



Installation and Configuration Manual

Настройка параметров системы WAY4 для выпуска смарт-карт

03.51.30

23.10.2020

СОДЕРЖАНИЕ

1	Аппаратный модуль безопасности	6
1.1	Настройка Thales HSM в системе WAY4 [Настройка аппаратного модуля безопасности]	6
1.2	Настройка SafeNet ProtectServer Gold в системе WAY4	6
1.3	Настройка Gemalto Luna HSM в WAY4	6
2	Этапы настройки параметров системы для выпуска смарт-карт	7
2.1	Категории параметров производства карт	7
2.2	Последовательность настройки параметров	8
3	Схемы Контроля Рисков смарт-карт	9
3.1	Правила назначения Схем Контроля Рисков смарт-карт	9
3.2	Правила создания Схем Контроля Рисков смарт-карт	9
3.3	Настройка параметров Схемы Контроля Рисков смарт-карт	11
3.3.1	Загрузка шаблона параметров Схемы Контроля Рисков из файла	15
3.3.2	Пример определения значений параметров Схемы Контроля Рисков смарт-карт для контракта	15
3.3.3	Типы параметров Схем Контроля Рисков смарт-карт	16
3.3.4	Пример настройки Схемы контроля рисков для параметров категории EMVC	17
4	Параметры производства смарт-карт	19
4.1	Параметры производства смарт-карт для финансового института	19
4.1.1	Параметры производства смарт-карт	19
4.1.2	Параметры контроля подлинности	20
4.2	Карточные приложения	22
4.2.1	Параметры карточного приложения	22
4.2.2	Настройка нескольких приложений для карты	24
4.2.3	Настройка дополнительного карточного приложения без создания иерархии Продуктов	25
4.3	Криптографические ключи	27
4.3.1	3-DES ключи	29
4.3.2	Настройка параметров 3-DES ключей для использования аппаратных модулей безопасности различной конфигурации	37
4.3.3	RSA-ключи	38
4.4	Управляющие команды эмитента (Issuer Scripts)	46

4.4.1	Настройка параметров управляющих команд эмитента	46
4.4.2	Просмотр списка управляющих команд	49
4.4.3	Формирование ответной криптограммы эмитента	49
4.4.4	Блокировка карт с несколькими карточными приложениями	49
5	Ограничение количества попыток разблокировки PIN-кода режима offline	51
6	Автоматическая разблокировка offline PIN при успешном выполнении PBT-транзакции	55
7	Бюро персонализации	56
7.1	Регистрация персобюро [Организация работы]	56
7.2	Формирование транспортных ключей [Организация работы]	57
7.3	Пайпы, на которых задается идентификатор персобюро [Организация работы]	57
7.4	Персобюро, используемое по умолчанию [Организация работы]	57
8	Формирование пула RSA ICC Keys	59
8.1	ЛМК-ключи	60

Данный документ предназначен для пользователей системы WAY4™ (сотрудников банков или процессинговых центров), обеспечивающих настройку параметров системы подготовки данных для персонализации смарт-карт и управления ключами.

Система WAY4 управляет ключами RSA Visa, MasterCard, JCB и AMEX в соответствии со следующими документами:

- 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.
- Interface Specification. Amex AEIPS Chipcard Certificate Authority. August 2006.

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

- "Контроль рисков";
- "Модуль управления криптографическим устройством ProtectServer. Описание консольных команд";
- "Модуль Электрической Персонализации Смарт-Карт. Руководство Пользователя";
- "Основные технические требования для подсистемы подготовки данных и управления ключами системы WAY4";
- "Выпуск карт с магнитной полосой в системе WAY4™";
- "Настройка параметров системы WAY4™ для производства карт с магнитной полосой";
- "Пакеты Сервисов системы WAY4™";
- "Продукты и суб-типы контрактов";
- "Работа с DB Manager";
- "Установка и настройка модуля управления криптографическим устройством ProtectServer в системе WAY4™";
- "Загрузка и выгрузка заданий на производство карт в формате XML".

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 Аппаратный модуль безопасности

Для выполнения криптографических операций при подготовке данных для персонализации смарт-карт в системе должен быть установлен аппаратный модуль безопасности (HSM). Подробное описание типов устройств, используемых в качестве криптографического оборудования, приведено в документе "Основные технические требования для подсистемы подготовки данных и управления ключами системы WAY4".

1.1 Настройка Thales HSM в системе WAY4 (Настройка аппаратного модуля безопасности)

Правила использования устройств Thales изложены в разделе "Криптографическое оборудование" документа "Data Preparation and Key Management Subsystem Main Technical Requirements".

Для настройки параметров устройства Thales HSM в системе WAY4 предназначена форма, доступная при выборе пункта меню пользователя "Full → Configuration Setup → Card Production Setup → Security Device". Подробное описание настройки параметров с помощью данной формы приведено в разделе "Настройка параметров соединения рабочей станции с аппаратным модулем безопасности" документа "Настройка параметров системы WAY4 для производства карт с магнитной полосой".



Следует иметь в виду, что в качестве значения параметра поля *Transparent Mode* данной формы необходимо указать значение "Yes".

1.2 Настройка SafeNet ProtectServer Gold в системе WAY4

Подробная инструкция по установке и настройке устройств SafeNet ProtectServer Gold, ProtectServer External, PSE-Refresh и PSI-e приведена в документе "Установка и настройка модуля управления криптографическим устройством ProtectServer в системе WAY4™".

1.3 Настройка Gemalto Luna HSM в WAY4

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

2 Этапы настройки параметров системы для выпуска смарт-карт

В данной главе изложены правила использования категорий параметров в карточных приложениях и последовательность настройки параметров для производства карт.

2.1 Категории параметров производства карт

Категория параметров производства карты – признак, позволяющий использовать один и тот же набор параметров (тегов) в карточных приложениях для различных интерфейсов (см. раздел "[Карточные приложения](#)"). Использование категорий для карт с несколькими приложениями позволяют упростить настройку Продукта для производства таких карт.

Например, для выпуска карты с контактным и бесконтактным интерфейсом используется два EMV-приложения. В обоих приложениях присутствует тег 82 (Application Interchange Profile (AIP)). Принадлежность параметра определенной категории позволяет задавать ему необходимые значения для соответствующего интерфейса.

Кроме того, в соответствии со спецификацией EMV, часть параметров (например, 9F50, 9F51 и т.д.) настраиваются по правилам платежных систем. Категории позволяют использовать такие теги в соответствии с требованиями МПС.

В текущей версии поддерживаются следующие категории параметров:

- EMVT – параметры производства смарт-карт. Данная категория используется по умолчанию. Если при подготовке данных других категорий не будут заданы обязательные параметры производства, то по умолчанию применяются параметры данной категории.
- EMVC – параметры бесконтактного приложения (EMV Contactless).
- MSDC – параметры бесконтактного приложения для карт с магнитной полосой.
- UICC – параметры бесконтактного приложения для карт платежной системы UnionPay International.



Значения параметров категорий EMVC, MSDC, UICC имеют более высокий приоритет и переопределяют значения параметров категории EMVT.



Регистрация и распределение параметров по категориям выполняются поставщиком системы WAY4.

Пример регистрации параметра ESDD (Extended SDA DOL) для использования в EMVC и MSDC-категориях представлен на Рис. 1.

PM Options Types			<< < > >>	1 of 2	X
	Name	Code	Request Type		
→	Contactless EMV ESDD	EMVC.ESDD	Production		
	Contactless Magstripe ESDD	MSDC.ESDD	Production		
Ins	Del	Query			

Рис. 1. Пример регистрации, позволяющий использовать тег ESDD для приложений с категориями параметров EMVC и MSDC

Набор параметров определенной категории, с которым будет работать EMV-приложение, определяется при создании шаблона Схемы Контроля Рисков. Категория параметра представляется в поле *Category* формы "ParmType for ParmType for <наименование Схемы Контроля Рисков>" (см. Рис. 10). Пример настройки Схемы Контроля Рисков приведен ниже (см. раздел "Пример настройки Схемы контроля рисков для параметров категории EMVC").

Значения параметров, используемых в качестве дополнительных параметров контроля подлинности карт, например ESDD (Extended SDA DOL), представленный на Рис. 1, задаются в форме "Options for <наименование параметра>" (см. Рис. 16).

2.2 Последовательность настройки параметров

Настройка параметров системы WAY4 для выпуска смарт-карт включает в себя следующие этапы:

- Создание Схемы Контроля Рисков смарт-карт на основе существующего шаблона (см. "Схемы Контроля Рисков смарт-карт").
- Назначение карточному контракту созданной Схемы Контроля Рисков (см. "Правила назначения Схем Контроля Рисков смарт-карт").
- Задание параметров производства смарт-карт и параметров контроля подлинности для финансового института (см. "Параметры производства смарт-карт для финансового института").
- Определение параметров карточного приложения и, при необходимости, настроить несколько карточных приложений (см. "Карточные приложения").
- Сформировать и настроить параметры криптографических ключей: 3DES ключей (см. "3-DES ключи") и RSA-ключей (см. "RSA-ключи").
- После выполнения настройки параметров необходимо произвести выпуск смарт-карт. Процесс выпуска смарт-карт аналогичен процессу выпуска карт с магнитной полосой (см. документ "Выпуск карт с магнитной полосой в системе WAY4™").

3 Схемы Контроля Рисков смарт-карт

Под Схемой Контроля Рисков смарт-карт подразумевается набор транзакционных ограничений (параметров), записываемых в память микропроцессора при персонализации. Данные параметры могут также записываться в память микропроцессора с помощью управляющих команд эмитента (см. "[Управляющие команды эмитента \(Issuer Scripts\)](#)"). К числу таких ограничений могут относиться допустимое количество попыток ввода неправильного PIN-кода, максимально допустимая сумма транзакции и т. д.

3.1 Правила назначения Схем Контроля Рисков смарт-карт

Для каждого карточного контракта при выпуске смарт-карт должна быть назначена Схема Контроля Рисков. При этом Схема Контроля Рисков может быть назначена:

- На уровне Пакета Сервисов в поле *Chip Scheme* (см. раздел "Дополнительные параметры Пакете Сервисов" документа "Пакеты Сервисов системы WAY4™"). В данном случае она будет назначена для всех контрактов, использующих данный Пакет Сервисов.
- На уровне карточного контракта в поле *Chip Scheme* формы "Risk / Chip for <наименование контракта>", вызываемой с помощью нажатия на кнопку [Risk / Chip] в формах, предназначенных для настройки параметров контрактов (см. документ "Модуль эмиссии. Руководство пользователя").



В случае если для контракта назначена Схема Контроля Рисков как на уровне Пакета Сервисов, так и на уровне контракта, действительной является Схема Контроля Рисков, назначенная на уровне контракта.

3.2 Правила создания Схем Контроля Рисков смарт-карт

Схемы Контроля Рисков должны создаваться на основе шаблонов Схем Контроля Рисков. Шаблон Схем Контроля Рисков – это набор параметров, использование которых допустимо при создании Схем Контроля Рисков.

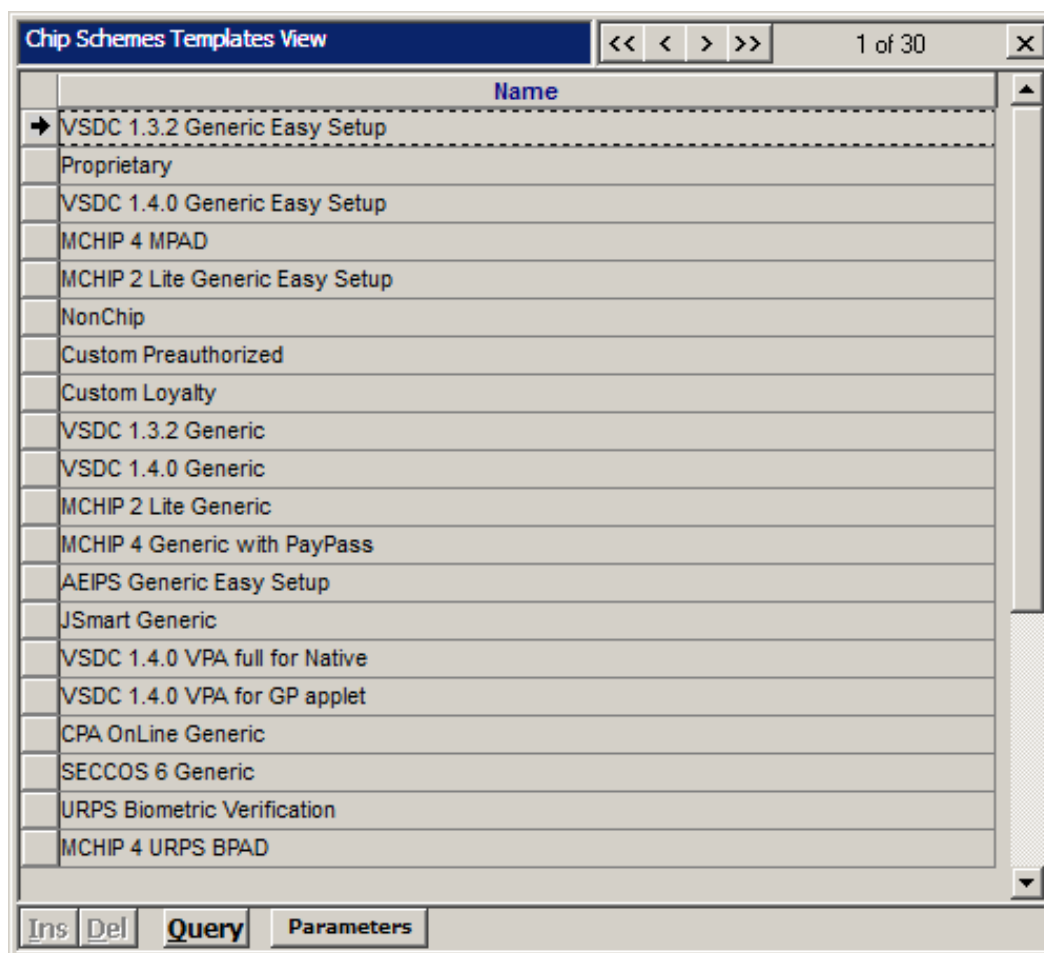


Использование параметров, которые не входят в состав шаблона, при создании Схемы Контроля Рисков недопустимо.



Создание шаблонов Схем Контроля Рисков осуществляется поставщиком системы.

Доступ к перечню шаблонов осуществляется с помощью формы "Chip Schemes Templates View" (см. [Рис. 2](#)), которая открывается при выборе пункта меню пользователя "EMV Smart Cards → Configuration → Chip Schemes Templates View".



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

Рис. 2. Шаблоны Схем Контроля Рисков

В поле *Name* данной формы указано наименование шаблона Схем Контроля Рисков.

Для просмотра параметров, входящих в состав шаблона Схем Контроля Рисков, предназначена форма "Parameters for <наименование шаблона>" (см. [Рис. 3](#)), которая вызывается с помощью нажатия на кнопку [Parameters] в форме "Chip Schemes Templates View".

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

Рис. 3. Набор параметров, входящих в состав шаблона Схем Контроля Рисков

Данная форма содержит следующие поля:

- *Parm Type* – тип параметра;
- *Parm Value* – значение параметра по умолчанию;
- *Parm Status* – статус параметра:
- "Mandatory" – параметр должен быть обязательно включен в Схему Контроля Рисков, и изменение его значения недопустимо;
- "Mandatory Changeable" – параметр должен быть обязательно включен в Схему Контроля Рисков, при этом его значение может быть изменено;
- "Optional" – параметр может быть включен в Схему Контроля Рисков, изменение его значения недопустимо;
- "Optional Changeable" – параметр может быть включен в Схему Контроля Рисков, при этом его значение может быть изменено.

3.3 Настройка параметров Схемы Контроля Рисков смарт-карт

Для настройки Схем Контроля Рисков для смарт-карт предназначена форма "Chip Schemes" (см. Рис. 4), которая открывается при выборе пункта меню "EMV Smart Cards → Configuration → Chip Schemes".

Chip Schemes			<< < > >>	2 of 6	X
	Name	Code	Scheme Template	Is Ready	
	VSDC EUR	VSDC_EUR	VSDC 1.3.2 Generic Easy Setup	Ready	
→	MCHIP 4 MPAD EUR	MPAD_EUR	MCHIP 4 MPAD	Ready	
	MC4 EUR PROFILED	MC4_PROFILED	MCHIP 4 Generic with PayPass	Ready	
	VSDC USD	VSDC_USD	VSDC 1.3.2 Generic	Ready	
	MC PayPass	MC_PAYPASS	MCHIP 4 Generic with PayPass	Ready	
	MCHIP2.1 EUR	MCHIP_EUR	MCHIP 2 Lite Generic Easy Setup	Ready	
Ins	Del	Query	Parms	Edit	Template

Рис. 4. Форма для настройки Схем Контроля Рисков для смарт-карт

Данная форма содержит следующие поля:

- *Name* – наименование Схемы Контроля Рисков;
- *Code* – код Схемы Контроля Рисков, присваиваемый пользователем и используемый в дальнейшем для идентификации схемы;
- *Scheme Template* – шаблон, на основе которого создана данная Схема Контроля Рисков;
- *Is Ready* – поле указывает, была ли утверждена Схема Контроля Рисков.

Для создания новой схемы следует нажать на кнопку [Ins] в указанной форме, при этом в форму будет добавлена новая запись. После этого необходимо выбрать новую запись и нажать на кнопку [Edit]. В результате на экране будет представлена форма "Edit for <наименование Схемы Контроля Рисков>" (см. Рис. 5).

Edit for MCHIP2.1 EUR		1 of 1		b X					
Base Scheme:	MCHIP2.1 EUR								
Scheme Template:	MCHIP 2 Lite Generic Easy Setu								
Code:	MCHIP_EUR								
Name:	MCHIP2.1 EUR								
Is Ready:	Not Ready								
<div> <div>Query</div> <div>Manage</div> <div>Parms</div> <div>Template</div> </div>									

Рис. 5. Форма для редактирования свойств Схемы Контроля Рисков

В данной форме необходимо заполнить поля, аналогичные полям формы "Chip Schemes" (см. Рис. 4).

После заполнения полей данной формы необходимо сконфигурировать параметры Схемы Контроля Рисков.

Конфигурирование параметров может быть выполнено автоматически с помощью загрузки шаблона (profile) параметров карточного продукта (см. [Загрузка шаблона параметров Схемы Контроля Рисков из файла](#)).

Для конфигурирования параметров Схемы Контроля Рисков вручную предназначена форма "Parms for <наименование Схемы Контроля Рисков>" (см. [Рис. 6](#)), которая открывается при нажатии в форме "Edit for <Наименование Схемы Контроля Рисков>" на кнопку [Parms].

Parms for VSDC 1.5								
			<< < > >>		12 of 21		b x	
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	DF4106000000005000DF51060000	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 & ScriptCmdCount RC00	0F	0F	Not Ready	Yes		
0,00	999,00	OAC CVR & ScriptCmdCount RC00	000000F0	000000F0	Not Ready	Yes		
0,00	999,00	OAC CVR & Script Fail	00000008	00000008	Not Ready	Yes		

Рис. 6. Форма для настройки параметров Схем Контроля Рисков

В данной форме заполняются следующие поля:

- *Risk Factor Max* и *Risk Factor Min* – максимальная и минимальная граница значения специального параметра "Risk Factor".
Текущие значения параметров Схемы Контроля Рисков для контракта зависят от того, в каком диапазоне находится значение параметра "Risk Factor" (см. ["Пример определения значений параметров Схемы Контроля Рисков смарт-карт для контракта"](#)).
- *Parm Type* – наименование параметра. Схема Контроля Рисков для смарт-карт должна содержать несколько обязательных параметров (для данных параметров в шаблонах определены соответствующие статусы).
- *Parm Value* – числовое значение параметра; параметр будет иметь данное значение в случае, если значение параметра "Risk Factor" контракта находится в пределах, заданных значениями, указанными в полях *Risk Factor Min* и *Risk Factor Max*. Данное поле будет недоступно для редактирования в случае, если параметр имеет тип "BER-TLV Container" (см. ["Типы параметров Схем Контроля Рисков смарт-карт"](#)), т.е. параметр состоит из нескольких параметров. В этом случае для определения значений подчиненных параметров необходимо нажать на кнопку [SubParms].

В случае если в данном поле содержится значение "VALUE_PROFILED", соответствующее выходное значение параметра, приведенное к типу параметра (значение поля *Parm Value Out*), было взято из загруженного файла шаблона (profile) параметров (см. ["Загрузка шаблона параметров Схемы Контроля Рисков из файла"](#)).



Если параметр *Parm Value* предназначен для определения суммы операции, то его значение указывается в минимальных единицах валюты (центах, пенсах и т.д.).

- *Parm Value Out* – выходное значение параметра, приведенное к типу параметра (см. раздел ["Типы параметров Схем Контроля Рисков смарт-карт"](#));

- *To OnLine* – при установлении в данном поле значения "Yes" параметр будет передаваться в режиме онлайн в виде управляющих команд эмитента (Issuer Script); при установлении значения "No" – параметр в режиме онлайн передаваться не будет;
- *Doc RC List* – список кодов ответа (Response Code) из системного перечня "Response Codes" ("Full → Main Tables → Response Code (Customise)"); в качестве разделителя используется запятая. При формировании управляющих команд эмитента (Issuer Script) будет выбрано значение параметра, соответствующее полученному коду ответа. Если не найдено значение параметра, соответствующее коду ответа, будет выбрано значение параметра с пустым кодом ответа.

Если параметр имеет тип "BER-TLV Container" (см. "Типы параметров Схем Контроля Рисков смарт-карт") в форме "Parms for <...>" (см. Рис. 6) будет доступна кнопка [SubParms]. При нажатии на данную кнопку будет представлена форма "SubParms for Parms for <...>", в поле *Parm Type* которой можно выбрать наименование подчиненного параметра, а в поле *Parm Value* указать значение параметра.

Кнопка [ParmType] формы "Parms for <...>" (см. Рис. 6) предназначена для просмотра информации о типе параметра (см. Типы параметров Схем Контроля Рисков смарт-карт).

После того как для Схемы Контроля Рисков будут сконфигурированы все параметры, необходимо утвердить Схему Контроля рисков. Для этого в форме "Edit for <наименование Схемы Контроля Рисков>" (см. Рис. 5) следует нажать на кнопку [Manage] и в открывшемся контекстном меню выбрать пункт "Approve".

В результате выбора данного пункта будет вызвана процедура проверки, соответствуют ли параметры Схемы Контроля Рисков шаблону, а также соответствуют ли значения параметров их типам. Помимо этого, произойдет заполнение поля *Parm Value Out*, данные которого получаются посредством форматирования данных поля *Parm Value*.

В случае если все данные о параметрах Схемы Контроля Рисков были указаны корректно, Схема Контроля Рисков будет утверждена, а на экран будет выведено окно с сообщением "Issuer Production Scheme approved".

В случае если какие-либо данные о параметрах Схемы Контроля Рисков были указаны некорректно, либо в состав Схемы Контроля Рисков не были включены какие-либо обязательные параметры, на экране появится окно с сообщением об ошибке. При этом Схема Контроля Рисков утверждена не будет.

Информация о причинах ошибок будет находиться в поле *Parm Value Out* формы "Parm for <наименование Схемы Контроля Рисков>" (например, см. Рис. 7).

Parms for VSDC 1.5							<< < > >>		2 of 21		b x	
	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 & ScriptCmdCount 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	0100000000000000	Ready	Yes					
Ins	Del	Query	ParmType									

Рис. 7. Пример сообщений об ошибках в конфигурировании параметров Схемы Контроля Рисков

3.3.1 Загрузка шаблона параметров Схемы Контроля Рисков из файла

Конфигурирование параметров Схемы Контроля Рисков смарт-карт может быть выполнено автоматически с помощью загрузки шаблона (profile) параметров карточного продукта.



Для VSDC данный шаблон может быть получен с помощью интернет-сервиса Visa. Для M/Chip данный шаблон может быть также получен от платежной системы MasterCard.

Для загрузки шаблона необходимо в форме "Edit for <наименование Схемы Контроля Рисков>" (см. [Рис. 5](#)) нажать на кнопку [Manage] и в контекстном меню выбрать пункт:

- "Load Profile" – для загрузки шаблона VSDC;
- "Load CPV Profile" – для загрузки шаблона M/Chip.
Загрузка профиля CPV/VPA, выполняемая с помощью пайпов `com.openwaygroup.pipe.cpv_import_chip_scheme.jar`, `com.openwaygroup.pipe.vpa_import_pm.jar`, может осуществляться с учетом категорий параметров (см. раздел "[Категории параметров производства карт](#)"). Данный механизм поддерживается с помощью параметра пайпов EMVCATEGORIES. Значения параметра EMVCATEGORIES:
- "Y" – загрузка параметров осуществляется с учетом категорий.
- "N" (значение по умолчанию) – загрузка параметров осуществляется без учета категорий.

После этого в открывшемся окне "Select files" необходимо выбрать соответствующий файл шаблона. Следует иметь в виду, что в диалоговом окне будут отображаться файлы с расширением "*.xml", расположенные в каталоге "<OWS_WORK>/data/card_prd/profiles/source".

В результате произойдет загрузка параметров в соответствии с выбранным шаблоном Схемы Контроля Рисков.



Следует иметь в виду, что для загруженных из файла параметров в поле *Parm Value* формы "Parms for <наименование Схемы Контроля Рисков>" (см. [Рис. 6](#)) будет указано значение "VALUE_PROFILED".

В случае если в файле содержатся параметры, которые отсутствуют в шаблоне Схемы Контроля Рисков, будет создан файл, содержащий данные параметры. Файл будет иметь имя "<имя исходного файла шаблона>.remainder.xml". Созданный файл необходимо загрузить в форму, содержащую параметры производства смарт-карт (см. "[Параметры карточного приложения](#)").

3.3.2 Пример определения значений параметров Схемы Контроля Рисков смарт-карт для контракта

Текущие значения параметров Схемы Контроля Рисков для контракта зависят от того, в каком диапазоне находится значение параметра "Risk Factor".

Значение данного параметра указывается в поле *Offline Limit Factor* формы "Risk Scheme for <имя клиента>" (см. Рис. 8), вызываемой на экран с помощью нажатия на кнопку [Risk Scheme] в формах, предназначенных для настройки параметров контрактов (см. документ "Модуль эмиссии. Руководства пользователя").

Рис. 8. Форма для назначения параметра "Risk Factor" Схемы Контроля Рисков для контракта

Таким образом, в случае указания параметру "Risk Factor" значения, равного "200", для параметра "9F54-VSDC Tot Cumul Amount Limit" текущим значением будет являться "1000" (см. Рис. 9).

Risk Factor Min	Risk Factor Max	Parm Type	Parm Value
0.00	100.00	CB-MCHIP Upper Cumul Amount	5000
100.01	999.00	CB-MCHIP Upper Cumul Amount	1000

Рис. 9. Определение значения параметра Схемы Контроля Рисков в зависимости от значения параметра "Risk Factor"

3.3.3 Типы параметров Схем Контроля Рисков смарт-карт

Описание типа параметра Схемы Контроля Рисков представлено в форме "ParmType for Parms for <наименование параметра>" (см. Рис. 10), которая открывается при нажатии на кнопку [ParmType] в форме "Parms for <наименование Схемы Контроля Рисков>" (см. Рис. 6) или в форме "SubParms for Parms for <...>".

Name	Code	Category	Min Length	Max Length	Value Format	Format Details	Is Custom	Parent Parameter Type
9F0D-Contactless IAC Default	9F0D	EMV contactless	10	10 Hex	h10	No	No	No

Рис. 10. Форма, содержащая определение типа параметра Схемы Контроля рисков

- Данная форма содержит следующие поля:
- *Name* – наименование параметра;
- *Code* – код параметра;

- *Category* – категория параметра (см. раздел "[Категории параметров производства карт](#)");
- *Min Length* – минимальная длина в символах значения параметра, указываемого пользователем в поле *Parm Value* формы "Parms for <наименование Схемы Контроля Рисков>" (см. [Рис. 6](#));
- *Max Length* – максимальная длина в символах значения параметра, указываемого пользователем в поле *Parm Value* формы "Parms for <наименование Схемы Контроля Рисков>";
- *Value Format* – формат значения, указываемого пользователем в поле *Parm Value* формы "Parms for <наименование Схемы Контроля Рисков>":
 - "Numeric" – десятичное число;
 - "String" – строка символов;
 - "Hex" – шестнадцатеричное число;
 - "BER-TLV Container" – тип BER TLV (Basic Encoding Rules Tag Length Value), данный тип представляет собой "контейнер", т.е. составной параметр, содержащий другие (подчиненные) параметры.
- *Format Details* – описание формата выходного значения:
 - "h<Число>" – шестнадцатеричное значение указанной длины, дополненное слева до указанной длины нулями;
 - "h?" – шестнадцатеричное значение с длиной, не противоречащей заданному диапазону *Min Length* – *Max Length*;
 - "h" – шестнадцатеричное значение; длина равна длине значения параметра в шаблоне;
 - "h<Число>P<Символ>" – шестнадцатеричное значение, дополненное справа до указанной длины указанными символами;
 - "n<Число>" – десятичное значение указанной длины, дополненное слева до указанной длины нулями;
 - "tag" – одна буква.
- *Is Custom* – поле, служащее для определения, является ли данный тип параметра стандартным типом параметра системы, либо данный тип является индивидуально настроенным типом для конкретного клиента.
- *Parent Parameter Type* – наименование родительского параметра; данное поле будет заполнено в случае, если данный параметр включен в составной параметр с типом "BER-TLV Container".

3.3.4 Пример настройки Схемы контроля рисков для параметров категории EMVC

Набор параметров, с которыми будет работать EMV-приложение, определяется в шаблоне Схемы Контроля Рисков.

Пример настройки параметров 9F0F, 9F0E, 9F0D для категории EMVC, а так же тегов BFxx, специфичных для платежной системы МИР, представлен ниже (см. [Рис. 11](#)).

[illegible]

Рис. 11. Настройка параметров категории EMVC

4 Параметры производства смарт-карт

К параметрам производства смарт-карт относятся как параметры, характерные для производства карт с магнитной полосой, так и параметры, характерные исключительно для производства смарт-карт. В данной главе приведено описание действий по настройке параметров производства смарт-карт.

Подробное описание действий по настройке параметров производства карт с магнитной полосой приведено в главе "Настройка параметров производства банковских карт" документа "Настройка параметров системы WAY4 для производства карт с магнитной полосой".

4.1 Параметры производства смарт-карт для финансового института

Настройка параметров для производства смарт-карт для финансового института осуществляется с помощью формы "Bank Production Parameters" (см. Рис. 12), которая открывается путем выбора пункта меню пользователя "Full → Configuration Setup → Card Production Setup → Bank Production Parameters". Настройка параметров осуществляется 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 55	0055	0055		Mr. Manager	
Test Bank 77	0077	0077		Mr. Manager	

Рис. 12. Форма для настройки параметров для производства смарт-карт



При настройке параметров для платежной системы MasterCard необходимо в поле *Production Details* данной формы указать наименование финансового института, под которым он зарегистрирован в платежной системе. В дальнейшем данное значение будет использоваться в наименовании файлов, участвующих в обмене ключами и сертификатами с бюро сертификации.

4.1.1 Параметры производства смарт-карт

Для задания параметров производства смарт-карт используется форма "Parameters for <наименование финансового института>" (см. Рис. 13), вызываемая на экран с помощью нажатия на кнопку [Parameters] в форме "Bank Production Parameters" (см. Рис. 12).

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	PROFIED	6799991000000000	6799991999999999	4	1111	MCHIP	MC	1	Ready	31/12/2012	1			
PIN Mailer	HH	0000000000000000	0000009999999999	4		Magnetic Card	PIN Mailer	1	Ready	00/00/0000	1			
Seccos		7777777777777777	7777777777777777	4	222	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. 13. Форма для ввода и настройки параметров производства смарт-карт

Значения параметров полей в данной форме для смарт-карт заполняются аналогично значениям параметров для карт с магнитной полосой за исключением значений в поле *Card Type*, где для платежной системы Visa должно быть указано значение "VSDC", для MasterCard – "MCHIP", для American Express – "AMEX EMV", для JCB – "JSmart", для UnionPay International (UPI) – "UICS".



Для карточного продукта MPAD на основе спецификации M/Chip4 в форме "Options for <наименование карточного продукта>", которая доступна при нажатии на кнопку [Options], необходимо указать дополнительный параметр "OAC CVR & MC4 Go Online Bit RC00", содержащий значение "0000000008".

4.1.2 Параметры контроля подлинности

Для задания параметров контроля подлинности банковской карты используется форма "Validation for <название финансового института>" (см. Рис. 14), вызываемая на экран с помощью нажатия на кнопку [Validation] в форме "Bank Production Parameters" (см. Рис. 12").

Validation for Test bank 1										<< < > >>			26 of 58	b x
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	5152540000000000	5152549999999999	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							

Рис. 14. Форма для настройки параметров проверки криптографических значений

Значения параметров полей в данной форме для смарт-карт заполняются аналогично значениям параметров для карт с магнитной полосой за исключением значений полей *EMV Crypto Scheme*, *EMV MAC Scheme* и *EMV Encr Scheme*, которые заполняются по следующим правилам:

- для карт VSDC (VISA Smart Debit Credit) указывается значение "VSDC";
- для карт VSDC++ указывается значение "VSDC+";
- для карт M/Chip2 указывается значение "MCHIP2";
- для карт M/Chip4 указывается значение "MCHIP4";

- для продуктов платежной системы JCB указывается значение "JSmart";
- для продуктов платежной системы American Express указывается значение "AMEX";
- для карт CPA v.4 указывается значение "EMV 2000 CPA V.4";
- для карт CPA v.5 указывается значение "CPA V.5";
- для продуктов платежной системы UnionPay International (UPI) указывается значение "CUP";
- для карт SECCOS указывается значение "SECCOS".

Формирование дополнительных параметров контроля подлинности смарт-карт осуществляется в форме "Options for <наименование параметра>" (см. Рис. 15), вызываемой с помощью кнопки [Options] в форме "Validation for <название финансового института>" (см. Рис. 14).

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. 15. Дополнительные параметры контроля подлинности смарт-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 параметров 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.

Пример настройки параметра EMVC.ESDD представлен ниже (см. Рис. 16).

Options for NSPK Mir Debit Classic Profile 313 Contactless Categorized		<< < > >>	1 of 14	b x
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+"00000000000000000000000000000000"			
Issuer PIN Format	UNDER_ZPK			
Chip CVC Present	Y			
		Ins Del	Query	Long Value

Рис. 16. Пример настройки ESDD категории EMVC

4.2 Карточные приложения

По стандарту EMV под карточным приложением подразумевается набор параметров, необходимых для обеспечения взаимодействия между терминалом и смарт-картой.

4.2.1 Параметры карточного приложения

Конфигурирование параметров карточного приложения может быть выполнено автоматически с помощью загрузки шаблона (profile) параметров карточного продукта.

Загрузка шаблона выполняется в форме "Parameters for <наименование финансового института>" (см. Рис. 13 в разделе "Параметры производства смарт-карт"). Для этого в данной форме необходимо нажать на кнопку [Manage] и выбрать пункт "Apply Profile" в открывшемся локальном меню. После этого в открывшемся окне "Select Files" необходимо выбрать соответствующий файл шаблона карточного приложения.



Если параметры карточного приложения используются только подсистемой PIN Management, необходимо загружать данные параметры из файла шаблона параметров карточного продукта. В случае настройки параметров Схемы Контроля Рисков смарт-карт загрузка параметров карточного приложения осуществляется из файла "<имя исходного файла шаблона>.remainder.xml", который был создан после загрузки параметров Схемы Контроля Рисков (см. "Загрузка шаблона параметров Схемы Контроля Рисков из файла").

Для настройки параметров приложения смарт-карты вручную предназначена форма "EMV for <...>" (см. Рис. 17), которая открывается с помощью нажатия на кнопку [EMV] в форме "Parameters for <наименование финансового института>" (см. см. Рис. 13 в разделе "Параметры производства смарт-карт"). Кнопки [VISA Parms] и [MC Parms] служат для вызова на экран форм, предназначенных для настройки специфичных для соответствующей платежной системы параметров.

Рис. 17. Форма для настройки параметров приложения смарт-карты



Значения полей формы "EMV for <наименование параметра>" следует заполнять в соответствии со значениями параметров шаблона приложения: для карт M/Chip в соответствии с требованиями, изложенными в документах "M/Chip 4 Issuer Guide to Debit and Credit Parameter Management" и "M/Chip Functional Architecture for Debit and Credit". В полях данной формы следует указывать значения полей таблицы "CARD DATA ELEMENTS" соответствующего шаблона.

Исключением является поле *Ext SDA Dol*, в котором определяется набор и последовательность данных, которые будут участвовать в SDA/DDA/CDA. Значение данного поля должно быть согласовано с системой электрической персонализации, установленной в банке.

В случае если в файле шаблона параметров содержатся дополнительные параметры, для которых в форме "EMV for <наименование параметра>" отсутствует соответствующее поле, данные параметры будут сохранены в тегированном виде. Для просмотра параметров и их значений используется форма "Options for <наименование параметра>" (см. Рис. 18), вызываемая с помощью нажатия на кнопку [Options] в форме "Parameters for <наименование финансового института>" (см. Рис. 13 в разделе "Параметры производства смарт-карт").

Options for Test VSDC	
7 of 7	
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
<input type="button" value="Ins"/> <input type="button" value="Del"/> <input type="button" value="Query"/> <input type="button" value="Long Value"/>	

Рис. 18. Дополнительные параметры приложения смарт-карты

4.2.2 Настройка нескольких приложений для карты

Согласно стандарту EMV на одну смарт-карту может быть загружено несколько приложений (multi-application card), в том числе и финансовых.

В системе WAY4 настройка нескольких приложений для карты обеспечивается за счет настройки иерархической структуры Продуктов в модуле эмиссии и настройки параметров карточных приложений в модуле подготовки данных и управления ключами.

Как в модуле эмиссии, так и в модуле подготовки данных и управления ключами для каждого карточного приложения настраивается отдельный диапазон номеров карт. При этом приложение, к диапазону номеров карт которого относится номер карты, эмбоосируемый на пластике, является основным, а остальные приложения – дополнительными.

4.2.2.1 Настройка иерархической структуры Продуктов

Для настройки нескольких приложений для карты в системе эмиссии необходимо настроить иерархическую структуру Продуктов с типом отношения Главный/Подчиненный (Main/Sub) (см. раздел "Ввод информации о Продуктах" документа "Продукты и суб-типы контрактов"). Для этого необходимо выполнить следующие действия:

- Для каждого диапазона номеров карт (карточных приложений) необходимо настроить суб-тип карточного контракта (см. раздел "Типы и суб-типы контрактов" документа "Продукты и суб-типы контрактов").
- Настроить иерархическую структуру Продуктов (см. раздел "Ввод информации о Продуктах" документа "Продукты и суб-типы контрактов"), где для главного Продукта указывается суб-тип контракта основного карточного приложения, а для подчиненных Продуктов – суб-типы дополнительных карточных приложений. Кроме того, для подчиненных Продуктов в форме "Full Info for <наименование Продукта>", открываемой с помощью нажатия на кнопку [Full Info] в форме для настройки параметров подчиненных Продуктов (см. Рис. 19), в поле *Relation Tag* необходимо выбрать из списка значение "Applet", а в поле *# of Contracts* указать значение "1".



Для приложений, использующих стандарт аутентификации CAP (Chip Authentication Program) следует в форме "Full Info for <наименование Продукта>" заполнить поле *Relation Type*, указав значение "CAP Applet".

В качестве примера на Рис. 19 продемонстрирована настроенная иерархическая структура Продуктов для карты, содержащей дебетовое приложение и приложение программы поддержки постоянных клиентов (loyalty programme).

The screenshot shows the 'Products' window with a tree view. The 'Principal' product is selected, and its details are shown in the 'Full Info for Loyalty Application' form. The form is divided into several sections: 'Main Properties', 'Accounting and Services', and 'Events'. The 'Main Properties' section includes fields for 'Category', 'Institution', 'Main Product', 'Product Name', 'Product Code', 'Code 2', 'Code 3', 'Contract Role', 'Date From', 'Date To', 'Is Active', 'IDT', 'Is Ready', 'Recur from', 'Scoring Model', '# of Contracts', 'Custom Data', and 'Product Group'. The 'Accounting and Services' section includes fields for 'Account Scheme', 'Contract Type', 'Contract Subtype', 'Service Pack', 'Report Type', 'Auth Scenario', 'Usage Scenario', 'Min Cr Limit', 'Max Cr Limit', 'Default Cr Limit', 'Tariff Domain', and 'Pers Tariff Domain Templ'. The 'Events' section includes fields for 'Duplicate', 'Events', 'Options', 'Serv Pack', 'Acc Scheme', 'Tagged Data', 'Choice Rules', and 'Mapping'.

Рис. 19. Иерархическая структура Продуктов для смарт-карты, содержащей два приложения



Следует обратить внимание на то, что для Продуктов иерархической структуры типа Главный/Подчиненный (Main/Sub) используется одна Схема Счетов.

После выполнения вышеуказанных действий по настройке иерархии Продуктов при регистрации карточного контракта необходимо указывать соответствующий Продукт, который является главным в иерархии (см. разделы "Регистрация карточных контрактов для физических лиц" и "Ввод новых контрактов юридических лиц (корпораций)" документа "Модуль Эмиссии. Руководство пользователя").

4.2.3 Настройка дополнительного карточного приложения без создания иерархии Продуктов

В системе существует возможность создания дополнительного карточного приложения без создания иерархии Продуктов. Данная возможность может использоваться только в случае, если

с помощью приложения (для которого не создается контракт) в системе не создаются и не обрабатываются документы. Таким приложением является, например, приложение биометрической верификации или апплет для бесконтактной части MasterCard PayPass.

Для создания дополнительного карточного приложения необходимо выполнить следующие действия:

- Для каждого диапазона номеров карт необходимо настроить иерархическую структуру суб-типов карточного контракта (см. раздел "Типы и суб-типы контрактов" документа "Продукты и суб-типы контрактов"). Для этого в форме "SubTypes for <наименование типа карточных контрактов>" необходимо выбрать суб-тип и нажать на кнопку [Applets]. В результате на экране будет представлена форма "Applets for <наименование суб-типа>" (см. [Рис. 20](#)).

SubTypes for Our VISA Cards										1 of 1		b x	
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			

Applets for 001-VISA Cards with Applet										1 of 1		b x	
Name	Prefix	Min Number	Max Number	PM Code	Fee Algorithm	Service Code	Validation Type	Add Params	Chip Scheme	Is Active			
Test Applet	12345	0000000000	9999999999	TST_APPL		101		CARD_PARAMS_LIST=ARQC_MK,AIP,PAN=MAIN;VSDC 1.5		Yes			

Рис. 20. Настройка иерархии суб-типов карточного контракта

В форме "Applets for <наименование суб-типа>" следует добавить запись о подчиненном суб-типе, а в поле *Chip Scheme* выбрать из списка Схему Контроля Рисков для карточного приложения.

В поле *Add Params* могут быть указаны следующие теги:

- "CARD_PARAMS_PREFIX=<строка>;" – префикс, который будет использоваться для идентификации параметров данного апплета во время обработки запросов по основному финансовому приложению карты.
- "CARD_PARAMS_LIST=<значения>;" – тег для указания кодов параметров, необходимых для проведения проверки. Коды перечисляются через запятую. Например, для приложения биометрической верификации необходимо указать "CARD_PARAMS_LIST=ARQC_MK,AIP;".
- "PAN=MAIN;" – тег, означающий, что номер карты для апплета наследуется из основного финансового приложения карты.
- Создать Продукт, указав в качестве суб-типа созданный на предыдущем шаге главный в иерархии суб-тип контракта. Следует иметь в виду, что на уровне Пакета Сервисов, заданного для Продукта, необходимо в поле *Chip Scheme* определить созданную ранее Схему Контроля Рисков (см. "[Схемы Контроля Рисков смарт-карт](#)").
Подробнее о создании Продукта см. в разделе "Ввод информации о Продуктах" документа "Продукты и суб-типы контрактов".
- Создать карточный контракт, в качестве суб-типа контракта указав главный в иерархии суб-тип. В результате при маркировке карт для выпуска будет создана запись о дополнительном карточном приложении, которая доступна при нажатии на кнопку [Applet] в форме "Plastics for <...>", открываемой при нажатии на кнопку [Plastics] карточного контракта (см. [Рис. 21](#)).

Рис. 21. Карточный контракт и дополнительное карточное приложение

4.3 Криптографические ключи

В данном разделе описывается процедура формирования и настройки параметров криптографических ключей.

Кроме того, в данном разделе описаны также особенности конфигурации системы для случая, когда для работы системы подготовки данных и системы обработки транзакций в режиме онлайн (Online Processing) используются аппаратные модули безопасности (HSM) различной конфигурации (различных производителей) (см. "[Настройка параметров 3-DES ключей для использования аппаратных модулей безопасности различной конфигурации](#)").

Формирование криптографических ключей, необходимых для производства смарт-карт, может производиться на аппаратных модулях, различных как по назначению, так и по типу конфигурации (см. [Рис. 22](#)).

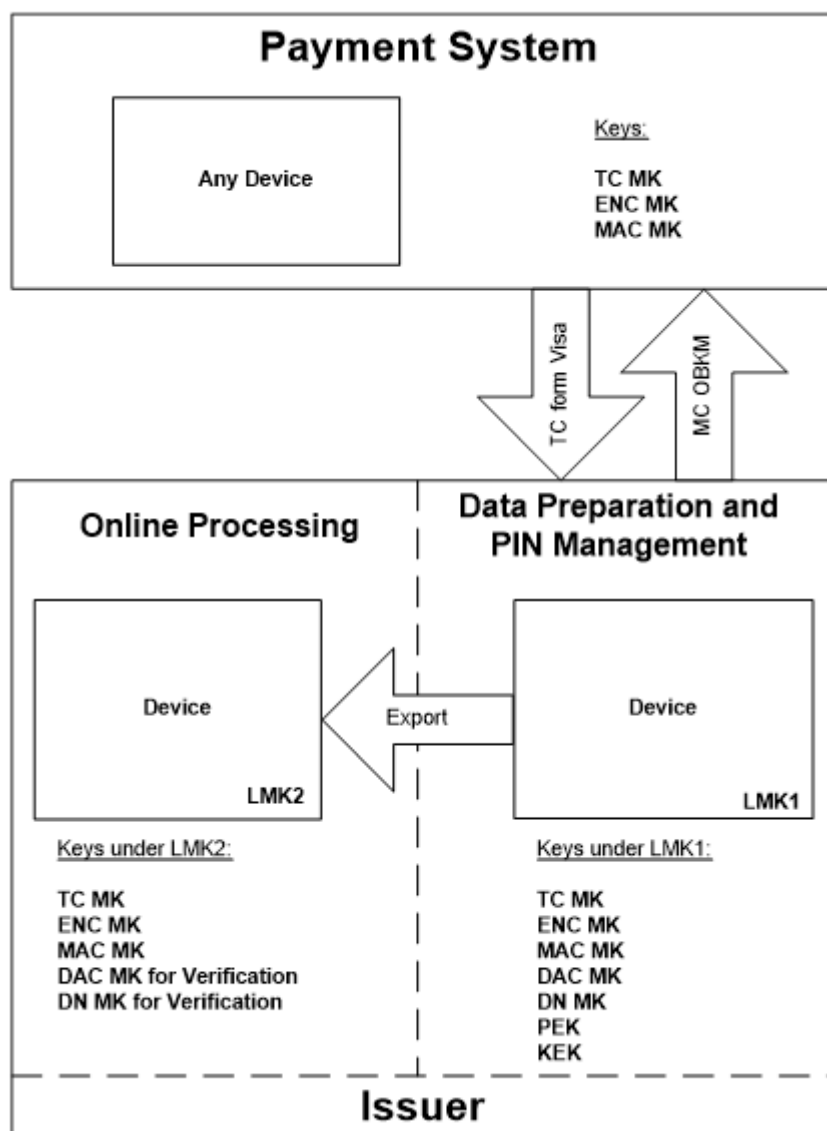


Рис. 22. Криптографические ключи производства смарт-карт в системе WAY4

В системе предусматриваются следующие варианты формирования криптографических ключей:

- формирование ключей на аппаратном модуле безопасности системы подготовки данных и управления ключами (Data Preparation and PIN Management);
- получение ключей от платежной системы.



Следует иметь в виду, что при формировании, а также импорте и экспорте криптографических ключей на устройствах различных конфигураций используются различные команды. При этом следует руководствоваться соответствующей документацией на аппаратный модуль безопасности, а именно:

- для Thales payShield 9000 – "payShield 9000 Security Operations Manual";
- для устройств SafeNet – "Модуль управления криптографическим устройством ProtectServer. Описание консольных команд".



Формирование криптографических ключей для устройств SafeNet OWSeM или Thales рекомендуется производить с помощью пайпа "DES Key Management" (см. "Формирование ключей").

4.3.1 3-DES ключи

При производстве смарт-карт используются следующие криптографические ключи алгоритма 3-DES:

- "TC Master Key" – данный ключ предназначен для формирования и подтверждения подлинности криптограмм ARQC, ARPC и TC.
- "MAC Master Key" – данный ключ предназначен для формирования и подтверждения подлинности цифровой подписи управляющих команд эмитента.
- "Encryption Master Key" – данный ключ предназначен для шифрования и дешифрации данных, содержащихся в управляющих командах эмитента, например, offline pin.
- "DAC Master Key" – данный ключ предназначен для формирования величины Data Authentication Code для карт M/Chip стандарта SDA (Static Data Authentication).
- "DAC Master Key for Verification" – данный ключ предназначен для проверки в режиме онлайн величины Data Authentication Code для карт M/Chip стандарта SDA (Static Data Authentication).
- "DN Master Key for Production" – данный ключ предназначен для формирования величины DN для карт стандарта DDA (Dynamic Data Authentication).
- "DN Master Key for Production & Verification" – данный ключ предназначен для проверки в режиме онлайн величины DN для карт стандарта DDA (Dynamic Data Authentication).
- "Key Encryption Key" – данный ключ предназначен для шифрования и дешифрации ключей при передаче данных из системы подготовки данных (PIN Management) в подсистему электрической персонализации.
- "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.
- "PayPass Dynamic CVC3 Master Key" – данный ключ предназначен для формирования и проверки в режиме онлайн величины Dynamic CVC для карт MasterCard PayPass.
- "PayPass Dynamic CVC3 Master Key for Production" – данный ключ предназначен для формирования величины Dynamic CVC для карт MasterCard PayPass. Этот тип ключа используется только для устройств Thales payShield 9000 (без базовой прошивки).
- "PayWave Dynamic CVV Master Key" – данный ключ предназначен для формирования величины Dynamic CVV для карт Visa PayWave.
- "AMEX CSC Key" – данный ключ предназначен для формирования и проверки в режиме онлайн величины CSC (Card Security Code) для карт платежной системы AMEX.
- "Bioverification TC Master Key" – данный ключ предназначен для формирования и подтверждения подлинности криптограммы приложения биометрической верификации.
- "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.
- "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.



В случае если в системе используется устройство Thales HSM payShield 9000, вместо ключа "DN Master Key for Production" необходимо использовать ключ "DN Master Key for Production & Verification".

Данные ключи являются мастер-ключами, т.е. ключами, при помощи которых выполняется диверсификация уникальных ключей карты.

Для настройки параметров 3-DES мастер-ключей предназначена форма "3-DES Keys for <наименование типа выпускаемой карты>" (см. [Рис. 23](#)), которая открывается с помощью нажатия на кнопку [3-DES Keys] в форме "EMV for <наименование параметра>".

3-DES Keys for VSDC DDA									
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	TC Master Key	USD44B4F3D5ACA848ABD75E22164E13F5	858E55	00/00/00 00	00/00/00 00		HSM / Host / Hex	Ready	00/00/0000
3DES ABA	MAC Master Key	UF49BCF23DDDD76D005B244C4A4E42B2AE	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

Рис. 23. Форма для настройки 3-DES ключей

В случае если для работы системы подготовки данных и системы обработки транзакций в режиме онлайн используются устройства HSM различной конфигурации необходимо выполнить инструкции, описанные в разделе ["Настройка параметров 3-DES ключей для использования аппаратных модулей безопасности различной конфигурации"](#).

Способ формирования 3-DES ключей зависит от типа устройства HSM, используемого в системе (см. ["Настройка аппаратного модуля безопасности"](#)).

Рекомендуемым способом формирования 3-DES ключей является их формирование с помощью пайпа "DES Key Management" (см. ["Формирование ключей"](#)). Запуск пайпа осуществляется в форме "DES Management Mode", вызываемой с помощью нажатия на кнопку [Manage] в форме "3-DES Keys for <наименование типа выпускаемой карты>". При формировании ключей данным способом их параметры автоматически загружаются в базу данных, и дополнительных действий по настройке их параметров не требуется.



Данный способ формирования поддерживается для всех типов устройств, используемых в системе (см. ["Настройка аппаратного модуля безопасности"](#)).

4.3.1.1 Формирование ключей

Формирование 3-DES 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.



Данный способ формирования поддерживается для всех типов устройств HSM, используемых в системе (см. "[Настройка аппаратного модуля безопасности](#)").

Перед началом формирования ключа в форме "3-DES Keys for <наименование типа выпускаемой карты>" (см. [Рис. 23](#) в разделе "[3-DES ключи](#)") 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;
- "OWSeM / Host / Hex" – для ключа, формируемого на устройстве производства компании SafeNet.
- "GL / Host / HEX" – формируемого на устройстве производства компании Gemalto.



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. [Рис. 23](#) в разделе "[3-DES ключи](#)") нажать на кнопку [Manage].

4.3.1.1.1 Кнопка (Manage)

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

- "Manage" – при выборе данного пункта на экране будет представлена форма "PM DES Management Mode" (см. [Рис. 24](#)).

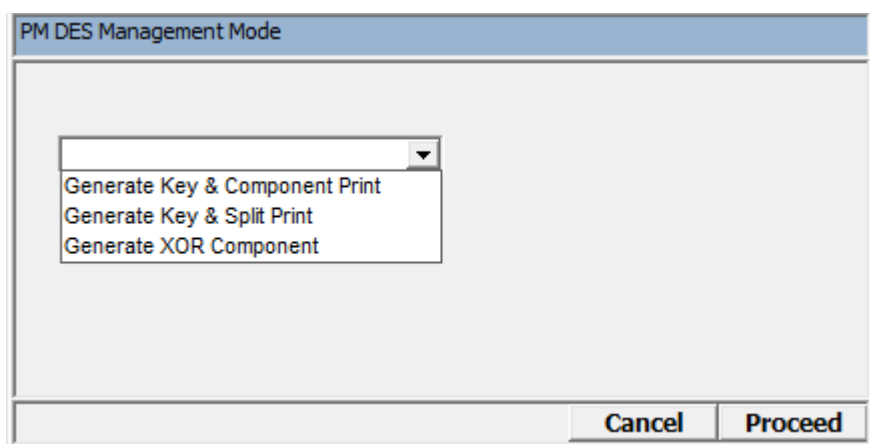


Рис. 24. Форма для выбора режима формирования криптографических ключей

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 отдельная 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 \(No Printing\)"](#)").

4.3.1.1.2 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 использования.

4.3.1.1.3 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. [Рис. 23](#) в разделе "[3-DES ключи](#)") 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 использования.

4.3.1.1.4 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. [Рис. 23](#) в разделе ["3-DES ключи"](#)), отличается от рассчитанного с помощью HSM, на экране будет представлено окно с сообщением об ошибке.

4.3.1.1.5 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.

4.3.1.1.6 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.

4.3.1.2 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. 25](#)) определить шаблоны для печати.

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

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

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

Рис. 25. 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. 25](#)).
- 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.

4.3.1.2.1 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}]  
-
```

4.3.1.2 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.

4.3.2 Настройка параметров 3-DES ключей для использования аппаратных модулей безопасности различной конфигурации

Для обеспечения работы системы подготовки данных и системы обработки транзакций в режиме онлайн используются 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 PSG), для данных устройств всегда используются различные наборы LMK. При этом при конфигурации системы необходимо руководствоваться следующими инструкциями:

- формирование ключей рекомендуется осуществлять на устройстве системы подготовки данных и управления ключами, либо ключи могут быть получены от платежной системы (см. раздел "[Криптографические ключи](#)");
- ключи, необходимые для подтверждения подлинности (validation) транзакционной информации, должны быть импортированы в устройство системы обработки транзакций в режиме онлайн;
- для каждого ключа, зашифрованного с помощью LMK различных устройств, необходимо вручную зарегистрировать две записи в форме "3-DES 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 устройство HSM компании Thales по методу Variant (при импорте ключа для параметра "Key Scheme" было указано значение "U"), в поле *DES Key* формы "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 LMK устройства производства компании Thales;
- "OWSeM / Host / Hex" – для ключа, зашифрованного под 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 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.

- "LN" – 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" документа "Настройка параметров системы WAY4™ для выпуска карт с магнитной полосой").



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 устройств, с помощью которых будет производиться расчет криптографических величин;
- для второго подпункта меню указать с помощью параметра "SM_ID" указать идентификатор устройства, 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™").

4.3.3 RSA-ключи

Для производства смарт-карт используются два типа RSA-ключей:

- Открытый ключ эмитента (Issuer Public Key), используемый в виде сертификата для подписи данных при производстве всех типов смарт-карт (см. "[Открытый ключ эмитента](#)"), подписанный открытым ключом бюро сертификации (см. "[Открытые ключи бюро сертификации](#)").



Бюро сертификации являются организациями, выдающими сертификаты для открытых ключей сторонних организаций, в частности – банков-эмитентов. В случае получения сертификатов, необходимых банкам-эмитентам для производства смарт-карт, бюро сертификации является подразделением соответствующей платежной системы.

- Секретный ключ карты (ICC Key – Integrated Circuit Card Private Key), используемый как дополнительное средство для подтверждения подлинности карты (см. "[Секретный ключ карты](#)"). Данный ключ используется только для карт DDA (Dynamic Data Authentication) и CDA (Combined Data Authentication).

4.3.3.1 Открытый ключ эмитента

Открытый ключ эмитента (Issuer Public Key) формируется эмитентом с помощью аппаратного модуля безопасности, установленного в системе (см. "[Настройка аппаратного модуля безопасности](#)"). Затем данный ключ должен быть отослан на подпись в бюро сертификации в виде файла специального формата (формат файла определяется соответствующей платежной системой). В результате подписи открытого ключа эмитента секретным ключом бюро сертификации формируется сертификат ключа эмитента. Далее данный сертификат должен быть получен от бюро сертификации совместно с открытым ключом бюро сертификации. Затем полученный открытый ключ бюро сертификации и сертификат ключа эмитента необходимо загрузить в систему WAY4, после чего данный сертификат может быть использован для верификации карт.



Следует обратить внимание на то, что загрузку открытого ключа бюро сертификации в систему WAY4 необходимо осуществить перед загрузкой в систему сертификата открытого ключа эмитента (см. раздел "[Открытые ключи бюро сертификации](#)").

Схема обмена ключами и сертификатами с бюро сертификации представлена на [Рис. 26](#).

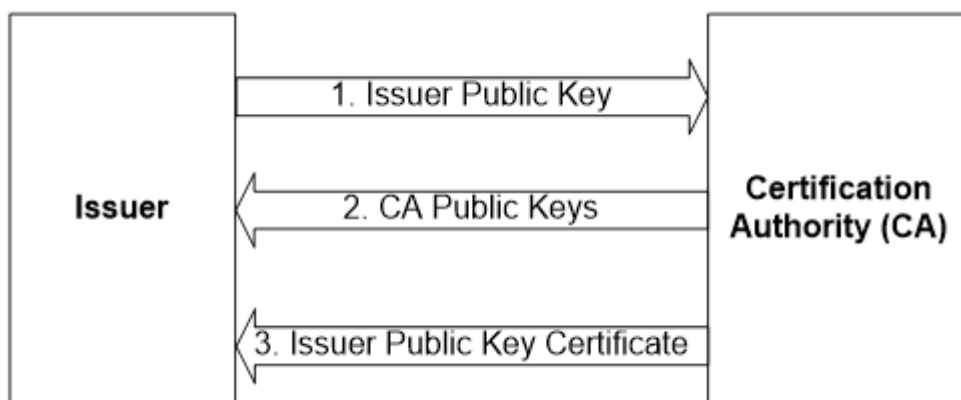


Рис. 26. Обмен открытыми ключами и сертификатами с бюро сертификации

Для настройки параметров открытого ключа эмитента в системе WAY4 необходимо выполнить следующие действия:

- Открыть форму для настройки параметров RSA-ключей "RSA Keys for <наименование параметра>" (см. [Рис. 27](#)), нажав на кнопку [RSA Keys] в форме "EMV for <наименование параметра>" (см. [Рис. 17](#) в разделе "Карточные приложения").

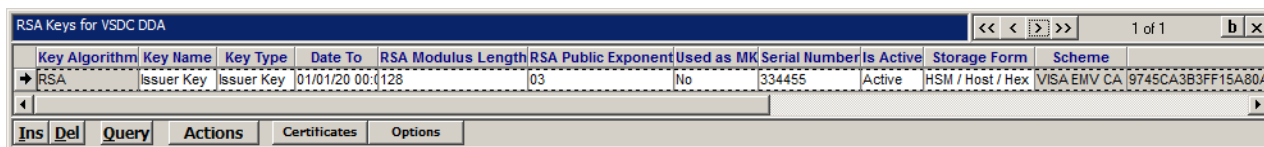


Рис. 27. Форма для настройки параметров RSA-ключей

- В открывшейся форме необходимо заполнить следующие поля:
- Key Name** – наименование ключа.
- Key Type** – тип ключа. Для открытого ключа эмитента в данном поле следует выбрать значение "Issuer Key".
- Date To** – дата окончания действия ключа.
- RSA Modulus Len** – длина ключа, указывается в байтах.
- RSA Public Exponent** – открытая экспонента, используемая в RSA-шифровании; поле может принимать одно из двух значений: "03" или "010001".
- Serial Number** – шестизначный номер ключа. Данный номер используется в наименовании файла открытого ключа эмитента, отсылаемого на подпись в бюро сертификации. Для платежной системы VISA значение номера ключа будет предоставлено платежной системой; для платежной системы MasterCard – заполнено автоматически при формировании ключа.
- Storage Form** – способ хранения ключа.
- После заполнения значений полей вышеуказанной формы необходимо в локальном меню, которое вызывается при нажатии на кнопку [Actions], выбрать пункт [Manage]. В результате на экране отобразится форма "RSA Management Mode" (см. [Рис. 28](#)), в которой следует выбрать процедуру "Generate Key Pair" и нажать на кнопку [Proceed].

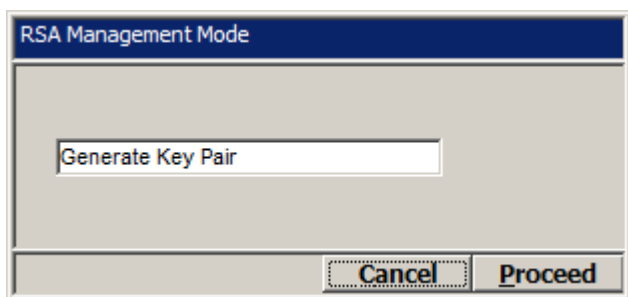


Рис. 28. Форма для выбора процедуры формирования RSA-ключей

В случае если открытый ключ эмитента был успешно сформирован, файл сформированного ключа эмитента будет помещен в каталог, указанный в параметре SOURCE_DIR (либо в параметре DEFAULT_PATH) пайпа "RSA EMV Key Management". Если параметры SOURCE_DIR, DEFAULT_PATH не заданы, будет сформировано сообщение об ошибке.

Вместе с формированием файла с открытым ключом эмитента будут также сформированы два сертификата:

- сертификат, имеющий тип "Self Signed" и используемый для верификации открытого ключа эмитента в бюро сертификации;
- сертификат, имеющий тип "Public Key MAC" и используемый для хранения сертификата эмитента в БД.

Параметры данных сертификатов будут отражены в форме "Certificates for <наименование ключа>" (см. [Рис. 30](#)), которая открывается с помощью нажатия на кнопку [Certificates] в форме "RSA Keys for <наименование параметра>" (см. [Рис. 27](#)).

После того, как открытый ключ эмитента был сформирован, необходимо отправить его на подпись в бюро сертификации. Отправка открытого ключа эмитента на подпись осуществляется в соответствии с требованиями платежной системы.

После того, как открытый ключ эмитента был подписан секретным ключом бюро сертификации и получен эмитентом в виде сертификата совместно с открытым ключом бюро сертификации, необходимо произвести загрузку данного сертификата, а также открытого ключа бюро сертификации в систему WAY4.



В соответствии с требованиями платежных систем все файлы (выгружаемые и загружаемые), участвующие в обмене открытыми ключами и сертификатами, имеют заданную структуру имен файлов. Поэтому не рекомендуется переименовывать данные файлы вручную.



Следует обратить внимание на то, что до загрузки в систему сертификата ключа эмитента необходимо произвести загрузку открытого ключа бюро сертификации. Последовательность действий, выполнение которых необходимо для загрузки в систему открытого ключа бюро сертификации, описана в разделе "[Открытые ключи бюро сертификации](#)".

Для загрузки сертификата необходимо выполнить следующие действия:

- в форме "Certificates for <наименование ключа>", которая открывается при нажатии на кнопку [Certificates] в форме "RSA Keys for <наименование параметра>", следует создать новую запись, выбрав в поле *Type* значение "EMV CA" и выбрав в поле *Master Key* название предварительно загруженного открытого ключа бюро сертификации, с помощью которого был подписан данный сертификат.
- в форме "RSA Keys for <наименование параметра>", нажать на кнопку [Actions] и в появившемся локальном меню выбрать пункт [Manage], в результате чего на экране отобразится форма "RSA Management Mode", в которой следует выбрать процедуру "Load Issuer PK Certificate" и нажать на кнопку [Proceed] (см. [Рис. 29](#)).

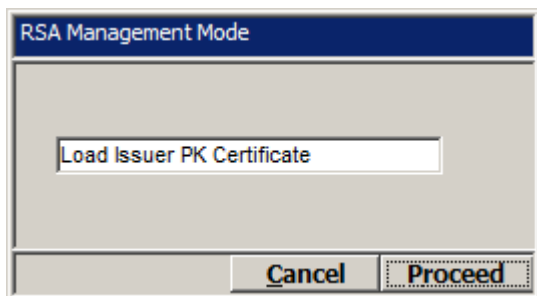


Рис. 29. Процедура загрузки сертификата открытого ключа эмитента

Выбрать необходимый файл из каталога, указанного в параметре SOURCE_DIR папки "RSA EMV Key Management". Если параметр SOURCE_DIR не задан, будет выбран первый подходящий файл из каталога, заданного в параметре DEFAULT_PATH (если задан DEFAULT_PATH и SOURCE_DIR не задан). Если параметры SOURCE_DIR, DEFAULT_PATH не заданы, будет сформировано сообщение об ошибке.

В случае успешной загрузки сертификата открытого ключа эмитента информацию о данном сертификате можно получить в форме "Certificates for <наименование ключа>", которая открывается при нажатии на кнопку [Certificates] в форме "RSA Keys for <наименование параметра>" (см. Рис. 30).

Certificates for Issuer Key												3 of 3		b	x
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		22809745CA3B3FF15A6		D5D3EA6923	Ready	00/00/0000				
EMV CA		SHA-1	RSA	Test CA VISA 22	334455		606AA18F05832DA1CC	0362F56A5666259E2F6144		Ready	00/00/0000				

Рис. 30. Сертификаты открытого ключа эмитента

Если, в соответствии с бизнес-требованиями, клиенту необходимо сохранить в файле значение сформированного открытого ключа эмитента без сопутствующей дополнительной информации (например, keyblock header), то следует воспользоваться процедурой "Extract Public Key" (см. Рис)

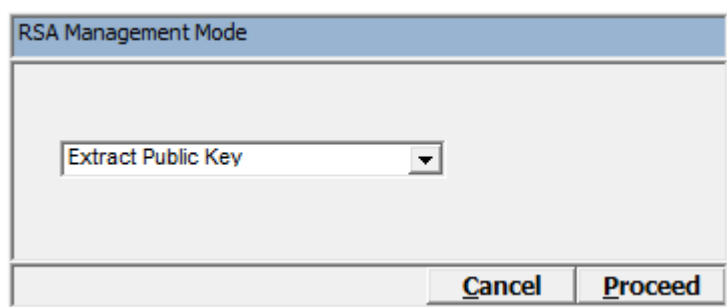


Рис. Форма для выбора процедуры выгрузки RSA-ключей

Файл со значением открытого ключа эмитента будет помещен в каталог, указанный в параметре SOURCE_DIR (либо в параметре DEFAULT_PATH) папки "RSA EMV Key Management".

4.3.3.2 Открытые ключи бюро сертификации

Для настройки параметров открытого ключа бюро сертификации в системе WAY4 необходимо выполнить следующие действия:

- В форме "CA Keys for <наименование банка>" (см. Рис. 31), которая открывается при нажатии на кнопку [CA Keys] в форме "Bank Production Parameters" (см. Рис. 12 в разделе "Параметры производства смарт-карт для финансового института"), необходимо создать новую запись, заполнив для нее обязательные поля следующими значениями:
- в поле *Scheme Code* необходимо указать принадлежность к платежной системе;
- в значении поля *Scheme Add Data* следует указывать идентификатор приложения (RID+PIX), который, в соответствии со стандартом VSDC Personalization Template, либо MasterCard Minimum Card Requirements составляется посредством конкатенации следующих двух значений:
- первые десять символов – значение RID (Registered Application ID) идентификатора приложения, хранящегося на смарт-карте (фактически идентифицирует владельца приложения VISA, MC);
- вторая часть – значение PIX (Proprietary Extension) – тип приложения;
- в поле *Key IDT in Scheme* необходимо указать индекс открытого ключа бюро сертификации, который может иметь значение в пределах от "00" до "FF";
- *Key Type* – тип ключа.

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 OWtest2	VISA EMV CA	23	A0000000031010	Active

Рис. 31. Форма для ввода и настройки открытых ключей бюро сертификации

- Затем в форме "CA Keys for <наименование банка>", следует нажать на кнопку [Manage], при нажатии на которую на экране будет представлена форма "RSA Management Mode" (см. Рис. 32), где следует выбрать процедуру "Import CA Public Key" и нажать на кнопку [Proceed].

RSA Management Mode

Import CA Public Key

Cancel Proceed

Рис. 32. Форма для вызова процедуры загрузки ключа

- В случае успешной загрузки открытого ключа бюро сертификации в поле *RSA Modulus* формы "CA Keys for <наименование банка>" для ключа будет представлено его зашифрованное значение. Кроме того, в форме "Certificates for <наименование ключа>" (см. Рис. 33), которая открывается при нажатии на кнопку [Certificates] в форме "CA Keys for <наименование банка>", будут представлены два сертификата с типами "Public Key MAC" и "Self Signed".

Certificates for Test CA VISA 22								<div><< < [x] >></div>		2 of 2		<div>b x</div>	
	Type	Format	Hash Alg	Signature Alg	Master Key	Serial #	Authentication Data	Certificate Body					
	Public Key MAC							D6FE3B79					
→	Self Signed		SHA-1	RSA	5430			201010000000800101A00000000322AFDF88D93					
<div>< [input type="text"/> ></div>													
<div>Ins Del Query</div>													

Рис. 33. Сертификаты открытого ключа бюро сертификации

4.3.3.3 Секретный ключ карты

Секретный ключ карты (Integrated Circuit Card Private Key) используется как дополнительное средство подтверждения подлинности карты при аутентификации DDA (Dynamic Data Authentication).

Данный ключ формируется как уникальное для каждой карты значение с помощью аппаратного модуля безопасности при выпуске карт.

Настройка параметров секретного ключа карты осуществляется в форме "RSA Keys for <наименование параметра>" (см. Рис. 34).

RSA Keys for VSDC DDA										<< < > >>		1 of 1		b x	
	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:	128	03			Active	HSM / Host / Hex					
<div></div>															
Ins Del Query Actions Certificates Options															

Рис. 34. Форма для настройки параметров секретного ключа карты

Для секретного ключа карты следует заполнить следующие поля данной формы: *Key Type* (в данном поле необходимо выбрать значение "ICC Key"), *RSA Modulus Len*, *RSA Public Exponent*.



Не следует выполнять формирование данного ключа с помощью выбора пункта контекстного меню "Manage", доступного при нажатии на кнопку [Actions] данной формы.

4.3.3.4 Режим предварительной генерации секретных ключей карты

В случае если необходимо сформировать большое количество секретных ключей карты, что может потребовать значительных временных затрат, рекомендуется использовать режим предварительной генерации ключей.

Пул предварительно созданных ICC ключей хранится в отдельной таблице PM_PREGENED_KEYS. Алгоритм генерации ICC ключей зависит от типа устройства HSM (подробнее см. раздел "Формирование пула RSA ICC Keys").

Для этого необходимо использовать следующие настройки:

- Добавить в форму "RSA Keys for <наименование параметра>" (см. Рис. 35) новую запись, заполнив поля *Key Type*, *RSA Modulus Len*, *RSA Public Exponent*. Кроме того, в поле *Is Active* необходимо указать значение "Active for Pre-Generation".

Рис. 35. Настройка режима предварительной генерации секретного ключа карты

- Указать количество формируемых ключей. Для этого в форме "Parameters for <наименование финансового института>" (см. Рис. 13 в разделе "Параметры производства смарт-карт") необходимо нажать на кнопку [Options], после чего в форму "Options for <наименование карточного продукта>" (см. Рис. 36) добавить параметр "ICC Keys To Gen", указав в поле Value необходимое количество ключей.

Рис. 36. Количество формируемых ключей



В данной форме рекомендуется также задать формат ключа с помощью параметра "ICC Key Format". Описание форматов ключа представлено в разделе "Формат ключа ICC RSA" документа "Загрузка и выгрузка заданий на производство карт в формате XML".

Генерация ключей осуществляется одним из следующих способов:

- В форме "RSA Keys for <наименование параметра>" (см. Рис. 35) необходимо выбрать запись, у которой в поле Is Active указано значение "Active for Pre-Generation", затем нажать на кнопку [Actions] и в открывшемся контекстном меню выбрать пункт "PRE-generate ICC Keys". Записи о сгенерированных ключах будут доступны в данной форме, при этом в поле Is Active каждой записи будет указано значение "Pre-Generated".
- Выбрать в меню пользователя пункт "EMV Smart Cards → Card Production → RSA ICC Keys PRE-Generation → RSA ICC Keys PRE-Generation". В результате на экране будет представлена форма "RSA ICC Keys PRE-Generation" (см. Рис. 37), содержащая список всех записей из формы "RSA Keys for <наименование параметра>" (см. Рис. 35), для которых необходимо сгенерировать секретные ключи карты.

Рис. 37. Список ключей для предварительной генерации

Для того чтобы сгенерировать ключи, необходимо в данной форме нажать на кнопку [Proceed], после чего в контекстном меню выбрать один из пунктов:

- "Generate keys for current row" – генерация ключей для текущей записи.
- "Generate keys for all" – генерация ключей для всех записей таблицы.
- "Wipe ICC keys" – удалить предварительно сгенерированные секретные ключи для выбранной строки (карты). Данная возможность может использоваться, например, в случае изменения длины или формата ключа.



Подробнее об особенностях предварительной генерации RSA ICC ключей см. раздел ["Формирование пула RSA ICC Keys"](#).

4.4 Управляющие команды эмитента (Issuer Scripts)

На протяжении всего срока действия смарт-карты со стороны эмитента ей могут быть отправлены управляющие команды (Issuer Scripts). Существуют следующие разновидности данных команд:

- сменить PIN-код;
- разблокировать PIN-код;
- заблокировать карту;
- заблокировать приложение;
- разблокировать приложение;
- изменить параметры Схемы Контроля Рисков;
- отправить на карту ответную криптограмму (ARPC – Authorization Response Cryptogram).

4.4.1 Настройка параметров управляющих команд эмитента

Для настройки параметров управляющих команд эмитента предназначена форма "Commands for <наименование параметра>" (см. [Рис. 38](#)), которая открывается с помощью нажатия на кнопку [Commands] в форме "EMV for <наименование параметра>" (см. раздел ["Карточные приложения"](#)).



Следует иметь в виду, что параметры управляющих команд эмитента заданы в соответствующих шаблонах Схем Контроля Рисков (см. ["Просмотр списка управляющих команд"](#)). Возможность настройки параметров управляющих команд в форме "Commands for <наименование параметра>" присутствует в системе для обеспечения совместимости с предыдущими версиями.

Набор, а также параметры управляющих команд эмитента следует задавать в соответствии с требованиями платежной системы к типу микропроцессора смарт-карты, используемой

эмитентом. На рисунках в данном разделе представлен набор параметров управляющих команд эмитента, которые необходимо задавать для соответствующих типов карт.

Commands for MChip2.1 Lite										
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 Domestic 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										

Рис. 38. Параметры команд карточных приложений для карт M/Chip2

Commands for MC MChip4 MPAD SDA										
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										

Рис. 39. Параметры команд карточных приложений для карт M/Chip4

Commands for VSDC SDA										
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	

Рис. 40. Параметры команд карточных приложений для карт VSDC

Commands for JSmart										
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	

Рис. 41. Параметры команд карточных приложений для карт JSmart

Commands for AMEX EMV Chip										
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	

Рис. 42. Параметры команд карточных приложений для карт AMEX EMV

4.4.2 Просмотр списка управляющих команд

В системе существует возможность просмотра списка управляющих команд эмитента. Для этого необходимо в форме "Chip Schemes" (см. Рис. 4 в разделе "Настройка параметров Схемы Контроля Рисков смарт-карт") нажать на кнопку [Template], после чего в форме "Template for <Наименование Схемы Контроля Рисков>" нажать на кнопку [Scr.Cmnd]. В результате на экране будет представлена форма "Scr.Cmnd for <наименование шаблона Схемы Контроля Рисков>" (см. Рис. 43).

Scr.Cmnd for MCHIP 2 Lite Generic Easy Setup										
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	

Рис. 43. Список управляющих команд эмитента

4.4.3 Формирование ответной криптограммы эмитента

Система WAY4 при совершении контактной операции по смарт-карте может отправлять платежному приложению специальные управляющие биты вместе с ответной криптограммой эмитента - Authorisation Response Cryptogram (ARPC).

Поддерживаются две технологии отправки управляющих битов:

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

Использование той или иной технологии определяется параметрами платежного приложения карты.

Для формирования ARPC RC в схеме контроля рисков должны быть определены параметры (*Parm Type*) "APPROVE_ONLINE_TRANS" и "DECLINE_ONLINE_TRANS".

Для формирования CSU - параметры (*Parm Type*) "CPA CSU *".



Для каждой схемы контроля рисков может быть определена только одна из двух групп параметров.

4.4.4 Блокировка карт с несколькими карточными приложениями

Для смарт-карт используются специальные тип команд на блокировку ("APPLICATION BLOCK") и разблокировку ("APPLICATION UNBLOCK") приложения карты, что позволяет временно заблокировать одно или несколько приложений карты.

Таким образом поддерживается возможность работы с картой, одно из приложений которой может быть заблокировано до определенного момента времени.

В случае утраты карты (потери, кражи), может осуществляться одновременная блокировка всех приложений карты.

При попытке авторизации, для предотвращения дальнейшего использования карты, по заблокированному номеру одного из приложений смарт-карты должна быть отправлена специальная команда "CARD BLOCK".

Для этого в поле *Chip card action type* справочника "Contract Statuses", пункт меню Full → Configuration Setup → Contract Types → Contract Statuses, для карт в соответствующих статусах ("карта утеряна", "карта украдена") следует установить значение "CARD BLOCK".

Contract Statuses						<< < > >>	1 of 1	X
	Category	Name	Code	Is Valid	External Code	Code Parms	Chip Card Action Type	
→	Card	PickUp L 41	41	Decline	41		Block Card	
</								

5 Ограничение количества попыток разблокировки PIN-кода режима offline

В системе существует возможность ограничить количество попыток разблокировки PIN-кода режима offline.

Для реализации данной функциональности необходимо выполнить следующие настройки:

1. Добавить в перечень дополнительных онлайн-операций (Additional Online Services) новый тип с кодом "OFFLINE_PIN_UNBLOCK". Для выполнения этой операции необходимо выбрать в меню пользователя пункт "Full → Configuration Setup → Merchant Device Setup → Additional Online Services", после чего добавить новый тип онлайн-операции в форму "Additional Online Services" (см. [Рис. 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					
<div> Ins Del Query Services Full Info Quota </div>										

Рис. 44. Добавление дополнительной онлайн-операции

1. Зарегистрировать новый тип транзакции в перечне "Transaction – All" (Full → Configuration Setup → Transaction Types → Transaction – All). Затем необходимо определить специальный тип сообщения в форме "Msg Types for <...>", вызываемой с помощью нажатия на кнопку [Msg Types] после выбора в перечне "Transaction – All" созданного типа транзакции (см. [Рис. 45](#)).

Transactions - All												
Service Class	Source	Target	Name	DR/CR	Previous	Chain Type	Is Authorized	s Required	Category	BS Code	RBS Rev Code	Dispute Class
Additional Online Service	Device	Card	Offline PIN Unblock	None		Original		Yes	Individual			
<div> Ins Del Query Fill SubTypes Msg Types Reasons Requirements Msg Dict </div>												

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
<div> Ins Del Query </div>							

Рис. 45. Создание типа транзакции и соответствующего типа сообщения

1. Создать новый тип События (Event Type) в форме "Event Types" (Full → Configuration Setup → Products → Event Types). Тип События представлен на [Рис. 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			
<div> Ins Del Query Check Messages Full Info Event Chain Used By Classifiers </div>										

Рис. 46. Создание нового типа События

1. В перечень "Usage Operations" (Full → Configuration Setup → Alerting Setup → Usage Operations) добавить следующую запись (см. Рис. 47).

Usage Operations			<< < > >>		1 of 1	X
Name	Usage Type	Event Code				
→ Incorrect PIN	Negative RC					
Ins Del Query						

Рис. 47. Добавление записи в перечень "Usage Operations"

Для данной операции из справочника "Usage Operations" необходимо зарегистрировать коды ответов на авторизационный запрос. Коды ответов регистрируются в форме "Response Code Usage" (Full → Configuration Setup → Alerting Setup → Response Code Usage). Коды ответов представлены на Рис. 48.

Response Code Usage			<< < > >>		2 of 2	X
Contract Category	Response Code	Usage Operation				
Card	Incorrect PIN	Incorrect PIN				
→ Card	Allowable number of PIN tries exceeded	Incorrect PIN				
Ins Del Query						

Рис. 48. Настройка кодов ответов

1. В Пакете Сервисов, используемом для карточных контрактов, необходимо создать ограничитель активности контракта. Для этого в форме "Private Card Service Packs" (Full → Configuration Setup → Products → Issuing Private Products → Private Card Service Packs) выбираем требуемый Пакет Сервисов, после чего нажимаем на кнопку [Usage] и добавляем ограничитель активности в форму "Usage For <...>" (см. Рис. 49).

Usage for 001-Our Priv MCHIP													<< < > >>			1 of 1		b x	
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	0,00	Yes	Ready			
Ins		Del	Query	Details	Approved	Messages													

Рис. 49. Настройка ограничителя активности

Следует иметь в виду, что в поле *Max #* указано максимальное количество попыток разблокировки PIN-кода режима offline.

Кроме того, в форме дополнительной информации об ограничителе "Details for <...>" следует заполнить поля *Trans Type*, *Event Type* и *Custom RC* (см. Рис. 50).

Рис. 50. Настройка дополнительных параметров ограничителя

1. Создать подключаемый (Additional) Пакет Сервисов в форме "Private Card Service Packs", в который необходимо добавить требуемые Target-сервисы, указав в поле *Transaction Type* тип транзакции, созданный в пункте 2. Пример Пакета Сервисов представлен на Рис. 51.

Private Card Service Packs											<< < > >>			1 of 1		x	
	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		b	x
	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													

Рис. 51. Создание подключаемого Пакета Сервисов

1. Для обеспечения сброса счетчика при успешной смене PIN-кода режима offline необходимо для каждого сервиса из подключаемого Пакета Сервисов в поле *Service Details* указать тег "ZEROIZE_USAGE_COUNTERS=<usage_code>;", где <usage_code> – код созданного

в Пакете Сервисов ограничителя активности. В нашем примере следует указать код "OFF_PIN_UNBLK".



Если в Схеме Контроля Рисков смарт-карты задан параметр "RESET_PTC_ON_PIN_SET", для которого указано значение "N" (см. Рис. 6 в разделе "[Настройка параметров Схемы Контроля Рисков смарт-карт](#)"), то при успешной смене PIN-кода режима offline не выполняется сброс счетчика количества попыток неправильного ввода PIN-кода. Если параметр "RESET_PTC_ON_PIN_SET" не задан или для него указано значение "Y", то при успешной смене PIN-кода происходит сброс счетчика количества попыток неправильного ввода PIN-кода.

- Подключить созданный в пункте 6 Пакет Сервисов к основному Пакету Сервисов, для которого был создан ограничитель активности (см. пункт 5). Настроить отключение дополнительного Пакета Сервисов при открытии События с типом, определенном в пункте 3.

6 Автоматическая разблокировка offline PIN при успешном выполнении PBT-транзакции

В системе существует возможность обнуления счетчика количества попыток неправильного ввода offline PIN-кода при первом успешном вводе онлайн PIN-кода, т.е. при успешном выполнении PBT-транзакции (PIN Based Transaction).

Для этого необходимо в форме для настройки параметров Схем Контроля Рисков смарт-карт (см. Рис. 6 в разделе "[Настройка параметров Схемы Контроля Рисков смарт-карт](#)") определить параметр "OAC CVR & PIN Try Lim Exc RC00", указав для платежной системы Visa (карты "VSDC") значение "00004000", а для платежной системы MasterCard (карты "MCHIP") – "000000080000".

После выполнения данной настройки проверка количества попыток неправильного ввода PIN-кода осуществляется следующим образом:

- Если на смарт-карте превышено число попыток неправильного ввода offline PIN-кода, смарт-карта формирует запрос на ввод онлайн PIN-кода.
- Если держатель карты ввел правильное значение онлайн PIN-кода, системы формирует управляющую команду эмитента на разблокирование offline PIN-кода. В этом случае счетчики количества попыток неправильного ввода offline и онлайн PIN-кода будут синхронизированы.
- Если держатель карты ввел неверное значение онлайн PIN-кода, система присваивает максимальное значение счетчику количества попыток неправильного ввода онлайн PIN-кода, т.е. блокирует онлайн PIN-код. Следовательно, карта будет заблокирована, что приведет к невозможности выполнения по ней операций.

7 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 смарт-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.

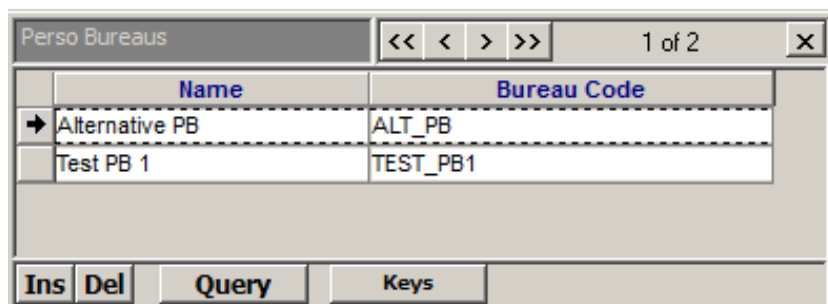
Для каждого персобюро создаются свои транспортные ключи шифрования. Таким образом, имея один набор параметров производства карт (PM Params), но используя транспортные ключи того или иного персобюро, поддерживается возможность оптимизировать процесс персонализации карт сразу в нескольких персобюро.

Персобюро, используемое по умолчанию для персонализации карт, задается для соответствующего набора параметров (PM Params) финансового института (см. раздел 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 Params.

7.1 Регистрация персобюро (Организация работы)

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

Рис. Перечень персобюро

Заполнить поля:

- *Name* – наименование персобюро.

- *Bureau Code* – код персобюро.

Перечень персобюро хранится в таблице PM_KEY_OWNER (OWNER_TYPE="PERSO_BUREAU").

7.2 Формирование транспортных ключей (Организация работы)

Транспортные ключи создаются стандартно, с помощью аппаратного модуля безопасности (см. раздел "3-DES ключи").

Транспортные ключи формируются в форме "Keys for <>" (см. Рис. 53) стандартным способом (см. раздел "Формирование ключей"). Форма "Keys for <>" вызывается с помощью кнопки "Keys" из формы "Perso Bureaus".

Keys for Test PB 1					
<div> <div><< < > >></div> <div>1 of 2</div> <div>b x</div> </div>					
Perso Bureau	Key Algorithm	Key Type	DES Key	DES Key Check	Storage Form
→ 1	3DES ABA	PIN Export Key	U7568FA7C6EB1C8A84A5290AA90ADC87C	E2F243	HSM / Host / Hex
1	3DES ABA	Key Encryption Key	UA940CC330472671D0CDA49CCF19924DD	EE21F1	HSM / Host / Hex
<div> <div>Ins Del</div> <div>Query</div> <div>Manage</div> <div>Options</div> </div>					

Рис. 53. Транспортные ключи PEK и KEK

7.3 Пайпы, на которых задается идентификатор персобюро (Организация работы)

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

7.4 Персобюро, используемое по умолчанию (Организация работы)

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. 54).

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_T	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
SF28 - 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. 54. 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. 55), форма открывается с помощью кнопки [Bureau Keys] (см. Рис. 54).

Perso Bureau	Key Algorithm	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

Рис. 55. Транспортные ключи персобюро

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

8 Формирование пула RSA ICC Keys

Формирование пула ICC-ключей зависит от типа устройства HSM:

- Thales™ payShield 9000 Card Issuer Firmware или устройства SafeNet через интерфейс OWSEM;
- Thales™ payShield 9000 Base Firmware.

При формировании пула определяется модель HSM, на котором производится предварительная генерация ICC-ключей.

В том случае если устройство поддерживает генерацию ICC-ключа только под транспортным ключом KEK, то создается ключ под соответствующим ключом выбранного персобюро. К таким устройствам относятся Thales™ payShield 9000 Card Issuer Firmware и устройства SafeNet, работающие через интерфейс OWSEM.

Если устройство поддерживает генерацию ICC-ключа под LMK-ключом HSM, то процедура формирования пула меняется: для выбранного устройства запрашивается контрольное значение LMK-ключа. Далее, по полученному контрольному значению находится запись о LMK-ключе в таблице PM_KEYS (см. Рис. 57 в разделе "[LMK-ключи](#)"). Если для полученного контрольного значения ещё нет записи в таблице PM_KEYS, то она будет создана автоматически. Вновь созданный ICC-ключ будет сохранен в таблице PM_PREGENED_KEYS с указанием ссылки на используемый LMK-ключ.

Правила предварительной генерации ICC-ключей подробно изложены в разделе "[Режим предварительной генерации секретных ключей карты](#)". Кроме того, для PM Parms следует указать персобюро, используемое по умолчанию (см. раздел "Персобюро, используемое по умолчанию").

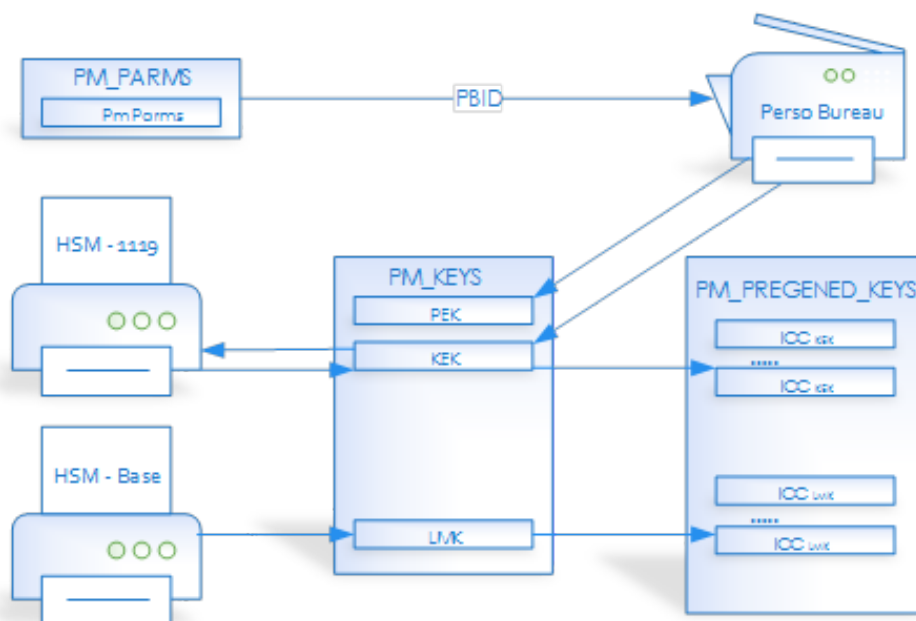


Рис. 56. Генерация и хранение RSA ICC Keys

8.1 LMK-ключи

Информация о LMK-ключах, использовавшихся при генерации ICC-ключей, доступна для просмотра в форме "LMK Keys", пункт меню Full → Configuration Setup → Card Production Setup → LMK Keys (см. Рис. 57).

LMK Keys				<< < > >>		1 of 1		X
	Name		DES Key Check		Storage Form		Additional Data	
→	THALES9000BASE_NEWIP 268604		268604		HSM / Device / Hex			
Ins	Del	Query						

Рис. 57. Перечень LMK-ключей для ICC LMK

В таблице представлены поля:

- *Name* – наименование ключа.
- *DES Key Check* – контрольной суммы сформированного ключа (Key Check Value, KCV).
- *Storage Form* – способ хранения ключа. Для ключа, формируемого на устройстве производства компании Thales, значения поля равно "HSM / Host / Hex".
- *Additional Data* – поле зарезервировано, в текущей версии не используется.