "Transaction – All" list (Full → Configuration Setup → Transaction Types → Transaction – All). Then specify a special type of message in the form "Msg Types for <...>" opened by clicking the [Msg Types] button after selecting the created transaction type from the "Transaction – All" list (see Fig. 45).

Transactions - All

Service Class	Source	Target	Name	DR\CR	Previous	Chain Type	Is Authorized	s Require	Category	RBS Code	RBS Rev Code	Dispute Class	Trans Type IDT
Additional Online Service	Device	Card	Offline PIN Unblock	None		Original		Yes	Individual				

Ins Del Query Fill SubTypes Msg Types Reasons Requirements Msg Dict

Msg Types for Offline PIN Unblock

Channel	Name	Code	Category	Is Authorization	Trans Type	Msg Details	Service Class
	Offline PIN Unblock	OFFLINE_PIN_UNBLOCK	Request	Auth	Offline PIN Unblock		Additional Online Service

Ins Del Query

Fig. 45. Creating a transaction type and corresponding message type

1. Create a new Event Type in the "Event Types" form (Full → Configuration Setup → Products → Event Types). An Event Type is shown in Fig. 46.

Event Types

Product	Contract	Institution	Name	Code	Group Code	Duration Type	Duration	Next Event	Custom Code	Special Parms
Issuing	Card	Principal	Disable Offline PIN Unblock	DISABLE_OFFL_PIN_UNBLK		Unique	0			

Ins Del Query Check Messages Full Info Event Chain Used By Classifiers

Fig. 46. Creating a new Event Type

1. Add the following record (see Fig. 47) to the "Usage Operations" list (Full → Configuration Setup → Alerting Setup → Usage Operations).

Usage Operations | << < > >> | 1 of 1

Name	Usage Type	Event Code
Incorrect PIN	Negative RC	

Ins Del Query

Fig. 47. Adding a record to the "Usage Operations" list

For this operation register the authorisation request response codes from the "Usage Operations" dictionary. Response codes are registered in the form "Response Code Usage" (Full → Configuration Setup → Alerting Setup → Response Code Usage). Response codes are shown in Fig. 48.

Response Code Usage | << < > >> | 2 of 2

Contract Category	Response Code	Usage Operation
Card	Incorrect PIN	Incorrect PIN
Card	Allowable number of PIN tries exceeded	Incorrect PIN

Ins Del Query

Fig. 48. Configuring response codes

1. In the Service Package used for card contracts, create a usage limiter. To do so, in the form Private Card Service Packs" (Full → Configuration Setup → Products → Issuing Private Products → Private Card Service Packs) select the required Service Package, click the [Usage] button, and add the limiter to the form "Usage For <...>" (see

Usage for 001-Our Priv MCHIP | << < > >> | 1 of 1

Usage Code	Usage Type	SIC Group	Channel	Operation	Period	Period Type	Usage Event	Fee Type	Max #	Max Amnt	Max Pcnt	Max Sngl Amnt	Amnt Curr	Is Active	Is Ready
OFF_PIN_UNBLK	Negative RC			Incorrect PIN	1	Forever	Event Only		3	0,00	0,00	0,00		Yes	Ready

Ins Del Query Details Approved Messages

Fig. 49. Configuring usage limiters

Note that the maximum number of offline PIN unblock attempts are specified in the *Max #* field. Moreover, in the "Details for <...>" form with additional information about the limiter, fill in the *Trans Type*, *Event Type* and *Custom RC* fields (see Fig. 50).

Details for Usage for 001-Our Priv MCHIP

Conditions

Channel
Area
SIC Group
Contra FI
Preference Type
Trans Type: Offline PIN Unblock
Trans Condition
Service
Serv Group Code
Max Trans Amount: 0,00
Min Trans Amount: 0,00

Inverse Conditions

Hierarchy

Parent Usage
Exclude from Parent

Balance Type

For Max Amount
For Current Amount

Threshold Calculation

Algorithm
Cycles: 0
Tariff

Action

Event Type: Disable Offline PIN Unblock
Custom RC: Successfully completed
Usage Fee
Spc Parms

Fig. 50. Configuring additional limiter parameters

1. In the form "Private Card Service Packs", create an Additional Service Pack to which the required target services must be added, in the *Transaction Type* field, specify the transaction type created in Item 2. An example of a Service Package is shown in Fig. 51

Private Card Service Packs (1 of 1)

Name	Contract Type	Parent Pack	For Contracts	Use Default	Code	Fee Contract	Special Parms	Is Ready
001-Offline PIN Unblock	Our EuroCard/MasterCard		Additional	For Dispute				Ready

Ins | Del | Query | Approve | Details | Misc | Source | Target | Additional | Usage | Messages | Events | Preferred | Tariffs

Target for 001-Offline PIN Unblock (3 of 3)

Source Type	Transaction Type	Condition	Currency	Rate Type	Fee Dir	Fee Curr	Base	%	Min	Is Ready	Name	Fee Code	Account Type	Fee Account
MasterCard Acq	Offline PIN Unblock			Middle	None		0,00	0,00	0,00	Ready	Offline PIN Unblock (MasterCard Acq)			
EuroCard Acq	Offline PIN Unblock			Middle	None		0,00	0,00	0,00	Ready	Offline PIN Unblock (EuroCard Acq)			
Our ATM	Offline PIN Unblock			Middle	None		0,00	0,00	0,00	Ready	Offline PIN Unblock (Our ATM)			

Ins | Del | Query | Full Info | History

Fig. 51. Creating an Additional Service Pack

1. To ensure counters are reset when after a successful offline PIN unblock, for each of the Additional Service Pack's services, specify the tag "ZEROIZE_USAGE_COUNTERS=<usage_code>;"

in the *Service Details* field, where usage code is the code of the usage limiter created in the Service Pack. In the example, the code "OFF_PIN_UNBLK" is specified.

> If the "RESET_PTC_ON_PIN_SET" parameter with the "N" value is set in a smart card's Risk Scheme (see Fig. 6 in the section "Configuring Smart Card Risk Schemes"), when an offline PIN is changed successfully, the PIN try counter is not reset. If the "RESET_PTC_ON_PIN_SET" parameter is not set or its value is "Y", when the PIN is changed successfully, the PIN try counter will be reset.

Connect the Service Pack created in Item 6 to the main Service Package for which the usage limiter was created (see Item 5). Configure disabling of the Additional Service Pack when an Event with the type specified in Item 3 opens.

6. Automatically Unblocking Offline PIN after Successful PBT

In WAY4 it is possible to reset the offline PIN counter the first time the PIN is successfully entered online; i.e. when a PBT (PIN Based Transaction) is made successfully.

To do so, in the form for configuring smart card Risk Schemes (see Fig. 6 in the section "Configuring Smart Card Risk Schemes") define the parameter "OAC CVR & PIN Try Lim Exc RC00", specifying the value "00004000" for Visa ("VSDC" cards) and "000000080000" for MasterCard ("MCHIP" cards).

After this setting has been made, the number of PIN attempts is checked as follows:

- If the smart card's number of offline PIN attempts has been exceeded, the smart card generates a request to enter an online PIN.
- If the cardholder entered the correct value of the online PIN, WAY4 generates an issuer script to unblock the offline PIN. In this case, the offline and online PIN counters will be synchronised.
- If the cardholder entered an incorrect value for the online PIN, WAY4 assigns the maximum value to the online PIN counter; i.e., it blocks the online PIN. Consequently, the card will be blocked, making it impossible for it to be used for transactions.

7. Personalisation bureaus

A personalisation bureau (perso bureau) is a hardware and software system used to personalize plastic. Cards are personalized based on parameters prepared in WAY4 (see "Smart Card Issuing 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.

7.1 Registering a Perso Bureau (Working with Perso Bureaus)

The "Perso Bureaus" form contains a list of perso bureaus, menu item Full → Configuration Setup → Card Production Setup → Perso Bureaus (see Fig. 52).

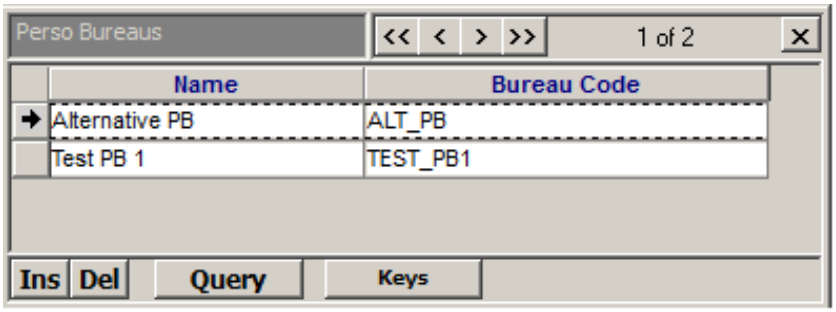


Fig. 52. List of perso bureaus

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.

7.2 Generating Transport Keys (Working with Perso Bureaus)

Transport keys are generated in the standard way, using a hardware security module (see the section "3 -DES Keys").

Transport keys are generated in the "Keys for < >" form (see Fig. 53) in the standard way (see the section "Key Generation"). 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

Perso Bureau	Key Algorythm	Key Type	DES Key	DES Key Check	Storage Form
1	3DES ABA	PIN Export Key	U7568FA7C6EB1C8A84A5290AA90ADCB7C	E2F243	HSM / Host / Hex
1	3DES ABA	Key Encryption Key	UA940CC330472671D0CDA49CCF19924DD	EE21F1	HSM / Host / Hex

Ins Del Query Manage Options

Fig. 53. PEK transport key

7.3 Pipes in which a Perso Bureau ID is Set (Working with Perso Bureaus)

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

7.4 Default Perso Bureau (Working with Perso Bureaus)

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. 54).

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 (28 of 80)

Name	Code	PAN MIN	PAN MAX	PIN Len	ICA	Card Type	Encoding Method	PVKI	Is Ready	Ready Till	Bank
[ITest]Main PayPass OW	ITEST_MAIN_PP_OW	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[ITest]Main PayPass Dc	ITEST_MAIN_PP_ZPSN_O	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[ITest]Main PayPass Dc	ITEST_MAIN_PP_ZPSN_TH	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[ITest]Sub PayPass OW	ITEST_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 [ITest]Main PayPass OW (12 of 15)

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	PVKI+PVV+"0"+"0000"+CVC1
Track 1 Discr. Data Format	PVKI+PVV+"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. 54. Default personalization bureau for the [ITest]Main PayPass OW set of card production parameters

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

- *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. 55) opened by clicking on the [Bureau Keys] button (see Fig. 54).

Bureau Keys for [ITest]Main PayPass OW (1 of 2)

Perso Bureau	Key Algorythm	Key Type	DES Key	DES Key Check	Storage Form
25	3DES ABA	Key Encryption Key	C6351A596166E48CA687D56BB8D50796	EE21F1	OWSeM / Host / Hex
25	3DES ABA	PIN Export Key	0B7DF6F9886A8C05053E65214C0342CD	E2F243	OWSeM / Host / Hex

Query | Manage | Options

Fig. 55. Personalization bureau transport keys

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

8. Generating RSA ICC Key Pools

Generation of an ICC key pool depends on the type of HSM:

- Thales™ payShield 9000 Card Issuer Firmware or SafeNet devices through the OWSEM interface.
- Thales™ payShield 9000 Base Firmware.

When generating a pool, the HSM on which ICC keys are pre-generated is determined.

If the device supports generation of ICC keys only under a KEK transport key, a key is created under the corresponding key of the selected perso bureau. These devices include Thales™ payShield 9000 Card Issuer Firmware and SafeNet devices operating through the OWSEM interface.

If the device supports generation of ICC keys under an HSM LMK key, the procedure for generating the pool is different: an LMK key check value is requested for the selected device. Then, according to the key check value, a record for the LMK is found in the PM_KEYS table (see Fig. 57). If the PM_KEYS table doesn't have a record for this check value, the record will be created automatically. The ICC key that was created will be saved in the PM_PREGENED_KEYS table specifying a link to the LMK key that was used.

Rules for pre-generation of ICC keys are described in detail in the section "Mode for pre-generation of Integrated Circuit Card Private Keys". In addition, the default perso bureau should be specified for PM Parms (see the section "Default Perso Bureau").

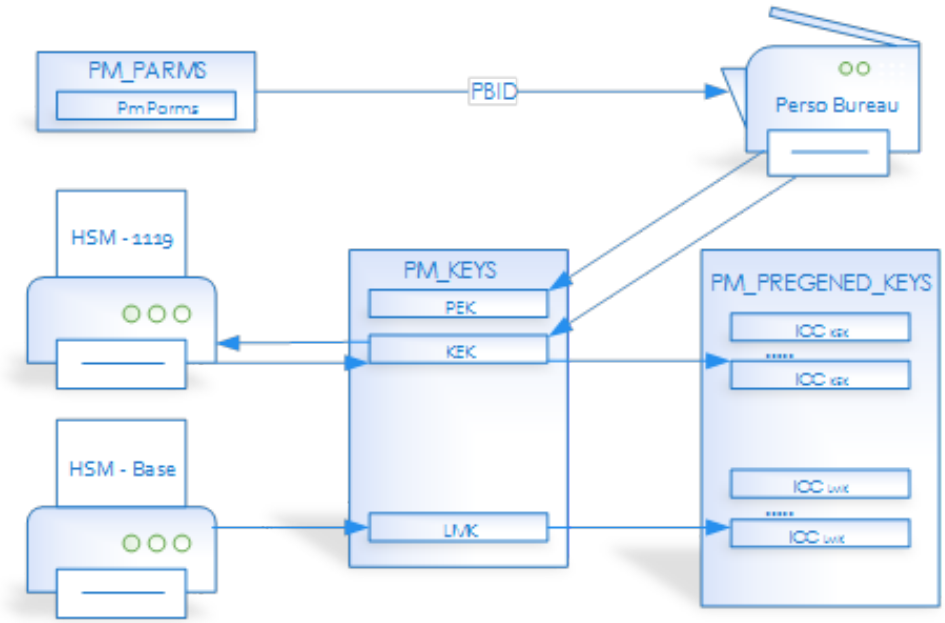


Fig. 56. Generating and storing RSA ICC keys

8.1 LMK Keys

Information about LMK keys used when generating ICC keys can be viewed in the "LMK Keys" form, menu item Full → Configuration Setup → Card Production Setup → LMK Keys (see Fig. 57).

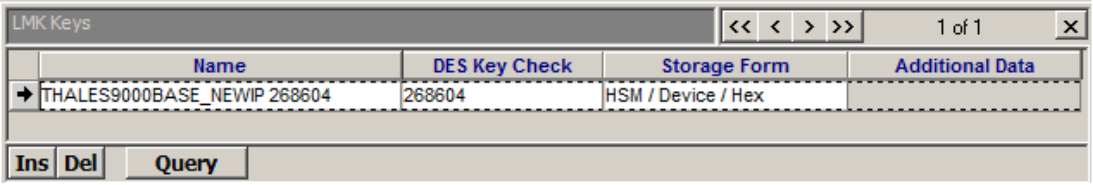


Fig. 57. List of LMK keys for ICC LMK

The table contains the following fields:

- *Name* – key name.
- *DES Key Check* – key check value (KCV).
- *Storage Form* – key storage method. The field value is "HSM / Host / Hex" for keys generated on a Thales device.
- *Additional Data* – reserved. Not used in the current version.