



## Installation and Configuration Manual

# Настройка параметров системы WAY4 для выпуска карт с магнитной полосой

03.51.30

03.02.2021

# СОДЕРЖАНИЕ

<b>1</b>	<b>Настройка аппаратного модуля безопасности</b>	<b>5</b>
1.1	Настройка Thales HSM в системе WAY4	5
1.2	Настройка SafeNet ProtectServer в системе WAY4	5
1.3	Настройка Gemalto Luna HSM в системе WAY4	5
1.4	Настройка параметров соединения рабочей станции с аппаратным модулем безопасности	6
<b>2</b>	<b>Параметры производства банковских карт</b>	<b>11</b>
2.1	Параметры производства карт для финансового института	11
2.2	Параметры контроля подлинности	12
2.3	Параметры производства карт	15
2.3.1	Ключи шифрования	19
2.3.2	Настройка параметров ключей для аппаратных модулей безопасности различной конфигурации	27
2.3.3	PIN-конверт	29
2.3.4	Печать величины PIN2	31
2.3.5	Трансляция ключей между двумя аппаратными модулями безопасности	33
2.3.6	Изменение набора параметров производства карт в пределах одного диапазона PAN	34
2.3.7	Автоматическое обнуления счетчика числа попыток ввода неправильного PIN-кода при перевыпуске карты	35
<b>3</b>	<b>Организация работы с бюро персонализации</b>	<b>36</b>
3.1	Регистрация персобюро	36
3.2	Формирование транспортных ключей	37
3.3	Пайпы, на которых задается идентификатор персобюро	37
3.4	Персобюро, используемое по умолчанию	38

Система подготовки данных для персонализации предназначена для конфигурирования параметров производства банковских карт (карт с магнитной полосой и смарт-карт), расчета и хранения криптографических величин, а также формирования шаблонов PIN-конвертов.

В данном документе приведено описание действий по настройке параметров производства карт с магнитной полосой. Описание действий по настройке специфичных параметров производства смарт-карт приведено в документе "Настройка параметров системы WAY4 для производства смарт-карт".

Функционирование модуля подготовки данных для персонализации карт обеспечивается рабочей станцией банка (процессингового центра), подключенной к аппаратному модулю безопасности (HSM), предназначенному для формирования данных, необходимых при производстве пластиковых карт. К данному устройству HSM подключается принтер для печати PIN-конвертов.

Настоящий документ предназначен для администраторов системы WAY4 (сотрудников банков или процессинговых центров), обеспечивающих настройку параметров системы подготовки данных для персонализации при производстве карт с магнитной полосой.

При работе с данным документом рекомендуется пользоваться следующими источниками из комплекта документации OpenWay:

- "Работа с DB Manager";
- "Редактор меню";
- "Модуль эмиссии. Руководство пользователя";
- "Настройка параметров системы WAY4™ для выпуска смарт-карт";
- "Продукты и суб-типы контрактов";
- "Загрузка и выгрузка заданий на производство карт в формате XML";
- "Установка и настройка модуля управления криптографическим устройством ProtectServer в системе WAY4™";
- "Выгрузка криптографических ключей в платежную систему MasterCard".

В документе используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- названия кнопок экранных форм приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: "Database => Change password";
- комбинации клавиш, используемые при работе с DB Manager, приводятся в угловых скобках, например, <Ctrl>+<F3>;
- различные переменные значения, например, имена каталогов и файлов, а также пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS\_HOME>;



Предостережения в связи с возможностью совершения неправильных действий.



Сообщения, содержащие информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

# 1 Настройка аппаратного модуля безопасности

Для выполнения криптографических операций при подготовке данных для персонализации банковских карт в системе должен быть установлен аппаратный модуль безопасности (HSM).

В системе WAY4 поддерживаются следующие типы аппаратных модулей безопасности:

- Thales™payShield 9000;
- SafeNet™:
- SafeNet ProtectServer Gold (PSG).
- SafeNet ProtectServer External (PSE).
- SafeNet PSE-Refresh (с одним COM-портом) в режиме ручного ввода LMK без использования smart card.
- SafeNet PSI-e (с одним COM портом) в режиме ручного ввода LMK без использования smart card.
- SafeNet PSE 2 в режиме ручного ввода LMK без использования smart card.
- SafeNet PSI-e 2 в режиме ручного ввода LMK без использования smart card.
- Gemalto SafeNet Payment HSM.

## 1.1 Настройка Thales HSM в системе WAY4

Подробная инструкция по установке и настройке устройств Thales HSM приведена в документе "PayShield 9000 Installation Manual".

## 1.2 Настройка SafeNet ProtectServer в системе WAY4

Подробная инструкция по установке и настройке устройств SafeNet приведена в документе "Установка и настройка модуля управления криптографическим устройством ProtectServer в системе WAY4™".

## 1.3 Настройка Gemalto Luna HSM в системе WAY4

Инструкция по установке и настройке устройств Gemalto Luna приведена в пакете документов "SafeNet Payment HSM 2.2.0".

## 1.4 Настройка параметров соединения рабочей станции с аппаратным модулем безопасности

Для настройки соединения рабочей станции системы подготовки данных для персонализации с аппаратным модулем безопасности следует выбрать пункт меню "Full → Configuration Setup → Card Production Setup → Security Device". По этой команде на экране будет представлена форма "Security Device" (см. Рис. 1).

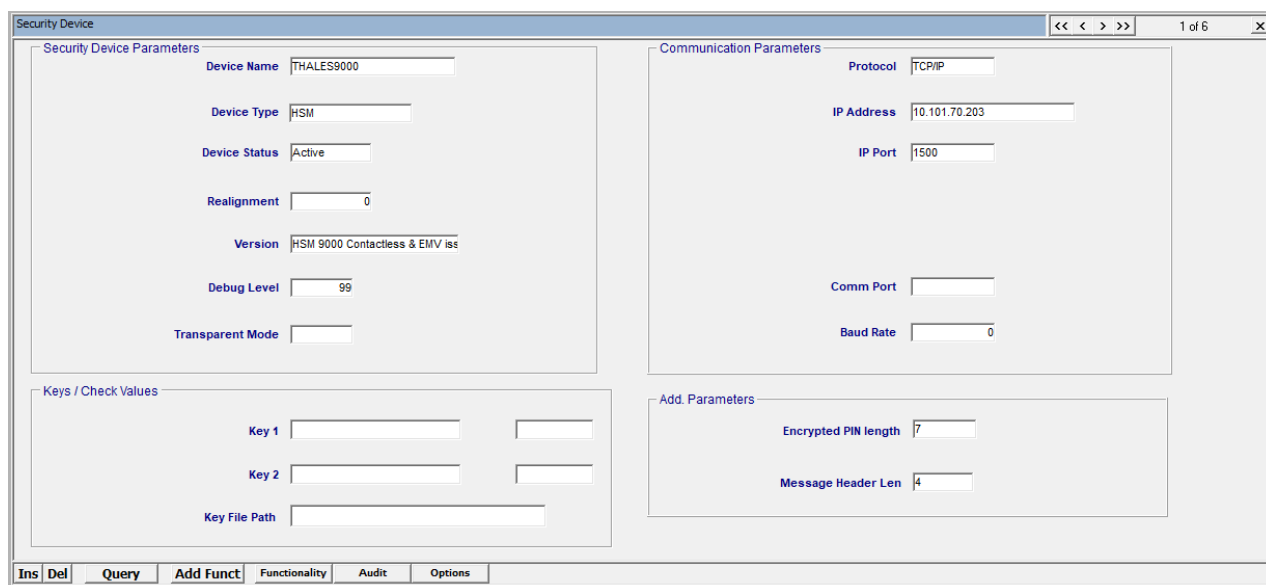


Рис. 1. Форма для настройки параметров соединения с аппаратным модулем безопасности

В данной форме необходимо заполнить следующие поля:

- *Device Name* – наименование устройства.
- *Device Type* – тип устройства.
- "HSM" – устройство HSM производства Thales™;
- "OWSEM" – устройство ProtectServer производства SafeNet.
- "GL" – устройство SafeNet Payment HSM производства Gemalto.
- *Device Status* – статус устройства; в данном поле могут быть указаны следующие значения:
- "Active" – используется для активизации устройства, к которому относится текущая запись; для используемой в текущий момент записи данное поле должно содержать значение "Active";
- "Inactive" – используется для деактивации устройства, к которому относится текущая запись.
- *Realignment* – количество PIN-конвертов, печатаемых на принтере до его остановки для того, чтобы вручную поправить подачу бумаги;



По умолчанию в данном поле указывается значение "10". В случае если в остановках печати для позиционирования бумаги нет необходимости, в данном поле следует указывать значение "0".

- *Version* – версия программного обеспечения устройства:
- "HSM 5.04 Smart OW" – для SafeNet ProtectServer;
- "HSM 8000 Smart" – для Thales™ HSM 8000;
- "HSM 8000 Smart & Perso" – для Thales™ HSM 8000 co Smart Card Issuer Firmware;



В текущей версии устройство Thales™ HSM 8000 не поддерживается. Значение оставлено для совместимости с предыдущими версиями.

- "HSM 9000 Smart & Perso" – для Thales™ HSM 9000 co Smart Card Issuer Firmware;
- "HSM 9000 Contactless & EMV Issuing" – для Thales™ HSM 9000 с базовой прошивкой (HSM9-LIC001 Base Firmware версии 2.2a и выше) и набором лицензий "HSM9-LIC002 RSA License", "HSM9-LIC011 Magnetic Stripe Contactless Card Data Preparation License" и "HSM9-LIC016 EMV based Card Data Preparation License";
- "GL 2.x Native" – для SafeNet Payment HSM производства Gemalto.
- *Debug Level* – уровень детализации информации о выполнении заданий, записываемой в файл журнала; возможные значения:
- "0" – сохраняется только информация об ошибках (уровень "Error");
- от "1" до "49" – сохраняются информационные сообщения и сообщения об ошибках (уровень "Info");
- от "50" до "74" – сохраняется отладочная информация (уровень "Debug");
- от "75" до "98" – сохраняется отладочная информация, но более детальная, чем для уровня "Debug", при этом не сохраняется дампы команд, отправленных на HSM.
- "99" (или более) – выводятся все сообщения, включая дампы запросов и ответов от HSM.

Информация о расположении log-файлов журнала сообщений будет представлена в журнале выполнения процессов в форме "Process Log" (Full → Process Log → Process Log). Для каждого процесса, взаимодействующего с HSM, в журнале будет содержаться сообщение "Security Device Interaction Logs directory: <Path>". Следует иметь в виду, что данные log-файлы являются временными, т.е. содержатся в каталоге только до момента успешного завершения работы клиентского приложения (DB Manager / WAY4 Manager).

- *Transparent Mode* – в данном поле в целях совместимости с режимом работы для выпуска смарт-карт рекомендуется установить значение "Yes", выполнив соответствующие настройки на устройстве (см. раздел "Настройка Thales HSM в системе WAY4" документа "Настройка параметров системы WAY4 для производства смарт-карт").
- *Protocol* – тип протокола, с помощью которого устанавливается соединение аппаратного модуля безопасности с рабочей станцией системы подготовки данных для персонализации:

- "TCP/IP" – протокол TCP/IP;
- "Serial" – соединение при помощи интерфейса RS-232.
- *IP Address/IP Port* – поля, в которых следует указать IP-адрес (или DNS-имя) и номера порта для соединения с аппаратным модулем безопасности в случае использования протокола TCP/IP.
- – номер последовательного порта рабочей станции, к которому подключено устройство в случае использования устройства с интерфейсом RS-232.
- *Baud Rate* – поле с выбором из списка значения скорости передачи данных.
- Поля *Key1*, *Key2* и *Key File Path* используются для совместимости с предыдущими версиями – их заполнение необязательно.
- *Encrypted PIN length* – длина зашифрованного значения PIN; значение данного поля определяется как увеличенная на единицу максимальная длина PIN-кода, рассчитываемого на данном устройстве. Например, если на данном устройстве выпускаются карты с длиной PIN-кода 4 или 6 цифр, то в данном поле необходимо указать значение "7". В случае если поле не заполнено (значение "0"), длина зашифрованного PIN-кода равна "5". Данный параметр используется только для устройств Thales (в поле *Device Type* указано значение "HSM"); значение поля должно совпадать со значением параметра "Encrypted PIN length", определенного на устройстве.



Данное поле должно совпадать со значением параметра "Encrypted PIN Length", указанным в настройках аппаратного модуля безопасности Thales.

- *Message Header Len* – длина идентификатора сообщения; идентификатор сообщения добавляется в начало любого сообщения, отправляемого или получаемого от HSM. Значение данного поля должно совпадать со значением аналогичного параметра, определенного на устройстве. По умолчанию (значение "0") длина идентификатора составляет четыре цифры.

При нажатии на кнопку [Add Funct] на экране будет представлено контекстное меню, содержащее следующие пункты:

- "Add Funct" – данный пункт присутствует в системе для обеспечения совместимости с предыдущими версиями.
- "Audit Upload" – предназначен для выгрузки журнала аудита (Audit Log) из аппаратного модуля безопасности. Для просмотра журнала аудита необходимо в данной форме нажать на кнопку [Audit]. В результате на экране будет представлена форма "Audit for <...>" (см. [Рис. 2](#)).
- "Verify Audit" – верификация всех сообщений, содержащихся в выгруженном журнале аудита, т.е. выполнение электронной подписи каждого сообщения и сравнение полученного результата со значением поля *Audit Record MAC* формы "Audit for <...>" (см. [Рис. 2](#)).
- "LMK migration for Audit" – предназначен для формирования новой MAC-подписи (Message Authentication Code) для каждого сообщения из журнала аудита (Audit Log) в случае, если для устройства HSM был изменен LMK-ключ.
- "Load Default Weak PIN Table" – предназначен для загрузки в аппаратный модуль безопасности списка predetermined "слабых" PIN-кодов (например, "0000", "1111"), которые не будут сгенерированы устройством. Данный пункт меню доступен только для



устройств Thales, при этом для выполнения загрузки на HSM необходимо включить соответствующий режим загрузки "слабых" PIN-кодов.

- "Load Weak PIN Table" – предназначен для загрузки в аппаратный модуль безопасности (HSM) списка "слабых" PIN-кодов, которые не будут сгенерированы устройством. Для формирования списка необходимо определить следующие глобальные параметры (Full → Configuration Setup → Main Tables → Additional Global Parameters):
- "PM\_PIN\_LENGTH=<число>" – длина PIN-кода в списке "слабых" PIN-кодов, используемых при определении глобального параметра "PM\_WEAK\_PIN\_TABLE".
- "PM\_WEAK\_PIN\_TABLE=<список значений>" – Определяет список "слабых" PIN-кодов (например, "0000", "1111"). Список содержит "слабые" PIN-коды в открытом виде, которые не должны порождаться аппаратным модулем безопасности (HSM) при генерации новых PIN-кодов. Значения в списке не разделяются пробелами или запятыми; длина каждого PIN-кода определяется глобальным параметром "PM\_PIN\_LENGTH". Максимальное количество загружаемых "слабых" PIN-кодов определено в документации к HSM. Данный пункт меню доступен только для устройств Thales, при этом для выполнения загрузки на HSM необходимо включить соответствующий режим загрузки "слабых" PIN-кодов.
- "Test HSM" – предназначен для тестирования соединения рабочей станции с аппаратным модулем безопасности.

Кнопка [Functionality] формы "Security Device" (см. Рис. 1) присутствует в системе для обеспечения совместимости с предыдущими версиями.

При нажатии на кнопку [Audit] на экране будет представлена форма "Audit for <...>" (см. Рис. 2), содержащая журнал аудита (Audit Log), т.е. информацию о выполнении команд на аппаратном модуле безопасности (HSM).

Audit for HSM Thales 9000										<< < > >>		1 of 463	b	x	
Audit Counter	Produce Date	Upload Date	Command Code	Command Code Type	Settings	Response Error Codes	Audit Record MAC	Random MAC Key							
→ 000001D2	15/08/14 16:12:15	15/08/14 21:02:09	EC	Fraud Event	9000	01	EEA0CCFD69401CBD	F3A578AD7A0106010							
000001D1	13/08/14 10:32:37	13/08/14 14:34:39	UT	User Action	D000	00	FBCD2F2FB75C2A62	AC885F6820EB6E1A4							
000001D0	13/08/14 10:32:04	13/08/14 14:34:39	UT	User Action	D000	00	D0786FAD33F8A672	0526CE448E7B5152C5							
000001CF	13/08/14 10:31:21	13/08/14 14:34:39	UT	User Action	D000	00	2D0A2544ED11FEB4	58666EFFAD00B93FE8							
000001CE	13/08/14 10:31:08	13/08/14 14:34:39	UT	User Action	D000	00	03DC18EA31E576D8	578E4E8255170FCF16							
000001CD	13/08/14 10:30:32	13/08/14 14:34:39	UT	User Action	D000	00	9AA1812FD58A1DCE	E9AA7D663F846737C							
000001CC	13/08/14 10:28:49	13/08/14 14:34:39	UT	User Action	D000	00	F0CDC01227621BBE	046899155AA5EC293							
000001CB	13/08/14 10:03:40	13/08/14 14:34:39	UT	User Action	D000	00	0EF60266D796E151	93CAC889FA95B6950							
000001CA	04/08/14 16:41:02	05/08/14 13:11:02	A1	User Action	D000	00	0AABD3F427A9C493	3CD8259E4A0991F33							
Intr Del Query Verify															

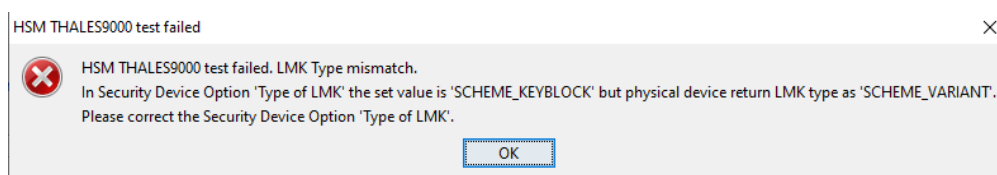
Кнопка [Options] предназначена для доступа к форме "Options for <...>", в которой формируется и хранится дополнительная информация о HSM (см. Рис.).

Option	Value
Type of LMK	SCHEME_KEYBLOCK
LMK Check Value	LMK_KCV
Previous LMK Check Value	LMK_KCV_PREVIOUS

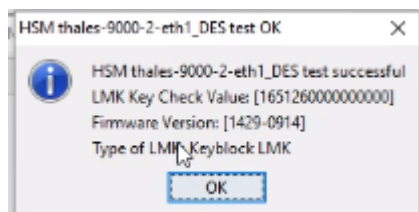
Рис. Дополнительная информация о HSM

Параметр "Type of LMK" может иметь одно из значений: SCHEME\_VARIANT или SCHEME\_KEYBLOCK. Если "Type of LMK" в форме "Options for <...>" указан, следует выполнить проверку поддерживает ли настраиваемый тип устройства указанный формат шифрования: "Variant LMK" или "Keyblock LMK". Проверка выполняется с помощью [Add Funct] → "Test HSM" в форме "Security Device".

Например, если "Type of LMK" задан и имеет значение SCHEME\_KEYBLOCK, но устройство не поддерживает формат "Keyblock LMK", будет сформировано сообщение об ошибке.



Если устройство поддерживает формат "Keyblock LMK", будет сформировано сообщение вида



## 2 Параметры производства банковских карт

В данной главе приведено описание действий по настройке параметров производства карт с магнитной полосой. Описание действий по настройке специфичных параметров производства смарт-карт приведено в документе "Настройка параметров системы WAY4 для производства смарт-карт".

### 2.1 Параметры производства карт для финансового института

Настройка параметров для производства банковских карт для финансового института осуществляется с помощью формы "Bank Production Parameters" (см. Рис. 3), которая открывается путем выбора пункта меню пользователя "Full → Configuration Setup → Card Production Setup → Bank Production Parameters", а также с помощью форм, подчиненных форме "Bank Production Parameters".

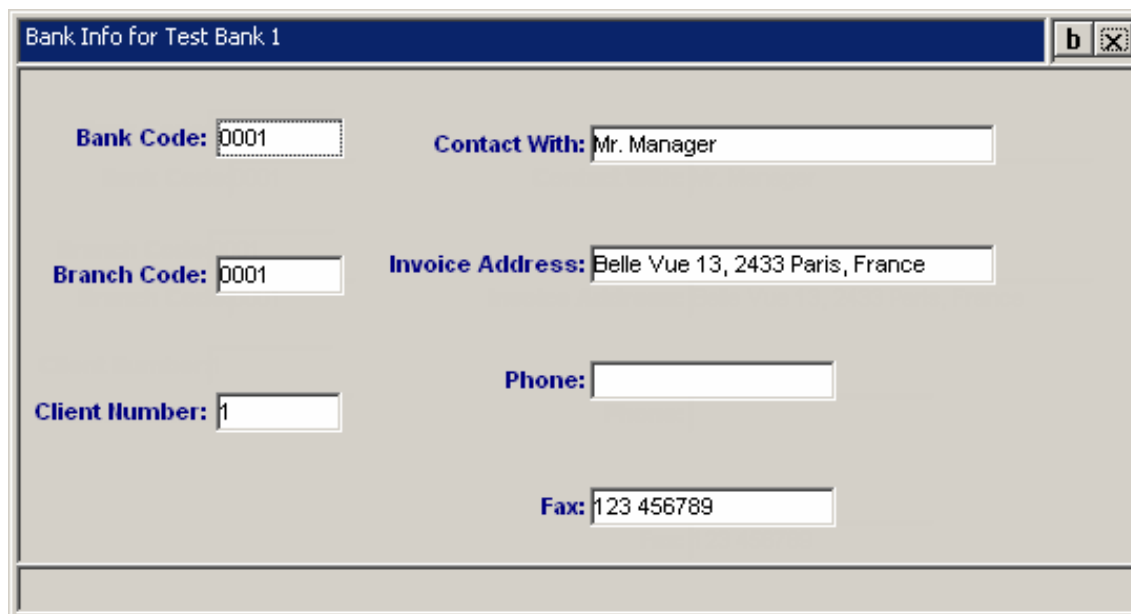
Name	Bank Code	Branch Code	Phone	Contact With	Production Details
Test Bank 1	0001	0001		Mr. Manager	
Test Bank 2	0002	0002		Mr. Manager	

Рис. 3. Форма для настройки параметров финансового института для производства банковских карт

Данная форма содержит следующие поля:

- *Name* – наименование банка, для которого осуществляется выпуск банковских карт;
- *Bank Code* – код банка; внутренний параметр системы, используемый при формировании заданий на выпуск банковских карт; этот идентификатор может быть использован при формировании выгружаемых данных, необходимых для производства карт; значение в данном поле должно совпадать со значением поля *Bank Code* формы "Financial Institutions" (Full → Configuration Setup → Main Tables → Financial Institutions);
- *Branch Code* – код подразделения банка (внутренний параметр системы); этот идентификатор используется модулем "PIN Management" для настройки параметров производства банковских карт, значение в данном поле должно совпадать со значением поля *Branch Code* формы "Financial Institutions" (Full → Configuration Setup → Main Tables → Financial Institutions);
- *Phone* – номер телефона для связи с клиентом-заказчиком производства карт;
- *Contact With* – контактное лицо;
- *Production Details* – дополнительная информация.

Дополнительная информация о банке-заказчике может быть указана в подчиненной форме, вызываемой с помощью нажатия на кнопку [Bank Info] (см. Рис. 4).



Bank Info for Test Bank 1

Bank Code: 0001 Contact With: Mr. Manager

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

Client Number: 1 Phone:

Fax: 123 456789

Рис. 4. Форма для указания дополнительной информации о банке-клиенте.

Ряд параметров производства банковских карт задается с помощью подчиненных форм, вызываемых из формы "Bank Production Parameters". Кнопки [CA Keys] и [Certificates] вызывают на экран подчиненные формы для задания параметров производства смарт-карт (см. документ "Настройка параметров системы WAY4™ для выпуска смарт-карт").

Кнопка [MC OBKM] предназначена для регистрации транспортных ключей при использовании сервиса MasterCard On-behalf Key Management (OBKM). Подробнее см. в документе "Выгрузка криптографических ключей в платежную систему MasterCard".

## 2.2 Параметры контроля подлинности

Для задания параметров контроля подлинности банковской карты используется форма "Validation for <наименование финансового института>" (см. Рис. 5), вызываемая на экран с помощью нажатия на кнопку [Validation] в форме "Bank Production Parameters" (см. рисунок Рис. 3 в разделе "[Параметры производства карт для финансового института](#)").

Validation for Test Bank 1									
Name	PAN MIN	PAN MAX	PIN Valid Scheme	PVK Offs Trk2	PVK Offs Trk1	PVV Offs Trk2	PVV Offs Trk1	CVV Check Mode	
PIN Mailer	0000000000000000	0000009999999999	HSM by DB	0	0	0	0	0 No CVV check	
USmart	3500000000000000	3500009999999999	VISA PVV	8	8	9	9	9 HSM both	
AMEX EMV Chip	3700000000000000	3700009999999999	HSM by DB	0	0	0	0	0 AMEX CSC	
VISA+Electron	4015500000000000	4015519999999999	VISA PVV	8	8	9	9	9 HSM both	
VSDC SDA	4025240000000000	4025249999999999	VISA PVV	8	8	9	9	9 HSM both	
CPA DDA	4025250000000000	4025259999999999	VISA PVV	8	8	9	9	9 HSM both	
VSDC DDA	4025250000000000	4025259999999999	VISA PVV	8	8	9	9	9 HSM both	
MC	5413330100000000	5413330199999999	MC PVV	8	8	9	9	9 HSM both	
MC MChip4 MPAD SDA	5413331000000000	5413331099999999	MC PVV	8	8	9	9	9 MC CVV	
Local	6000000000000000	6000009999999999	VISA PVV	8	8	9	9	9 HSM both	
Cirrus	6799990100000000	6799990199999999	IBM 3624	8	8	14	14	14 HSM both	
MChip2.1 Lite Profiled	6799991000000000	6799991999999999	MC PVV	8	8	9	9	9 MC CVV	
MChip2.1 Lite	6799991000000000	6799991999999999	MC PVV	8	8	9	9	9 MC CVV	
Seccos	7777777777777777	7777777777777777	MC PVV	8	8	9	9	9 MC CVV	

Ins Del Query Check Messages Options

Рис. 5. Форма для задания параметров контроля подлинности банковской карты

Данная форма содержит следующие поля:

- **Name** – наименование для обозначения типа выпускаемой карты;
- **PAN MIN, PAN MAX** – диапазон возможных значений номеров банковских карт;
- **PIN Valid Scheme** – поле с выбором из списка, предназначенное для задания способа контроля подлинности PIN-кода:
- **"IBM 3624"** – проверка осуществляется в соответствии со стандартом IBM3624 offset (функциональность оставлена для совместимости с предыдущими версиями, имеет ограниченную поддержку и не рекомендуется к использованию).
- **"HSM by DB"** – валидация PIN-кода осуществляется на основе величины HSM PIN OFFSET, сохраненной в базе данных (БД).
- **"VISA PVV"** – валидация PIN-кода по значению величины PVV, полученному в онлайн-сообщении от карты.
- **"VISA PVV by DB"** – валидация PIN-кода по значению величины PVV, сохраненной в БД.

Если значение PVV не хранится в БД, используется значение PVV, хранящееся на магнитной полосе карты (Track 2).

- **"DEP PVV"** – проверка осуществляется в соответствии со стандартом DEP.
- **"ESM PVV"** – оставлено для совместимости с предыдущими версиями.
- **"MC PVV"** – валидация PIN-кода по значению величины PVV, полученному в онлайн-сообщении от карты. Отличается от метода "VISA PVV" набором используемых ключей.
- **"MC PVV by DB"** – валидация PIN-кода по значению величины PVV, сохраненной в БД. Отличается от метода "VISA PVV by DB" набором используемых ключей.

Если значение PVV не хранится в БД, используется значение PVV, хранящееся на магнитной полосе карты (Track 2).

- **"VISA PVV PVKI by DB"** – оставлено для совместимости с предыдущими версиями.
- **"Adaptive HSM or PVV by DB"** – оставлено для совместимости с предыдущими версиями.
- **PVK Offs Trk2** – позиция PVKI (PIN Verification Key Index) на второй дорожке магнитной полосы;
- **PVK Offs Trk1** – позиция PVKI на первой дорожке магнитной полосы;
- **PVV Offs Trk2** – позиция PVV (PIN Verification Value) на второй дорожке магнитной полосы;

- *PVV Offs Trk1* – позиция PVV на первой дорожке магнитной полосы;
- *CVV Check Mode* – поле с выбором из списка для указания способа проверки криптографических величин, используемых для верификации банковской карты (CVV, Card Verification Value в платежной системе VISA; CVC, Card Verification Code в платежной системе MasterCard; CSC, Card Security Code в платежной системе AMEX);
- "HSM both" – проверка CVV1 и CVV2 на HSM, при этом окончание срока действия карты для проверки CVV1 представляется в формате "YYMM", а для проверки CVV2 – в формате "MMYY";
- "HSM CVV1 only" – проверка на HSM только CVV1 с представлением окончания срока действия карты в формате "YYMM";
- "By DB both" – проверка CVV1 и CVV2 по значениям, хранящимся в БД;
- "HSM both, YYMM" – проверка CVV1 и CVV2 на HSM, при этом окончание срока действия карты представляется в формате "YYMM";
- "No CVV check" – проверка не производится;
- "HSM Both, no DB CVV2" – проверка CVV1 и CVV2 на HSM, при этом окончание срока действия карты для проверки CVV1 представляется в формате "YYMM", а для проверки CVV2 – в формате "MMYY"; при выполнении проверки по данной схеме учитывается, что значение CVV2 отсутствует в БД;
- "HSM both, YYMM, no DB CVV2" – проверка CVV1 и CVV2 на HSM, при этом окончание срока действия карты представляется в формате "YYMM"; при выполнении проверки по данной схеме учитывается, что значение CVV2 отсутствует в БД;
- "MC CVV" – проверка CVV по схеме MasterCard;
- "AMEX CSC" – проверка CSC по схеме AMEX.



При выборе значения в поле *CVV Check Mode* следует помнить, что стандартами безопасности запрещается:

- хранение CVV в БД.
- отсутствие проверки CVV.



Ответственность за использование таких значений как "HSM CVV1 only", "By DB both", "No CVV check" при формировании параметров контроля подлинности карт целиком лежит на пользователе.

- *CVV Offs Trk2* – позиция CVV1 на второй дорожке магнитной полосы;
- *CVV Offs Trk1* – позиция CVV1 на первой дорожке магнитной полосы;
- *Encr PIN Format* – поле, зарезервированное для будущего использования;
- *EMV Crypto Scheme*, *EMV MAC Scheme*, *EMV Encr Scheme* – поля, заполняемые для производства смарт-карт в соответствии с рекомендациями, изложенными в документе "Настройка параметров системы WAY4 для производства смарт-карт".

Формирование дополнительных параметров контроля подлинности осуществляется в форме "Options for <наименование параметра>" (см. Рис. 6), вызываемой с помощью кнопки [Options] в форме "Validation for <название финансового института>" (см. Рис. 5).

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

Рис. 6. Дополнительные параметры контроля подлинности карт



При формировании параметров контроля подлинности карт следует помнить, что стандартами безопасности запрещается:

- хранение CVV в БД.
- отсутствие проверки CVV.



Ответственность за использование параметров контроля подлинности карт, нарушающих стандарты безопасности, целиком лежит на пользователе. Например, тег "ICVV Skip = Y" позволяет не выполнять проверку CVV для заданного пула номеров карт.

Параметр "Trust to Prevalid. Rslt Sec.Val." позволяет задать список security-величин, не требующих проверки на стороне WAY4, если предварительная проверка данных величин была выполнена сторонней системой, например, МПС. В параметре указывается список кодов значений безопасности, разделенных запятыми: CVC1,CVC2,CAVV,PIN,CRYPT или константа ALL. Если предварительная проверка данных величин сторонней системой не выполнялась, их проверка будет выполнена на стороне WAY4. Если предварительная проверка данных величин сторонней системой была неуспешной, на стороне WAY4 такие транзакции будут отклонены.

## 2.3 Параметры производства карт



Для корректного определения ключей и других параметров производства рекомендуется задавать параметры производства для всего диапазона номеров карт (BIN Range), выданного банку или процессинговому центру платежной системой.



Для задания параметров производства банковских карт используется форма "Parameters for <наименование финансового института>" (см. Рис. 6), вызываемая на экран с помощью нажатия на кнопку [Parameters] в форме "Bank Production Parameters" (см. рисунок Рис. 3 в разделе "Параметры производства карт для финансового института").

Parameters for Test Bank 1										<< >>		9 of 14	b   x
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		7171717171717171	7171717171717171	4	2222	SECCOS	MC	1	Ready	00/00/0000	1		
VISA+Electron		4015500000000000	4015509999999999	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		

Рис. 6. Форма для задания параметров производства банковских карт

Данная форма содержит следующие поля:

- *Name* – наименование для обозначения типа выпускаемой карты;
- *Code* – идентификатор набора параметров производства карты; данное поле соответствует полю *PM Code* суб-типа контракта (см. раздел "Форма суб-типов карточных контрактов" документа "Продукты и суб-типы контрактов") и дает возможность изменять набор параметров производства карт в пределах одного диапазона PAN (см. "Изменение набора параметров производства карт в пределах одного диапазона PAN");
- *PAN MIN* – минимальное значение номера карты;
- *PAN MAX* – максимальное значение номера карты;
- *PIN Len* – длина PIN-кода;
- *ICA* – ICA-код выпускаемой карты;
- *Card Type* – тип выпускаемой карты:
  - "Magnetic Card" – карта только с магнитной полосой;
  - "VSDC" – смарт-карта платежной системы VISA;
  - "MCHIP" – смарт-карта платежной системы MasterCard;
  - "JSmart" – смарт-карта платежной системы JCB;
  - "AMEX EMV" – смарт-карта платежной системы AMEX;
  - "CPA" – смарт-карта типа CAP (Common Payment Application);
  - "SECCOS" – смарт-карта типа SECCOS (Security Chip Card Operating System);
  - "UICS" – смарт-карта платежной системы UnionPay International (UPI).
- *Encoding Method* – поле, определяющее набор параметров, которые будут рассчитываться и использоваться при кодировании величин, записываемых на магнитную полосу и печатаемых на пластиковой карте либо записываемых в память смарт-карты; заполнение данного поля производится с помощью выбора из списка значений, соответствующих стандартам кодирования:



- "Local" – стандарт IBM3624 offset (функциональность оставлена для совместимости с предыдущими версиями, имеет ограниченную поддержку и не рекомендуется к использованию). При этом окончание срока действия карты для расчета CVV1 представляется в формате "YYMM", а для расчета CVV2 – в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "VISA" – стандарт VISA PVV; при этом окончание срока действия карты для расчета CVV1 представляется в формате "YYMM", а для расчета CVV2 – в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "VISA with iCVV" – стандарт VISA iCVV; при этом окончание срока действия карты для расчета CVV1 представляется в формате "YYMM", а для расчета CVV2 – в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "MC" – стандарт MasterCard PVV; при этом окончание срока действия карты для расчета CVC1 и CVC2 представляется в формате "YYMM". Формат даты для расчета CVC2 может быть переопределен с помощью дополнительного параметра производства "MasterCard CVC2 MMYY".
- "MC PayPass" – стандарт MasterCard PayPass (бесконтактные смарт-карты); при этом окончание срока действия карты для расчета CVC1 и CVC2 представляется в формате "YYMM". Формат даты для расчета CVC2 может быть переопределен с помощью дополнительного параметра производства "MasterCard CVC2 MMYY".
- "DEP VISA" – стандарт DEP для VISA; при этом окончание срока действия карты для расчета CVV1 представляется в формате "YYMM", а для расчета CVV2 – в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "DEP MC" – стандарт DEP для MasterCard; при этом окончание срока действия карты для расчета CVC1 и CVC2 представляется в формате "YYMM". Формат даты для расчета CVC2 может быть переопределен с помощью дополнительного параметра производства "MasterCard CVC2 MMYY".
- "AMEX" – стандарт AMEX; при этом окончание срока действия карты для расчета CSC представляется в формате "YYMM".
- "VISA Virtual" – стандарт VISA Virtual (карта для использования в сети интернет; данная карта содержит только номер карты, дату окончания срока действия и CVV2); при этом окончание срока действия карты для расчета CVV2 представляется в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "MC Virtual" – стандарт MasterCard Virtual (карта для использования в сети интернет; данная карта содержит только номер карты, дату окончания срока действия и CVC2); при этом окончание срока действия карты для расчета CVC2 представляется в формате

"YYMM". Формат даты для расчета CVC2 может быть переопределен с помощью дополнительного параметра производства "MasterCard CVC2 MMY".

- "UPI (CUP)" – стандарт для UnionPay International; при этом окончание срока действия карты для расчета CVV1 представляется в формате "YYMM", а для расчета CVV2 – в формате "MMYY". Формат даты для расчета CVV2 может быть переопределен с помощью дополнительного параметра производства "VISA indent CVV YYMM".
- "Custom Loyalty" – набор параметров для приложений программы поддержки постоянных клиентов (loyalty programme);
- "Password List" – набор параметров для выпуска карты, содержащей список одноразовых паролей;
- "PIN Mailer" – стандарт для печати PIN-конверта.



Для значений "Local", "VISA", "VISA with iCVV", "DEP VISA", "VISA Virtual" и "UPI (CUP)" существует возможность переопределить формат даты для расчета величины CVV2; для этого необходимо в данной форме нажать на кнопку [Options] и в открывшуюся форму добавить параметр "VISA indent CVV YYMM". При указании параметру значения "Y" дата будет представлена в формате "YYMM", в противном случае (значение "N", значение по умолчанию) – в формате "MMYY". Аналогично для значений "MC", "MC PayPass", "DEP MC" и "MC Virtual" можно определить параметр "MasterCard CVC2 MMY". При указании значения "Y" дата определяется в формате "MMYY", при указании "N" (значение по умолчанию) – в формате "YYMM".

- PVKI – поле для ввода значения, необходимого при использовании стандартов кодирования VISA PVV и MasterCard PVV;

При нажатии на кнопку [Manage] на экране будет представлено контекстное меню, содержащее следующие пункты:

- "Check" – вызов процедуры проверки корректности введенных данных. В случае если данные введены корректно, на экране будет представлено окно с сообщением "Parameters Validated", а в поле *Is Ready* будет указано значение "Ready".
- "MC OBKM" – выгрузка ключей в платежную систему MasterCard (см. документ "Выгрузка криптографических ключей в платежную систему MasterCard");
- "Apply Profile" – загрузка шаблона параметров карточного приложения для смарт-карты (см. раздел "Параметры карточного приложения" документа "Настройка параметров системы WAY4 для производства смарт-карт").
- "Translate Keys" – передача ключей (трансляция ключей) между аппаратными модулями безопасности различных типов (см. ["Трансляция ключей между двумя аппаратными модулями безопасности"](#)).
- "Duplicate Iss Keys" – копирование параметров RSA-ключа эмитента и сертификата к данному ключу.



Операция "Duplicate Iss Keys" возможна только для параметров производства с одинаковым значением диапазона номеров карт (BIN Range), так как BIN Range является составной частью сертификата и используется в процессе аутентификации карты на POS-терминале. Копирование RSA-ключа и его сертификата для нового набора параметров производства с разными значениями BIN приведет к выпуску неработоспособного пластика. После выполнения процедуры копирования настоятельно рекомендуется провести тестирование пластика в части работы Offline Data Authentication на реальном POS-терминале.

Кнопки [PIN Mailer] и [PIN2 Mailer] предназначены для задания параметров печати PIN-конверта и конверта, содержащего величину PIN2 (см. разделы "[PIN-конверт](#)" и "[Печать величины PIN2](#)" соответственно).

Кнопка [EMV] предназначена для вызова подчиненной формы, используемой для ввода параметров основного карточного приложения смарт-карт.

Кнопка [IBM3624] предназначена для вызова подчиненной формы, с помощью которой задаются параметры для стандарта кодирования IBM3624 offset (функциональность оставлена для совместимости с предыдущими версиями, имеет ограниченную поддержку и не рекомендуется к использованию).

Кнопки [DES Keys] и [3-DES Keys] предназначены для задания параметров ключей шифрования (см. "[Ключи шифрования](#)").

Кнопки [3-DES Keys] и [RSA Keys] предназначены для вызова форм, используемых для ввода параметров криптографических ключей, необходимых для производства смарт-карт (см. раздел "Криптографические ключи" документа "Настройка параметров системы WAY4 для производства смарт-карт").

Кнопка [Add Keys] предназначена для вызова формы, используемых для ввода параметров 3DS HMAC ключей; алгоритм шифрования (*Key Algorithm*) "Generic Secret".

Кнопка [Options] предназначена для вызова формы, используемой для настройки дополнительных параметров производства карт.

Кнопка [Commands] предназначена для настройки параметров управляющих команд эмитента (см. раздел "Настройка параметров управляющих команд эмитента" документа "Настройка параметров системы WAY4 для производства смарт-карт").

## 2.3.1 Ключи шифрования

Для задания параметров DES (Data Encryption Standard) ключей шифрования используется форма "DES Keys for <наименование карточного продукта>", либо форма "3-DES Keys for <наименование карточного продукта>" (см. [Рис. 7](#)), вызываемая из формы "Parameters for <наименование финансового института>" с помощью нажатия на кнопку [DES Keys], либо кнопку [3-DES Keys] соответственно, в форме "Parameters for <наименование финансового института>" (см. раздел "[.Параметры производства карт v03.50](#)").

3-DES Keys for VISA Electron									
Key Algorithm	Key Type	DES Key	DES Key Check	Date From	Date To	MC OBKM Key Extra Data	Storage Form	Is Ready	Ready Till
3DES ABA	PIN Export Key	UDF1D258F4277C34B7129A0F9DEB9DCC4	30EDB4	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	PVK - 3DES	U1769DD53DC65A91EEC58576D0DBF538F	A0C111	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	CVK - 3DES	U5C862FAB20EBF6217050803E85406C4F	76F4CE	00/00/00 00:00	00/00/00 00:00		HSM / Host / Hex	Ready	00/00/0000

Рис. 7. Форма для задания параметров DES-ключей шифрования



Следует иметь в виду, что HSM поддерживает экспорт/импорт ключей шифрования только по стандарту ANSI X9.17.

При производстве карт с магнитной полосой используются следующие криптографические ключи алгоритма 3-DES:

- "PVK" (PIN Verification Key) – данный ключ предназначен для формирования и проверки в режиме онлайн величины PVV (PIN Verification Value);
- "CVK" (Card Verification Key) – данный ключ предназначен для формирования и проверки в режиме онлайн величины CVV (Card Verification Value);
- "CVK2" – данный ключ предназначен для формирования и проверки в режиме онлайн величины CVV2;
- "PEK" (PIN Export Key) – данный ключ предназначен для шифрования PIN-блока при персонализации карты, а также при передаче данных из системы подготовки данных (PIN Management) в подсистему электрической персонализации;
- "ZPK" (Zone PIN Key) – данный ключ предназначен для шифрования PIN-блока при передаче из модуля эмиссии в систему подготовки данных (PIN Management) в случае если используется режим трансляции PIN-блока.

Рекомендуемым способом формирования DES ключей является их формирование с помощью пайпа "DES Key Management" (см. "Формирование ключей"). Во время работы пайпа на аппаратный модуль безопасности будут передаваться соответствующие команды генерации ключей.

### 2.3.1.1 Формирование ключей

Формирование криптографических ключей в системе осуществляется с помощью пайпа "DES Key Management". При формировании ключей данным способом их параметры автоматически загружаются в базу данных, и дополнительных действий по настройке их параметров не требуется.

Перед началом формирования ключа в форме "3-DES Keys for <наименование типа выпускаемой карты>" (см. рисунок Рис. 7 в разделе "Ключи шифрования") необходимо выбрать из списка тип ключа (поле *Key Type*), а в поле *Storage Form* выбрать один из следующих способов хранения ключа:

- "HSM / Host / Hex" – для ключа, формируемого на устройстве производства компании Thales;

- "HSM / Host / Keyblock Hex" – для устройств производства компании Thales, поддерживающих формат хранения "Keyblock". Данный формат позволяет хранить ключ и все его атрибуты единым блоком.
- "OWSeM / Host / Hex" – для ключа, формируемого на устройстве производства компании SafeNet.
- "OWSeM / Host / Keyblock Hex" – для ключа, формируемого на устройствах производства компании SafeNet, поддерживающих формат хранения "Keyblock Hex".
- "GL / Host / HEX" – для ключа, формируемого на устройстве SafeNet Payment HSM производства Gemalto.
- "GL / Host / Keyblock Hex" – для ключа, формируемого на устройстве SafeNet Payment HSM, поддерживающего формат хранения "Keyblock Hex".
- "GL / Host / Keyblock Base64" – для ключа, формируемого на устройстве SafeNet Payment HSM, поддерживающего формат хранения "Keyblock Base64".



Категорически запрещается использование одного и того же ключа для нескольких типов карт.

Для запуска процедуры формирования ключей следует в форме "3-DES Keys for <наименование типа выпускаемой карты>" (см. рисунок [Рис. 7](#) в разделе "[Ключи шифрования](#)") нажать на кнопку [Manage].

### 2.3.1.1.1 Кнопка [Manage]

В результате на экране будет представлено контекстное меню, содержащее следующие пункты:

- "Manage" – при выборе данного пункта на экране будет представлена форма "PM DES Management Mode" (см. [Рис. 8](#)).

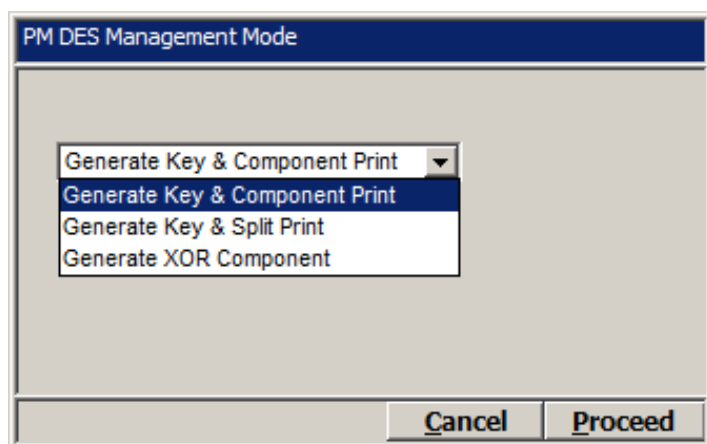


Рис. 8. Форма для выбора режима формирования криптографических ключей

В данной форме может быть выбран один из следующих режимов генерации ключей:

- "Generate Key & Component Print" – формирование ключа и печать компонент (см. "[Опция "Generate Key & Component Print"](#)").
- "Generate Key & Split Print" – формирование ключа и раздельная печать компонент.



Не рекомендуется использовать данный режим генерации ключей; режим присутствует в системе для обеспечения совместимости с предыдущими версиями.

- "Generate XOR Component" – формирование компонент той же длины, что и данный ключ (см. [Опция "Generate XOR Component"](#)).
- "Verify KCV" – проверка контрольной суммы ключа (Key Check Value, KCV); см. [Опция "Verify KCV"](#).
- "Generate Key (No Printing)" – формирование ключа без печати компонент (см. [Опция "Generate Key \(No Printing\)"](#)).

### 2.3.1.1.2 Опция "Generate Key & Component Print"

Режим "Generate Key & Component Print" предназначен для формирования компонент той же длины, что и данный ключ. Компоненты ключа будут сформированы внутри HSM в открытой форме и напечатаны на принтере, подключенном к HSM, после чего ключ заданной длины может быть собран из данных компонент посредством выполнения операции "исключающее ИЛИ" между ними. Для этого HSM собирает открытый ключ из зашифрованных компонент и шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных. Количество формируемых компонент задается с помощью параметра пайпа "KEY\_COMPONENTS" (см. [Параметры пайпа "DES Key Management"](#)) или с помощью дополнительного параметра типа ключа "Num of XOR Components" (см. [Шаблоны для печати ключей](#)).

Печать компонент ключа в PIN-конвертах будет осуществляться в соответствии с настроенными шаблонами (см. [Шаблоны для печати ключей](#)). Ключ в данном режиме печатается покомпонентно: сначала первая компонента ключа, затем вторая компонента ключа и т. д. Все конверты с компонентами ключа должны храниться у сотрудников службы информационной безопасности и быть безопасно уничтожены непосредственно после окончания срока действия ключа.

### 2.3.1.1.3 Опция "Generate Key (No Printing)"

Режим "Generate Key & Component Print" предназначен для формирования ключа без печати его на принтере, подключенном к HSM. Для этого HSM генерирует случайный ключ определенного типа, после чего шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных.

### 2.3.1.1.4 Опция "Generate XOR Component"

Режим "Generate XOR Component" предназначен для формирования компонент той же длины, что и данный ключ. Компоненты ключа будут сформированы в открытой форме и напечатаны на принтере, подключенном к HSM, после чего ключ заданной длины может быть собран из данных компонент посредством выполнения операции "исключающее ИЛИ" между ними. Для этого HSM собирает открытый ключ из зашифрованных компонент и шифрует его под соответствующей LMK-парой. Затем зашифрованный ключ сохраняется в базе данных. Количество формируемых

компонент задается с помощью параметра пайпа "KEY\_COMPONENTS" (см. "[Параметры пайпа "DES Key Management"](#)") или с помощью дополнительного параметра типа ключа "Num of XOR Components" (см. "[Шаблоны для печати ключей](#)"). Сформированный ключ, а также контрольная сумма ключа (KCV) будут занесены соответственно в поля *DES Key* и *DES Key Check* формы "3-DES Keys for <наименование типа выпускаемой карты>" (см. рисунок [Рис. 7](#) раздела "[Ключи шифрования](#)") после того, как будет сформирована последняя компонента ключа.



Следует иметь в виду, что при каждом вызове процедуры происходит формирование только одной компоненты ключа. Сборка компонент ключа будет осуществляться после формирования и печати последней компоненты ключа, количество которых определено с помощью параметра "KEY\_COMPONENTS" или с помощью дополнительного параметра типа ключа "Num of XOR Components".

Печать компонент осуществляется в соответствии с настроенными шаблонами (см. "[Шаблоны для печати ключей](#)"). Ключ в данном режиме печатается покомпонентно: сначала первая компонента ключа, затем вторая компонента ключа и т. д. Все конверты с компонентами ключа должны храниться у сотрудников службы информационной безопасности и быть безопасно уничтожены непосредственно после окончания срока действия ключа.

### 2.3.1.1.5 Опция "Verify KCV"

Режим "Verify KCV" предназначен для проверки контрольной суммы сформированного ключа (Key Check Value, KCV). Алгоритм проверки значения KCV задается с помощью параметра "KCV\_ALG" (см. "[Параметры пайпа "DES Key Management"](#)").

В случае если значение KCV, содержащееся в поле *DES Key Check* формы "3-DES Keys for <наименование типа выпускаемой карты>" (см. рисунок [Рис. 7](#) раздела "[Ключи шифрования](#)"), отличается от рассчитанного с помощью HSM, на экране будет представлено окно с сообщением об ошибке.

### 2.3.1.1.6 Параметры пайпа "DES Key Management"

Для пайпа "DES Key Management" можно указать следующие параметры:

- "COMM\_PARAMS" – предназначен для указания параметров сетевого соединения с аппаратным модулем безопасности по протоколу TCP/IP;
- "PRN\_TEMPL\_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта компоненты ключа;
- "LAST\_PRN\_TEMPL\_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта последней компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component");
- "KCV\_TEMPL\_FILE" – предназначен для указания пути, по которому хранится файл с шаблоном для печати PIN-конверта контрольной суммы ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component" после того, как будет

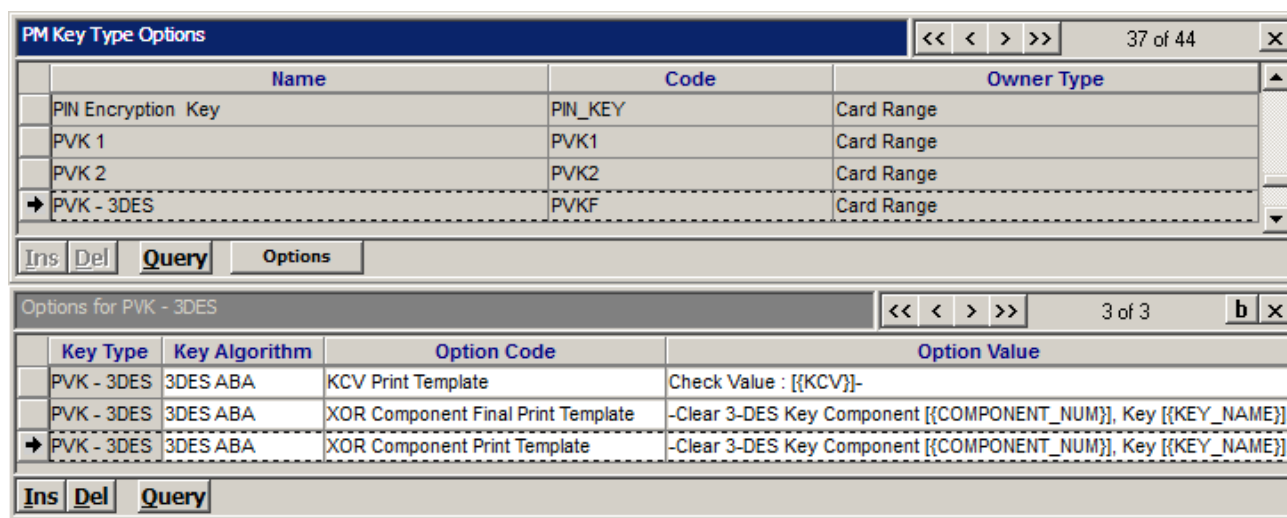


- сформирована последняя компонента). Если параметр принимает значение "NONE", то контрольная сумма ключа не печатается;
- "KEY\_COMPONENTS" – с помощью данного параметра указывается количество компонент ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component"). Возможные значения – "2" или "3" (значение по умолчанию – "3");
  - "KCV\_ALG" – предназначен для указания алгоритма проверки контрольной суммы сформированного ключа (KCV). При установлении параметру значения "S" будет использован алгоритм проверки значения KCV для карт SECCOS. В случае если параметр не задан, либо задано любое значение, отличное от "S", будет использован стандартный алгоритм проверки величины KCV;
  - SRC\_CODEPAGE - в параметре указывается кодировка, которая используется в файле шаблона для печати PIN-конверта. По умолчанию используется US-ASCII (Codepage 437);
  - DST\_CODEPAGE - в параметре указывается кодировка, в которой сформированный текст будет отправлен на принтер, подключенный к HSM..

### 2.3.1.2 Шаблоны для печати ключей

Для печати компонент ключей на PIN-конвертах необходимо настроить соответствующие шаблоны. Настройка шаблонов для печати ключей осуществляется одним из следующих способов:

- В форме "PM Key Type Options" (Full → Configuration Setup → Card Production Setup → PM Key Type Options) следует выбрать тип ключа, нажать на кнопку [Options] и в открывшейся форме "Options for <...>" (см. [Рис. 9](#)) определить шаблоны для печати.



The image shows two screenshots of a software interface. The top screenshot is titled "PM Key Type Options" and displays a table with columns: Name, Code, and Owner Type. The bottom screenshot is titled "Options for PVK - 3DES" and displays a table with columns: Key Type, Key Algorithm, Option Code, and Option Value.

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

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

Рис. 9. Задание шаблонов для печати ключей

В данной форме необходимо выбрать алгоритм шифрования ключа данного типа (поле *Key Algorithm*), дополнительный параметр типа ключа (поле *Option Code*), а также значение дополнительного параметра (поле *Option Value*). При этом для шаблонов печати ключей используются следующие дополнительные параметры:



- "Num of XOR Components" – количество компонент ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component"). Возможные значения – "2" или "3".
- "XOR Component Print Template" – шаблон для печати PIN-конверта компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component").
- "XOR Component Final Print Template" – шаблон для печати PIN-конверта последней компоненты ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component").
- "KCV Print Template" – шаблон для печати PIN-конверта контрольной суммы ключа (используется только для режимов "Generate Key & Component Print" и "Generate XOR Component" после того, как будет сформирована последняя компонента).
- Шаблон для печати необходимо сохранить в файле с расширением "\*.txt".

Переменные шаблонов для печати ключей и примеры шаблонов представлены в разделе ["Переменные шаблонов для печати ключей"](#).

В процессе формирования ключей поиск шаблона для печати осуществляется следующим образом:

- Сначала осуществляется поиск шаблона, настроенного в форме "Options for <...>" (см. [Рис. 9](#)).
- Если в форме "Options for <...>" не задан шаблон печати ключей, проверяется наличие параметров "PRN\_TEMPL\_FILE", "LAST\_PRN\_TEMPL\_FILE", "KCV\_TEMPL\_FILE" и "KEY\_COMPONENTS" пайпа "DES Key Management".
- Если в форме "Options for <...>" не задан шаблон и не заданы параметры пайпа, на экране будет представлено окно "Choose print template file", в котором следует выбрать созданный вручную файл шаблона для печати ключей.

### 2.3.1.2.1 Переменные шаблонов для печати ключей

В шаблонах для печати ключей используются следующие переменные:

- "COMPONENT\_NUM" – количество печатаемых компонент ключа;
- "KEY\_NAME" – наименование ключа;
- "KEY\_SERIAL" – серийный номер ключа (по умолчанию не используется для ключей устройств); поле может использоваться для хранения дополнительной идентификационной информации о ключе;
- "KEY\_TYPE" – тип ключа;
- "KCV" – контрольная сумма ключа;
- "KEY\_OWNER\_TYPE" – тип владельца ключа;
- "KEY\_OWNER\_ID" – идентификационный номер владельца ключа.

Кроме того, в шаблонах могут использоваться стандартные поля HSM (см. документацию HSM).

Пример шаблона:

```
-  
  
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}]  
  
-
```

### 2.3.1.2.2 Печать контрольной суммы ключа (KCV) на PIN-конверте с последней компонентой

Для печати контрольной суммы ключа (KCV) на PIN-конверте с последней компонентой ключа следует отредактировать соответствующие шаблоны. При этом необходимо, чтобы содержимое двух шаблонов могло быть напечатано на одном PIN-конверте.

Для этого в шаблоне для печати PIN-конверта последней компоненты ключа нужно оставить все переменные до "KCV" (не включая переменную "KCV"), а в шаблон для печати контрольной суммы ключа поместить переменную "KCV" и финальные отступы.

Таким образом, шаблон для печати последней компоненты ключа не должен содержать в конце указания перевода формы (FORM FEED) или группы переводов строк:

```
-  
  
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}]
```

Шаблон для печати контрольной суммы ключа будет иметь следующий вид:

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

Таким образом, после выполненных изменений в шаблонах контрольная сумма ключа (KCV) будет напечатана на PIN-конверте вместе с последней компонентой ключа.

## 2.3.2 Настройка параметров ключей для аппаратных модулей безопасности различной конфигурации

Для обеспечения работы системы подготовки данных и системы обработки транзакций в режиме онлайн могут использоваться два независимых аппаратных модуля безопасности (HSM).

В случае если в системе используются устройства компании Thales, рекомендуется использовать одинаковый набор локальных мастер-ключей (LMK) для данных устройств.

В случае если в системе используются устройства разных производителей (например, Thales HSM и SafeNet ProtectServer), для данных устройств всегда используются различные наборы LMK. При этом при конфигурации системы необходимо руководствоваться следующими инструкциями:

- Формирование ключей рекомендуется осуществлять на аппаратном модуле безопасности системы подготовки данных и управления ключами, либо ключи могут быть получены от платежной системы (см. раздел "[Формирование ключей](#)").
- Ключи, необходимые для подтверждения подлинности (validation) транзакционной информации, должны быть импортированы в устройство HSM системы обработки транзакций в режиме онлайн.
- Для каждого ключа, зашифрованного с помощью LMK различных аппаратных модулей безопасности, необходимо вручную зарегистрировать две записи в форме "DES Keys for <...>", либо "3DES Keys for <...>":
  - запись для ключа, зашифрованного с помощью LMK устройства системы подготовки данных и управления ключами (в случае если данная запись не была создана автоматически);
  - запись для ключа, зашифрованного с помощью LMK устройства системы обработки транзакций в режиме онлайн.



В случае если ключ был импортирован в аппаратный модуль безопасности компании Thales по методу Variant (при импорте ключа для параметра "Key Scheme" было указано значение "U"), в поле *DES Key* формы "DES Keys for <...>" или "3-DES Keys for <...>" для значения ключа в зашифрованном виде необходимо указать префикс "U".

- Для каждой из двух записей в поле *Storage Form* указать соответствующее значение:
  - "HSM / Host / Hex" – для ключа, зашифрованного под Variant LMK устройства производства компании Thales.
  - "HSM / Host / Keyblock Hex" – для ключа, зашифрованного под Keyblock LMK устройства производства компании Thales.
  - OWSeM / Host / Hex" – для ключа, зашифрованного под LMK устройства компании SafeNet.

- "OWSeM / Host / Keyblock Hex" – для ключа, зашифрованного под Keyblock LMK устройства компании SafeNet.
- "GL / Host / HEX" – для ключа, зашифрованного под LMK устройства SafeNet Payment HSM производства Gemalto.
- Для глобального параметра AUTH\_KEY\_STORAGE\_FORM указать значение "HH".
- Для перешифрования PIN-блока из-под ZPK под LMK необходимо глобальному параметру "PM\_PIN\_TRANSLATE" указать значение "Y". Кроме того, в форме "Options for <...>", вызываемой на экран при нажатии на кнопку [Options] в форме "Parameters for <наименование финансового института>" (см. рисунок Рис. 6), необходимо задать параметр "Issuer PIN Format", указав в качестве значения "UNDER\_ZPK".
- Для пайпа обработки заданий на выпуск карт "Produce Cards & PINs" (см. раздел "Обработка заданий" документа "Выпуск карт с магнитной полосой в системе WAY4™") с помощью параметра "STORAGE\_FORM" указать, устройство HSM какого производителя используется в системе подготовки данных и управления ключами:
  - "HH" – устройство производства компании Thales;
  - "WH" – устройство компании SafeNet.
  - "LH" – устройство компании Gemalto.
  - В качестве альтернативного варианта при помощи параметра "SM\_ID" можно указать наименование используемого в системе аппаратного модуля безопасности (значение поля Device Name формы "Security Device" – см. раздел "Настройка параметров соединения рабочей станции с аппаратным модулем безопасности").



Следует иметь в виду, что определение пункта меню "Produce Cards & PINs" состоит из двух подпунктов. Значение параметра "STORAGE\_FORM" ("SM\_ID") должно быть указано для обоих данных подпунктов.

В системе существует возможность осуществлять обработку заданий на выпуск карт одновременно на нескольких аппаратных модулях безопасности. Это может потребоваться в случае выпуска большого количества карт. Для одновременной обработки заданий на нескольких устройствах необходимо руководствоваться следующими инструкциями:

- Необходимо использовать устройства одного типа (например, Thales).
- Для всех устройств использовать одинаковый набор локальных мастер-ключей (LMK).
- Для пайпа одновременной обработки заданий на выпуск карт "Produce Cards & PINs Multithread" указать следующие идентификаторы устройств:
  - для первого подпункта меню с помощью параметра "SM\_ID" через запятую указать идентификаторы тех аппаратных модулей безопасности, с помощью которых будет производиться расчет криптографических величин;
  - для второго подпункта меню указать с помощью параметра "SM\_ID" указать идентификатор аппаратного модуля безопасности, к которому подключен специальный принтер для печати PIN-конвертов.



Следует иметь в виду, что печать PIN-конвертов осуществляется только на одном устройстве.

Для запуска процесса одновременной обработки заданий на выпуск карт необходимо выбрать в меню пользователя пункт "Card Production on HSM pool → Produce Cards & PINs Multithread". При этом одновременная обработка заданий происходит аналогично обработке заданий на выпуск карт с магнитной полосой (см. раздел "Обработка заданий" документа "Выпуск карт с магнитной полосой в системе WAY4™").

### 2.3.3 PIN-конверт

Для задания параметров печати PIN-конверта используется форма "PIN mailer for <наименование карточного продукта>" (см. [Рис. 10](#)), вызываемая из формы "Parameters for <наименование финансового института>" с помощью нажатия на кнопку [PIN Mailer] в форме "Parameters for <наименование финансового института>" (см. раздел "[.Параметры производства карт v03.50](#)").

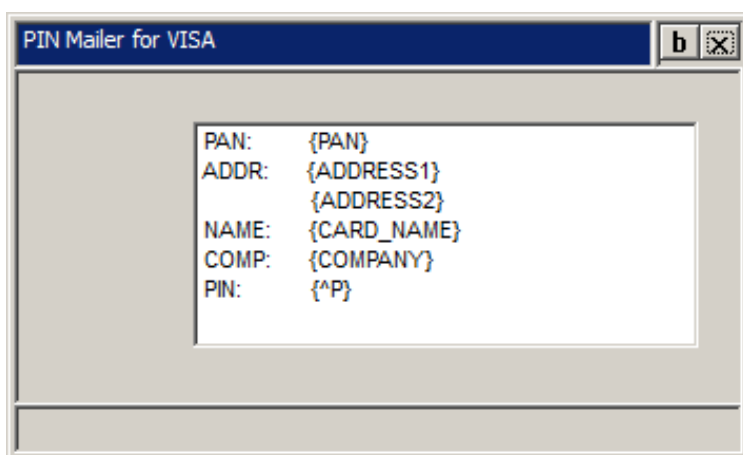


Рис. 10. Форма для задания параметров печати PIN-конверта

В данной форме указываются надписи, печатаемые на PIN-конверте, а в фигурных скобках указываются наименования переменных, значения которых будут подставляться при печати PIN-конверта. Расположение надписей на PIN-конверте будет соответствовать тому, как эти надписи представлены в данной форме.

В случае использования режима параллельной печати двух PIN-конвертов за один проход принтера форма "PIN mailer for <наименование карточного продукта>" должна содержать данные для обоих PIN-конвертов (см. [Рис. 11](#)).

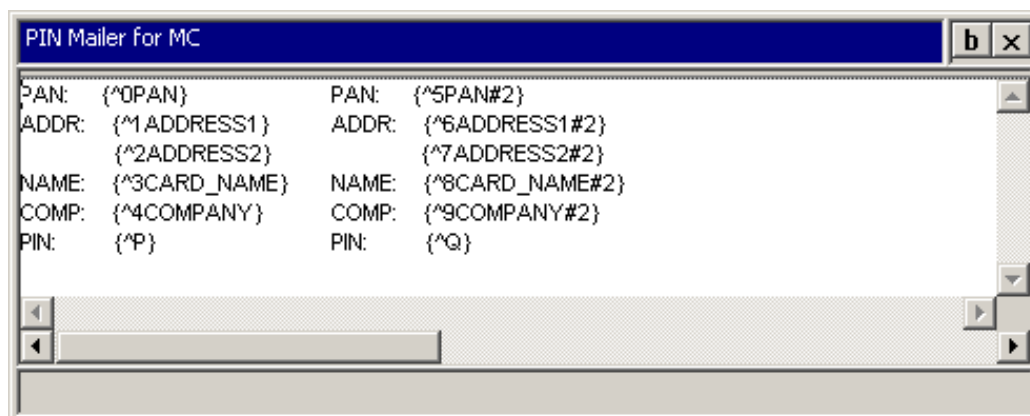


Рис. 11. Параметры печати при параллельной печати двух PIN-конвертов

В этом случае переменные, значения которых будут подставляться при печати PIN-конвертов, последовательно нумеруются (^0, ^1 и т. д.), а переменные второго PIN-конверта снабжаются постфиксом "#2".

При задании формата PIN-конверта допускается использование следующих переменных:

- "ICA\_NUM" – ICA код выпускаемой карты;
- "SHORT\_PAN" – сокращенный номер карты (последние четыре цифры полного номера);
- "EXP\_DATE" – дата окончания срока действия карты;
- "SERVICE\_CODE" – сервис-код банковской карты согласно требованиям платежной системы;
- "CARD\_NAME" – имя держателя банковской карты, эмбоссируемое на пластиковой карте, например, MR JOHN BROWN; данное значение содержится в поле *Name* формы "Plastics for <...>", вызываемой из формы параметров карточного контракта;
- "COMPANY" – наименование компании, указанное в соответствующем поле записи о клиенте;
- "COUNTRY" – наименование страны, указанное в соответствующем поле записи о клиенте;
- "CITY" – город, указанный в соответствующем поле записи о клиенте;
- "ZIP" – почтовый индекс, указанный в соответствующем поле записи о клиенте;
- "ADDRESS1", "ADDRESS2", "ADDRESS3", "ADDRESS4" – информация об адресе доставки PIN-конверта; в качестве значений переменных будет использована информация об адресе клиента из БД. Значения переменных могут быть переопределены с помощью параметров пайпа ("PINM\_ADDR\_LINE1\_FMT", "PINM\_ADDR\_LINE2\_FMT", "PINM\_ADDR\_LINE3\_FMT", "PINM\_ADDR\_LINE4\_FMT"), выгружающего задания на производство карт в модуль PIN Management и запускаемого с помощью пункта меню "Full → Issuing → Send / Receive Production Batches → PIN Management File Export". При определении данных параметров могут использоваться переменные, список которых представлен в разделе "Список переменных" документа "Настройка сообщений клиентам".
- "BRANCH\_CODE", "BANK\_CODE", "BANK\_NAME" – параметры производства банковских карт из таблицы "Bank Production Parameters" (см. рисунок [Рис. 3](#) в разделе ["Параметры производства карт для финансового института"](#));
- "ADD\_INFO\_01", "ADD\_INFO\_02", "ADD\_INFO\_03", "ADD\_INFO\_04" – дополнительная информация; данная информация представляет собой значения параметров пайпа, выгружающего задания на производство карт модулю PIN Management и запускаемого с помощью пункта меню "Full → Issuing → Send / Receive Production Batches → PIN Management File Export"; следует иметь в виду, что соответствующие параметры пайпа указываются в

следующем формате: ADD\_INFO\_1, ADD\_INFO\_2 и т. д.; данные параметры задаются при редактировании пункта меню (см. раздел "Тип Pipe" документа "Редактор меню");

- "PAN" – номер банковской карты;
- "BIN\_6D" – первые 6 цифр номера карты;
- "CVV2" – значение CVV2 выпускаемой карты;
- "JOB\_NUM" – номер пакета заданий (job), в котором находится данное задание на производство карты (task);
- "SEQ\_NUM" – порядковый номер карты с одинаковым PAN;
- "ADD\_FLD1", "ADD\_FLD2", "ADD\_FLD3", "ADD\_FLD4" – дополнительная информация; данные параметры аналогичны параметрам "ADD\_INFO\_01", "ADD\_INFO\_02", "ADD\_INFO\_03", "ADD\_INFO\_04" и представляют собой значение параметров пайпа, выгружающего задания на производство карт модулю PIN Management;
- "PIN\_S\_FORM" – PIN Selection Form;
- "^P" – значение PIN-кода в числовом формате, например, "1234";
- "^V" – значение PIN-кода в текстовом формате, например, "ONE TWO THREE FOUR";
- "^Q" – значение PIN-кода для второго PIN-конверта в числовом формате, например, "1234", или значение величины PIN2 (см. ["Печать величины PIN2"](#));
- "^W" – значение PIN-кода для второго PIN-конверта в текстовом формате, например, "ONE TWO THREE FOUR";
- "^T" – для устройств Thales HSM – последние 6 цифр номера карты без контрольного разряда (т.е. без последней цифры); для устройств SafeNet ProtectServer – последние 12 цифр номера карты без контрольного разряда.

В форме "PIN mailer for <наименование карточного продукта>" могут быть также указаны управляющие последовательности (Escape-последовательности) для принтера в следующем формате: "<L><hh hh hh...>", где:

- "|" – символ с кодом 0x6a для кодировки ASCII или 0x7c для кодировки EBCDIC;
- "L" – шестнадцатеричное представление длины последующих данных в байтах; допустимый диапазон значений (0 – F);
- hh – шестнадцатеричный код байта.

Например, запись вида "<A><01 02 03 04 05 06 07 08 09 0A>" инициирует посылку на принтер 10 байт с кодами 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A.

## 2.3.4 Печать величины PIN2

Печать криптографической величины PIN2 может осуществляться одним из следующих способов:

- Совместно с PIN-кодом на одном PIN-конверте.
- На отдельном PIN-конверте в рамках отдельного задания на производство для выпущенной ранее карты.

Для печати величины PIN2 совместно с PIN-кодом на одном PIN-конверте необходимо выполнить следующие настройки:

- Для причины производства карты (Production Event), определяемой в справочнике "Production Events" (Full → Configuration Setup → Transaction Types → Production Events), необходимо в поле *Add Prod Params* указать тег "PTPIN2=Y;".



Следует иметь в виду, что для совместной печати величины PIN2 тег "PTPIN2=Y;" необходимо указывать для причин производства карт, которые предполагают печать PIN-конверта, т.е. для которых в поле *Production Type* формы "Production Events" указано значение "Replace All", "Replace PIN" или "Reorder PIN".

- В шаблоне печати PIN-конверта (см. "[PIN-конверт](#)") для печати величины PIN2 следует указать переменную "^Q". Пример шаблона представлен на рисунке [Рис. 12](#).

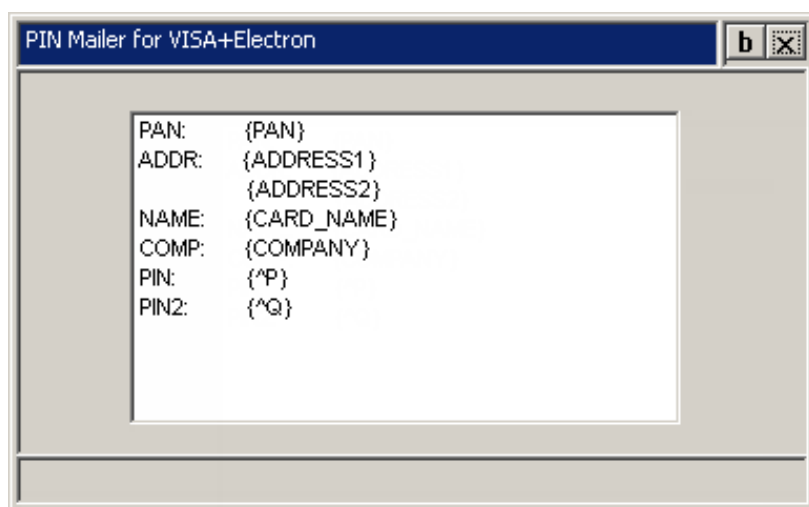


Рис. 12. Пример PIN-конверта для печати величины PIN2



В случае если необходимо выключить режим печати величины PIN2 совместно с PIN-кодом на одном PIN-конверте, следует не только удалить тег "PTPIN2=Y;" из причины производства карты, указанной в форме "Production Events", но и удалить переменную "^Q" из шаблона PIN-конверта. Если удалить только тег "PTPIN2=Y;", но не удалить переменную "^Q", то будет включен режим параллельной печати двух PIN-конвертов за один проход принтера, и в эту переменную будет помещено значение PIN-кода для второго PIN-конверта.

Для печати величины PIN2 на отдельном PIN-конверте в рамках отдельного задания на производство необходимо выполнить следующие настройки:

- В справочнике "Production Events" (Full → Configuration Setup → Transaction Types → Production Events) создать новую причину производства карты (Production Event), указав следующие параметры:
  - в поле *Event* указать значение "Replace Card";
  - в поле *Production Type* указать значение "Replace Add Params";



- в поле *Add Prod Parm*s указать тег "PTPIN2=Y;".
- В форме "Parameters for <наименование финансового института>" (см. рисунок Рис. 6) нажать на кнопку [PIN2 Mailer], после чего определить в шаблоне печати PIN2-конверта переменную "^P". Пример шаблона PIN2-конверта представлен на рисунке Рис. 13.

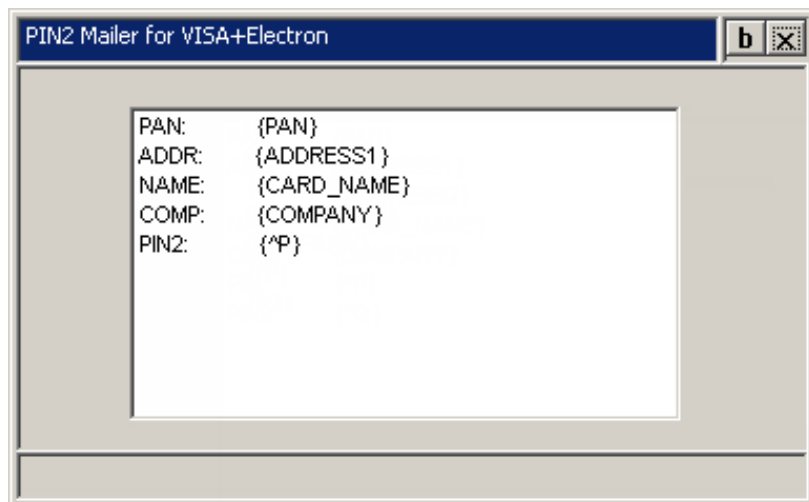


Рис. 13. Пример PIN2-конверта для печати величины PIN2



Для печати PIN2-конверта могут использоваться те же переменные, что и для печати PIN-конверта (см. "[PIN-конверт](#)"), за исключением "^Q".

### 2.3.5 Трансляция ключей между двумя аппаратными модулями безопасности

В системе существует возможность автоматической трансляции 3DES ключей, заданных для определенного диапазона номеров карт, между двумя различными аппаратными модулями безопасности (из-под LMK одного устройства под LMK другого устройства). Трансляция ключей может выполняться, например, в случае использования устройства Thales для обработки транзакций в режиме онлайн и устройства SafeNet для производства карт.

Для этого необходимо в форме "Parameters for <...>" (см. рисунок Рис. 6) нажать на кнопку [Manage], после чего выбрать в контекстном меню пункт "Translate Keys".

Для настройки трансляции ключей необходимо руководствоваться следующими инструкциями (описание параметров пайпа см. в разделе "Параметры пайпа "KM DES Key Management" документа "Загрузка и выгрузка заданий на производство карт в формате XML"):

- Убедиться, что для параметра "MODE" пайпа трансляции ключей "KM DES Key Management" указано значение "TRANSLATE\_CARD\_RANGE\_KEYS".
- Для пайпа трансляции ключей "KM DES Key Management" необходимо определить идентификаторы первого HSM (под LMK которого зашифрованы криптографические ключи) и второго HSM (под LMK которого необходимо перешифровать ключи). Идентификаторы задаются, соответственно, с помощью параметров "SRC\_SM\_ID" и "DEST\_SM\_ID".

- Для пайпа "KM DES Key Management" необходимо с помощью параметров "SRC\_ZMK" и "DEST\_ZMK" определить ключ ZMK (Zone Master Key), зашифрованный, соответственно, под LMK первого и второго устройства HSM.
- Для пайпа "KM DES Key Management" с помощью параметров "SRC\_STORAGE\_FORM" и "DEST\_STORAGE\_FORM" определить способ хранения ключей, соответственно, для первого и второго устройства HSM. Следует иметь в виду, что значения параметров для первого и второго HSM должны быть различными. Для транслированных ключей в поле *Storage Form* формы "3-DES Keys for <...>" (см. рисунок [Рис. 7](#) в разделе "[Ключи шифрования](#)") будет указано значение параметра "DEST\_STORAGE\_FORM".
- Во время трансляции ключей для того же диапазона номеров карт будут созданы записи, соответствующие ключам, зашифрованным под LMK второго устройства (идентификатор которого определен с помощью параметра пайпа "DEST\_SM\_ID"). Поэтому не рекомендуется выполнять трансляцию ключей между двумя устройствами одного типа, т.к. такие ключи (ключ, зашифрованный под LMK первого устройства, и тот же ключ, зашифрованный под LMK второго устройства) будут иметь одинаковое значение поля *Storage Form*.
- Следует иметь в виду, что помимо трансляции ключей двойной длины может быть также выполнена трансляция ключей одинарной длины: для двух ключей одинарной длины "CVK A" и "CVK B" в результате трансляции будет сформирован один ключ двойной длины "CVK", который будет помещен в форму "3-DES Keys for <...>" (см. рисунок [Рис. 7](#) в разделе "[Ключи шифрования](#)"); для двух ключей одинарной длины "PVK 1" и "PVK 2" – ключ двойной длины "PVK". Режим трансляции ключей одинарной длины определяется параметром пайпа "TRANSLATE\_SINGLE\_CVK\_PVK".

## 2.3.6 Изменение набора параметров производства карт в пределах одного диапазона PAN



Настройки, приведенные в данном разделе, следует выполнять сначала на тестовой системе. Только в случае отсутствия ошибок данные настройки могут быть использованы на производственной системе.

Для изменения набора параметров производства карт в пределах одного диапазона PAN (например, при выпуске карт стандарта DDA (Dynamic Data Authentication) вместо карт стандарта SDA (Static Data Authentication) или при миграции на новые параметры контроля подлинности) необходимо выполнить следующие настройки:

- В форме "Parameters for <наименование финансового института>" (см. рисунок [Рис. 6](#)) создать новую запись, в полях *PAN MIN* и *PAN MAX* которой следует указать такие же значения, как и для "старых" параметров производства, а в поле *Code* – уникальное значение идентификатора набора параметров.
- В поле *PM Code* формы "SubTypes for <наименование типа карточных контрактов> (Full → Configuration Setup → Contract Types → Card Contract Types → [SubTypes])" указать идентификатор нового набора параметров производства (значение поля *Code* из

предыдущего пункта) для суб-типа тех карточных контрактов, параметры производства которых необходимо изменить.

После выполнения данных настроек "старые" карты (маркировка и выпуск которых выполнялась до изменения настроек суб-типа) во время авторизации будут использовать старые параметры производства карт, а "новые" и перевыпущенные "старые" карты будут использовать новые параметры производства карт.

## 2.3.7 Автоматическое обнуления счетчика числа попыток ввода неправильного PIN-кода при перевыпуске карты

В системе существует возможность автоматически обнулять счетчик числа попыток ввода неправильного PIN-кода при перевыпуске карты. Обнуление счетчика происходит при загрузке в модуль эмиссии ответа, полученного из модуля PIN Management.

Для автоматического обнуления счетчика необходимо в справочнике "Production Events" (Full → Configuration Setup → Transaction Types → Production Events) для причины производства карты (Production Event) в поле *Add Prod Params* указать тег "CLEAR\_PIN\_ATTEMPTS;". Данный тег следует указывать для причин производства карт, которые предполагают печать PIN-конверта, т.е. для которых в поле *Production Type* формы "Production Events" указано значение "Replace All", "Replace PIN" или "Reorder PIN". Пример настройки представлен на рисунке [Рис. 14](#).

Production Events						8 of 8	X
Contract	Event	Production Type	Name	Code	Add Prod Params		
Card	Replace Card	Replace PIN	Replace PIN - Expired	RPIN			
Card	Replace Card	Replace PIN	Replace PIN - Renew	RPINRE	CLEAR_PIN_ATTEMPTS;		
Card	Replace Card	Replace Plastic	Replace Plastic - Expired	RPL			
Card	Replace Card	Replace Plastic	Replace Plastic - Renew	RPLRE			
Card	Replace Card	Replace All	Replace All - Expired	RALL			
Card	Replace Card	Replace All	Replace All - Renew	RALLRE	CLEAR_PIN_ATTEMPTS;		

Рис. 14. Настройка автоматического обнуления счетчика числа попыток ввода неправильного PIN-кода

## 3 Организация работы с бюро персонализации

Бюро персонализации (персобюро) – программно-аппаратный комплекс, используемый для персонализации выпускаемого пластика. Персонализация карт выполняется на основании параметров, подготовленных в системе WAY4 (см. раздел "[Параметры производства карт](#)") и переданных в персобюро. Клиент может выполнять персонализацию своих карт в нескольких персобюро. Шифрование данных, передаваемых в персобюро, выполняется с помощью транспортных ключей:

- PEK (PIN Export Key) – ключ для шифрования PIN-кода.
- KEK (Key Encryption Key) – ключ для шифрования криптографических величин.



Следует помнить, что KEK используется только для выпуска смарт-карт.

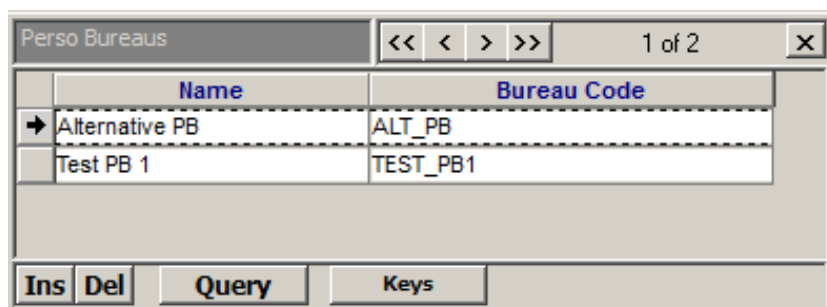
Для каждого персобюро создаются свои транспортные ключи шифрования. Таким образом, имея один набор параметров производства карт (PM Parms), но используя транспортные ключи того или иного персобюро, поддерживается возможность оптимизировать процесс персонализации карт сразу в нескольких персобюро.

Персобюро, используемое по умолчанию для персонализации карт, задается для соответствующего набора параметров (PM Parms) финансового института (см. раздел "[Персобюро, используемое по умолчанию](#)").

Выбор персобюро на этапе вычисления криптографических величин, выгрузке персофайла и т.д. выполняется на основании параметра пайпа PBID. В параметре PBID необходимо указать код персобюро (см. раздел "[Пайпы, на которых задается идентификатор персобюро](#)"). Если параметр PBID не указан на пайпе, используется персобюро, заданное по умолчанию для PM Parms.

### 3.1 Регистрация персобюро

Перечень персобюро формируется в форме "Perso Bureaus", пункт меню Full → Configuration Setup → Card Production Setup → Perso Bureaus (см. [Рис.](#)).



Name	Bureau Code
Alternative PB	ALT_PB
Test PB 1	TEST_PB1

Buttons: Ins, Del, Query, Keys

Рис. Перечень персобюро

Заполнить поля:

- *Name* – наименование персобюро.
- *Bureau Code* – код персобюро.

Перечень персобюро хранится в таблице PM\_KEY\_OWNER (OWNER\_TYPE="PERSO\_BUREAU").

## 3.2 Формирование транспортных ключей

Транспортные ключи создаются стандартно, с помощью аппаратного модуля безопасности (см. раздел "[Ключи шифрования](#)").

Транспортные ключи формируются в форме "Keys for < >" (см. [Рис. 16](#)) стандартным способом (см. раздел "[Формирование ключей](#)"). Форма "Keys for < >" вызывается с помощью кнопки "Keys" из формы "Perso Bureaus".

Keys for Test PB 1						<< < > >>		1 of 2		b x	
	Perso Bureau	Key Algorithm	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					
<div> <div>Ins</div> <div>Del</div> <div>Query</div> <div>Manage</div> <div>Options</div> </div>											

Рис. 16. Транспортного ключа РЕК

## 3.3 Пайпы, на которых задается идентификатор персобюро

Перечень пайпов, на которых задается PBID:

- PM File Response Export – выгрузка файлов ответов из модуля PIN Management.
- PM Personalization File Export – формирование персонализационного файла (персо-файла) для карт.
- PM Security Calc&Mailer Printing – однопоточный расчет криптографических величин и печать PIN-конвертов.
- PM Security Calc (Multithread) – многопоточный расчет криптографических величин.

Подробнее о работе пайпов и их параметрах см документ "Загрузка и выгрузка заданий на производство карт в формате XML".



Пайпы, перечисленные ниже, используется только для выпуска смарт-карт:

- PM RSA ICC Keys Pre Generator – формирование RSA-ключей.
- PM RSA ICC Keys Pre Generator (Multithread) – формирование RSA-ключей в многопоточном режиме.

## 3.4 Персобюро, используемое по умолчанию

Персобюро, используемое по умолчанию, задается в дополнительных параметрах производства карт, пункт меню "Full → Configuration Setup → Card Production Setup → Bank Production Parameters → [Parameters] → [Options]" (см. Рис. 17).

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

Name	Code	PAN MIN	PAN MAX	PIN Len	ICA	Card Type	Encoding Method	PVKI	Is Ready	Ready Till	Bank
[Test]Main PayPass OW	TEST_MAIN_PP_OW	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Main PayPass DC	TEST_MAIN_PP_ZPSN_O	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Main PayPass DC	TEST_MAIN_PP_ZPSN_TH	5555550000000000	5555559999999999	4	2222	MCHIP	MC	1	Ready	01/01/2020	1
[Test]Sub PayPass OW	TEST_SUB_PP_OW	5555550000000000	5555559999999999	4	2222	MCHIP	MC PayPass	1	Ready	00/00/0000	1

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/CCV 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

Рис. 17. Персобюро, используемое по умолчанию для набора параметров "[Test]Main PayPass OW"

В форме "Options" для соответствующего набора PM Parms следует указать:

- Option – дополнительный параметр "Default Perso Bureau Id".
- Value – код персобюро, которое будет использоваться по умолчанию для соответствующего набора параметров производства карт.

Доступ к транспортным ключам персобюро осуществляется в форме "Bureau Keys for < >" (см. Рис. 18), форма открывается с помощью кнопки [Bureau Keys] (см. Рис. 17).

Perso Bureau	Key Algorithm	Key Type	DES Key	DES Key Check	Storage Form
253DES ABA	PIN Export Key	Key Encryption Key	C6351A596168E48CA687D56BB8D50796	EE21F1	OWSeM / Host / Hex
253DES ABA	PIN Export Key	Key Encryption Key	0B7DF6F9886A8C0503E65214C0342CD	E2F243	OWSeM / Host / Hex

Рис. 18. Транспортные ключи персобюро

С помощью кнопки [Manage] выполняются стандартные действия над ключами (см. раздел "Кнопка [Manage]").