

# Выгрузка криптографических ключей в платежную систему Mastercard

# Содержание

ВВЕДЕНИЕ	1
ГЛАВА 1. ОБЩИЕ ПРИНЦИПЫ РАБОТЫ С ОВКМ	2
ГЛАВА 2. ВЫГРУЗКА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ	3
Регистрация транспортных ключей Mastercard	3
Выгрузка ключей смарт-карт и карт с магнитной полосой	4
Параметры пайпа "МС ОВКМ Export"	8



## Введение

Настоящий документ предназначен для сотрудников банков или процессинговых центров, ответственных за выгрузку криптографических ключей в платежную систему Mastercard, а также за взаимодействие с сервисом Mastercard On-behalf Key Management (OBKM).

При работе с данным документом рекомендуется пользоваться следующими источниками:

- "Настройка параметров системы WAY4™ для выпуска карт с магнитной полосой";
- "Настройка параметров системы WAY4™ для выпуска смарт-карт";
- "On-behalf Key Management (OBKM) Document Set".

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 отмечены знаком ;
- сообщения, помеченные знаком , содержат информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

## Глава 1. Общие принципы работы с ОВКМ

Платежная система Mastercard предоставляет эмитенту сервис (Mastercard On-behalf Key Management, ОВКМ), с помощью которого она может осуществлять проверку криптографических величин карты, а также выполнять авторизацию вместо банка-эмитента. Данный сервис может быть использован, например, в случае временной недоступности (из-за сбоя или выполнения регламентных работ) производственной базы данных (БД).

Система WAY4 поддерживает двухуровневый механизм передачи ключей (Two-Level Key Hierarchy) эмитента в платежную систему. Это означает, что все ключи эмитента шифруются транспортными ключами, полученными от Mastercard, после чего передаются в платежную систему.

Для выгрузки криптографических ключей в платежную систему необходимо выполнить следующие настройки:

- Собрать из открытых компонент ключей, полученных от платежной системы Mastercard, транспортные ключи "ВКАМ" (Transport Key for Message Authentication) и "ВКЕМ" (Transport Key for Encryption).
- Сгенерировать ключ "OKEN" (Network Key). Данный ключ будет использоваться для шифрования/дешифрования PIN-блока или сессионных ключей. Значение данного ключа следует внести в конфигурацию NetServer, а также в канал взаимодействия с платежной системой Mastercard.
- Для ключей карт с магнитной полосой ("CVK1", "CVK2" и "PVK") и для ключа смарт-карты ("IMK<sub>ac</sub>") определить дополнительные параметры в соответствии с требованиями платежной системы Mastercard.
- Определить дополнительные параметры выгрузки: уникальный идентификатор эмитента в платежной системе Mastercard, идентификатор центра управления криптографическими ключами (КМС, Key Management Centre) и т. п.
- Сформировать файлы с криптографическими ключами и отправить их в платежную систему.

## Глава 2. Выгрузка криптографических ключей

Выгрузка криптографических ключей выполняется с помощью пайпа "МС ОВКМ Export" (см. "Параметры пайпа "МС ОВКМ Export"). Перед выгрузкой необходимо выполнить соответствующие настройки в БД системы WAY4.

### Регистрация транспортных ключей Mastercard

Платежная система Mastercard отправляет эмитенту открытые компоненты следующих транспортных ключей:

- "ВКЕМ" (Transport Key for Encryption) – данный ключ используется для шифрования/дешифрования ключей.
- "ВКАМ" (Transport Key for Message Authentication) – ключ, используемый для электронной подписи передаваемых ключей, т.е. аутентификации сообщения с помощью MAC (Message Authentication Code).

Из открытых компонент ключей с помощью команды "FK" консоли управления криптографическим устройством (HSM) необходимо собрать данные ключи:

- "ВКЕМ" – ключ двойной длины с типом "ZMK" (Zone Master Key). В качестве схемы ключа (Key Scheme) следует указать значение "U".
- "ВКАМ" – ключ двойной длины типа "ТАК" (Terminal Authentication Key). В качестве схемы ключа (Key Scheme) следует указать значение "U".

Кроме того, для шифрования/дешифрования PIN-блока необходимо на криптографическом устройстве с помощью команды "KG" сгенерировать ключ "ОКЕН" (Network Key), который представляет собой ключ двойной длины типа "ZPK" (Zone Pin Key). В качестве схемы ключа (Key Scheme) следует указать значение "U".

После того как получены зашифрованные под LMK криптографического устройства ключи "ВКЕМ", "ВКАМ" и "ОКЕН", необходимо зарегистрировать их в базе данных. Для этого необходимо в форме "Bank Production Parameters" (Full → Configuration Setup → Card Production Setup → Bank Production Parameters) нажать на кнопку [МС ОВКМ].

В результате на экране будет представлена форма "МС ОВКМ for <...>", в которую следует добавить три записи, указав в поле *Key Type* значения "МС ОВКМ ВКАМ key", "МС ОВКМ ВКЕМ (ZMK) key" и "МС ОВКМ ОКЕН (ZPK) key". В полях *DES Key* и *DES Key Check* следует указать значение и контрольную сумму, соответственно, ключей "ВКАМ", "ВКЕМ" и "ОКЕН". Кроме того, для данных ключей в поле *МС ОВКМ Key Set Id* следует указать уникальный идентификатор (четырёхзначное число) ключей, полученный от платежной системы Mastercard.



зависимости от типа ключа представлен в документе "On-behalf Key Management (OBKM) Document Set". Например, для ключа "PVK" в данном поле будет содержаться 40 байт информации: код ответа в случае ввода неправильного PIN-кода, метод проверки PIN-кода и т. п. Дополнительные параметры могут быть определены также с помощью следующих параметров пайпа "MC OBKM Export" (см. "Параметры пайпа "MC OBKM Export"); при этом значения параметров пайпа имеют более высокий приоритет:

- ["EXTRA PVK DATA"](#) – для ключа "PVK";
- ["EXTRA CVK1 DATA"](#) – для ключа "CVK1";
- ["EXTRA CVK2 DATA"](#) – для ключа "CVK2";
- ["EXTRA CVK3 DATA"](#) – для ключа "IMK<sub>CVK3</sub>";
- ["EXTRA TCMK DATA"](#) – для ключа "IMK<sub>ac</sub>";
- ["EXTRA CAVV DATA"](#) – для ключа "AAVK".

Пример заполнения полей формы "3-DES Keys for <...>" представлен на Рис. 2.

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	PVK	U08080808080808080808080808080808	D6A875	01/01/18 00:00:00	31/12/21 00:00:00	0550860750867701081601	HSM / Host / Hex	Ready	31/12/2021

Buttons: Ins, Del, Query, Manage, Options

Рис. 2. Дополнительные параметры ключей

Поле *Date From* формы "3-DES Keys for <...>" должно содержать значение, описанное в разделе "Floor Expiry Date" документа "On-behalf Key Management (OBKM) Document Set". Для всех выгружаемых ключей в данном поле должно быть указано одно и то же значение.

Поле *Date To* должно содержать дату окончания срока действия ключа, используемую для формирования имени файла экспорта в соответствии с рекомендациями раздела "Communication Requirements" документа "On-behalf Key Management (OBKM) Document Set". Для всех выгружаемых ключей в данном поле должно быть указано одно и то же значение.

Выгрузка ключа "AAVK" выполняется на основании параметров, заданных в форме "3-DES Keys for <...>" (см. Рис. 2). Если в указанной форме параметры для данного ключа не заданы, для выгрузки ключа будут использованы параметры, заданные в форме "DES Keys for <...>". Эта форма вызывается на экран после нажатия на кнопку [DES] в форме "Bank Production Parameters". Для обеспечения указанной возможности выгрузить ключ "AAVK", в форме "DES Keys for <...>" должны быть заданы параметры для DES-ключей "AAVK\_A" и "AAVK\_B". Эти составляющие при выгрузке будут использованы для формирования 3-DES-ключа "AAVK".

Для 3-DES ключей "PVK", "CVK1", "CVK2", "IMK<sub>ac</sub>", "IMK<sub>CVK3</sub>" и "AAVK" необходимо также определить дополнительные параметры выгрузки. Они задаются в форме "Options for <...>", вызываемой на экран при нажатии на кнопку [Options] в форме "Parameters for <...>", которая в свою очередь

открывается при нажатии на кнопку [Parameters] в форме "Bank Production Parameters" (Full → Configuration Setup → Card Production Setup → Bank Production Parameters). В форме "Options for <...>" необходимо определить следующие параметры (в поле *Option* выбрать из списка наименование параметра, а в поле *Value* указать значение):

- "МС ОВКМ КМС ID" – полученный от платежной системы идентификатор центра управления криптографическими ключами (КМС, Key Management Centre). Представляет собой двузначное число. Значение может быть определено также с помощью параметра пайпа "[МС КМС ID](#)" (см. "Параметры пайпа "МС ОВКМ Export"); при этом значение, определенное в форме "Options for <...>", будет иметь более высокий приоритет.
- "МС ОВКМ Member ID" – уникальный идентификатор эмитента в центре управления криптографическими ключами Mastercard КМС. Представляет собой десятизначное число. Значение может быть определено также с помощью параметра пайпа "[МС КМС MEM ID](#)" (см. "Параметры пайпа "МС ОВКМ Export"); при этом значение, определенное в форме "Options for <...>", будет иметь более высокий приоритет.
- "МС ОВКМ Key Set Ref. М" – уникальный идентификационный номер набора ключей для карт с магнитной полосой ("PVK", "CVK1" и "CVK2") и бесконтактных карт "IMK<sub>CVCS</sub>". Представляет собой четырехзначное число. Данный идентификатор необходимо менять каждый раз при выгрузке нового набора ключей. Значение может быть определено также с помощью параметра пайпа "[KEY\\_SET\\_REF](#)" (см. "Параметры пайпа "МС ОВКМ Export"); при этом значение, определенное в форме "Options for <...>", будет иметь более высокий приоритет.
- "МС ОВКМ Key Set Ref. Е" – уникальный идентификационный номер ключа для смарт-карт ("AAVK"). Представляет собой четырехзначное число. Данный идентификатор необходимо менять каждый раз при выгрузке нового ключа. В случае если параметр "МС ОВКМ Key Set Ref. Е" не указан, для выгрузки ключей смарт-карт будет использован параметр "МС ОВКМ Key Set Ref. М".
- "МС ОВКМ Key Set Ref. Р" – уникальный идентификационный номер ключа для смарт-карт ("IMK<sub>CVCS</sub>"). Представляет собой четырехзначное число. Данный идентификатор необходимо менять каждый раз при выгрузке нового ключа. В случае если параметр "МС ОВКМ Key Set Ref. Р" не указан, для выгрузки ключей смарт-карт будет использован параметр "МС ОВКМ Key Set Ref. М".
- "МС ОВКМ Key Set Ref. S" – уникальный идентификационный номер ключа для смарт-карт ("IMK<sub>ac</sub>"). Представляет собой четырехзначное число. Данный идентификатор необходимо менять каждый раз при выгрузке нового ключа. В случае если параметр "МС ОВКМ Key Set Ref. S" не указан, для выгрузки ключей смарт-карт будет использован параметр "МС ОВКМ Key Set Ref. М".



- "MC OBKM AAVK Index" – уникальный идентификационный номер ключа "AAVK". Представляет собой шестизначное число. Значение может быть определено также с помощью параметра пайпа "[AAVK INDEX](#)" (см. "Параметры пайпа "MC OBKM Export"); при этом значение, определенное в форме "Options for <...>", будет иметь более высокий приоритет.

Для того чтобы выгрузить ключи в платежную систему Mastercard, необходимо в форме "Bank Production Parameters" (Full → Configuration Setup → Card Production Setup → Bank Production Parameters) нажать на кнопку [Parameters]. В открывшейся форме "Parameters for <...>" следует выбрать требуемые параметры производства, содержащие выгружаемые ключи, нажать на кнопку [Manage], а затем выбрать в контекстном меню пункт "MC OBKM". В результате на экране будет представлена форма "MC OBKM Mode" (см. Рис. 3).

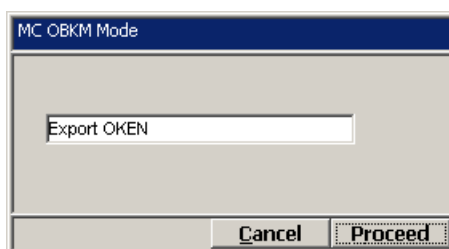


Рис. 3. Выбор режима выгрузки ключей

Существуют следующие режимы выгрузки ключей:

- "Export Chip Keys" – выгрузка ключа смарт-карты ("IMK<sub>ac</sub>").
- "Export Mag Stripe Keys (MC PVV)" – выгрузка ключей карт с магнитной полосой ("CVK1", "CVK2" и "PVK").
- "Export OKEN" – выгрузка ключа "OKEN" (Network Key), используемого для шифрования PIN-блока.
- "Export PayPass MagStripe CVC3 Validation Key" – выгрузка ключа "IMK<sub>CVC3</sub>", используемого для бесконтактных карт.
- "Export SecureCode AAV Validation Key" – выгрузка ключа "AAVK", используемого при обмене данными по протоколу 3-D Secure.

Выгрузка должна осуществляться последовательно: сначала необходимо выбрать пункт "Export OKEN", затем "Export Mag Stripe Keys (MC PVV)", а затем "Export Chip Keys". С помощью параметра пайпа "[OUTPUT DIRECTORY](#)" можно указать каталог исходящих файлов. В случае если параметр не определен, во время каждого запуска пайпа (выбора режима выгрузки) пользователю будет предложено выбрать каталог, в который следует поместить соответствующий файл.

Выгрузка ключей осуществляется пайпом "MC OBKM Export", параметры которого представлены в разделе "Параметры пайпа "MC OBKM Export".



Перед выгрузкой криптографических ключей следует убедиться, что для данной рабочей станции установлено соединение с криптографическим устройством (HSM). Процесс регистрации

криптографического устройства в системе WAY4 описан в разделе "Настройка параметров соединения рабочей станции с криптографическим устройством" документа "Настройка параметров системы WAY4 для производства карт с магнитной полосой".

Три сформированных в результате выгрузки файла необходимо отправить в платежную систему Mastercard.

## Параметры пайпа "МС OBKM Export"

Параметры пайпа "МС OBKM Export" представлены в Табл. 1.

Табл. 1. Параметры пайпа "МС OBKM Export"

Параметр	Значения	Описание параметра
AAVK_INDEX	Шестизначное число	Уникальный идентификационный номер ключа "AAVK". Формат идентификатора определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set". Значение параметра по умолчанию – "008001".
OUTPUT_DIRECTORY		Каталог исходящих файлов. В случае если параметр не задан, во время запуска пайпа пользователю будет предложено выбрать каталог, в который будет помещен файл.
STORAGE_FORM		Способ хранения ключа. Определяется типом криптографического устройства (HSM): "HH" – используется криптографическое устройства производства компании Thales; "WH" – используется криптографическое устройства производства компании SafeNet. Значение по умолчанию – "HH".
MC_KMC_MEM_ID	Десятизначное число	Уникальный идентификатор эмитента в центре управления криптографическими ключами Mastercard KMC. Значение может быть переопределено с помощью дополнительного параметра "МС OBKM Member ID" (см. "Выгрузка ключей смарт-карт и карт с магнитной полосой").
MC_KMC_ID	Двузначное число	Полученный от платежной системы идентификатор центра управления криптографическими ключами (KMC, Key Management Centre). Значение может быть переопределено с помощью дополнительного параметра "МС OBKM KMC ID" (см. "Выгрузка ключей смарт-карт и карт с магнитной полосой").

Параметр	Значения	Описание параметра
MODE		Параметр, определяющий режим выгрузки ключей. Возможные значения: С – выгрузка ключа смарт-карты ("IMK <sub>ac</sub> "); D – выгрузка ключа "IMK <sub>CVK3</sub> ", используемого для бесконтактных карт; M – выгрузка ключей карт с магнитной полосой ("CVK1", "CVK2" и "PVK"); O – выгрузка ключа "OKEN" (Network Key), используемого для шифрования PIN-блока; S – выгрузка ключа "AAVK", используемого при обмене данными по протоколу 3-D Secure; @COMMAND_TEXT@ – выгрузка ключа, выбранного с помощью формы <a href="#">"MC OBKM Mode"</a> .
KEY_SET_REF	Четырехзначное число	Уникальный идентификационный номер набора ключей для карт с магнитной полосой или смарт-карт. Данный идентификатор необходимо менять каждый раз при выгрузке нового набора ключей. Значение может быть переопределено с помощью дополнительных параметров "MC OBKM Key Set Ref. M", "MC OBKM Key Set Ref. E", "MC OBKM Key Set Ref. P" или "MC OBKM Key Set Ref. S" (см. "Выгрузка ключей смарт-карт и карт с магнитной полосой").
EXTRA_CAVV_DATA	7 символов	Дополнительные параметры для ключа "AAVK". Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK1_DATA	11 символов	Дополнительные параметры для ключа "CVK1". Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK2_DATA	7 символов	Дополнительные параметры для ключа "CVK2". Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".
EXTRA_TCMK_DATA	104 символа	Дополнительные параметры для ключа "IMK <sub>ac</sub> " (TC Master Key). Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".
EXTRA_PVK_DATA	40 символов	Дополнительные параметры для ключа "PVK". Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".
EXTRA_CVK3_DATA	82 символа	Дополнительные параметры для ключа "IMK <sub>CVK3</sub> ". Формат параметров определяется платежной системой и представлен в документе "On-behalf Key Management (OBKM) Document Set".

Параметр	Значения	Описание параметра
OKEN_ROLE	"D" / "I"	Параметр определяет назначение ключа "OKEN" (Network Key): "D" – ключ будет использоваться для шифрования/дешифрования PIN-блока; "I" – ключ будет использоваться для шифрования/дешифрования сессионных ключей. Значение по умолчанию – "D".
SM_ID		Наименование зарегистрированного в системе криптографического устройства (HSM), используемого выгрузки ключей. Список зарегистрированных устройств доступен в форме "Security Device" (Full → Configuration Setup → Card Production Setup → Security Device).
EXPORT_PVK	Y/N	Флажок, при установке которого (значение "N") в платежную систему не будет выгружаться ключ "PVK". Значение по умолчанию – "Y" ("PVK" выгружается).
EXPORT_CVK1	Y/N	Флажок, при установке которого (значение "N") в платежную систему не будет выгружаться ключ "CVK1". Значение по умолчанию – "Y" ("CVK1" выгружается).
EXPORT_CVK2	Y/N	Флажок, при установке которого (значение "Y") в платежную систему будет выгружаться ключ "CVK2". Значение по умолчанию – "N" ("CVK2" не выгружается). Следует иметь в виду, что сервис Mastercard OBKM не осуществляет проверку величины "CVC2"; ключ "CVK2" требуется только в случае, если эмитент пользуется сервисом Mastercard Emergency Card Replacement (ECR).