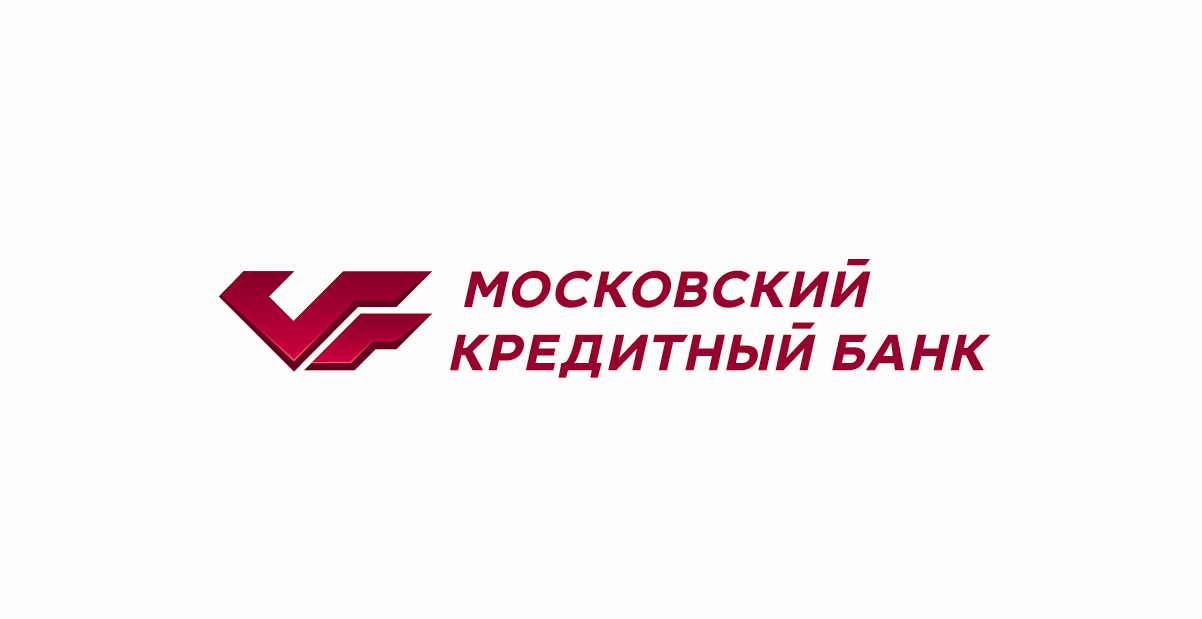
****

***Руководство администратора***

***по работе с сервисом***

***«Электронная Коммерция»***

***МОСКОВСКОГО КРЕДИТНОГО БАНКА***

**консультации по юридическим вопросам:**

**Ульянова Юлия** [**Ulyanovayu@mkb.ru**](mailto:Ulyanovayu@mkb.ru) **,** 8 (495) 797-42-22, доб. 6716

**Левина Дарья** [**DLevina@mkb.ru**](mailto:DLevina@mkb.ru) **,** 8 (495) 797-42-22, доб. 6602

**Парамонов Александр** [**Paramonov@mkb.ru**](mailto:Paramonov@mkb.ru) **,** 8 (495) 797-42-22, доб. 6779

**консультации по техническим вопросам:**

8 (925) 082-22-51 (круглосуточно)

8 (926) 996-54-72

8 (495) 797-42-22, доб.6997, 6816

[**pos@mkb.ru**](mailto:pos@mkb.ru)

Оглавление

[1. Основные положения 3](#_Toc474226641)

[1) Требования к сайту 3](#_Toc474226642)

[2) Рекомендации по размещению правил оплаты в интернет-магазине 3](#_Toc474226643)

[2. Основной запрос на оплату: формирование страницы оплаты (MPI) 5](#_Toc474226644)

[1) Поля, используемые для работы с сервером 7](#_Toc474226645)

[2) Пример формы для формирования запроса 9](#_Toc474226646)

[3) Взаимодействие клиента с сервисом 9](#_Toc474226647)

[4) Формирование поля signature 9](#_Toc474226648)

[5) Результат обработки транзакции (ответ от сервера) 10](#_Toc474226649)

[6) Пример ответа от сервера MPI 12](#_Toc474226650)

[7) Передача и обработка поля resp\_url 12](#_Toc474226651)

[8) Передача и обработка поля directposturl 13](#_Toc474226652)

[9) Общий пример приёма пакета ответа на Java 13](#_Toc474226653)

[10) Пример содержимого в ответе от сервера 13](#_Toc474226654)

[11) Тестовая карта 14](#_Toc474226655)

[3. Сервис «EXPRESS PAYMENT» 15](#_Toc474226656)

[1) Демоверсия 15](#_Toc474226657)

[2) Начало работы 15](#_Toc474226658)

[3) Формирование заказа 17](#_Toc474226659)

[4) Проверка статуса платежа 17](#_Toc474226660)

[4. Дополнительный запрос: FinancialLink 18](#_Toc474226661)

[1) Формирование запроса на сервер 18](#_Toc474226662)

[2) Формирование поля Signature 19](#_Toc474226663)

[3) Результат обработки транзакции (ответ от сервера) 19](#_Toc474226664)

[4) Возможные ответы от сервера в Financial Link 21](#_Toc474226665)

[5) Адрес боевого сервера 22](#_Toc474226666)

[5. Дополнительный запрос: статус операции 23](#_Toc474226667)

[1) Формирование HTTPS POST запроса на сервер 23](#_Toc474226668)

[2) Пример формы для отправки запроса на сервер 23](#_Toc474226669)

[3) Пример ответа на запрос статуса заказа 24](#_Toc474226670)

[4) Возможные статусы 24](#_Toc474226671)

[6. Дополнительное описание в транзакции 26](#_Toc474226672)

[7. Вложения 27](#_Toc474226673)

[1) Логотип Visa 27](#_Toc474226674)

[2) Логотип Mastercard 27](#_Toc474226675)

[8. Коды ответов от сервера (Response, Reason) 28](#_Toc474226676)

[1) Оригинальные коды ответов, которые согласованы с Международными Платёжными Системами 28](#_Toc474226677)

[2) Расшифровки и описания наиболее встречающихся кодов ответов при работе с основной платёжной страницей MPI и сервисом Express Payment 29](#_Toc474226678)

# Основные положения

Данная инструкция описывает методы и типы подключения электронной коммерции МОСКОВСКОГО КРЕДИТНОГО БАНКА для оплаты картами на сайтах организаций (далее сайт).

Перед полноценным подключением сайту **обязательно** необходимо протестировать выбранную схему с использованием указанных в соответствующем пункте настроек.

После тестирования необходимо обратиться к своему менеджеру в Банке для получения «боевых» настроек.

## Требования к сайту

Технические требования:

1. Страница, с которой производится переход на страницу оплаты Банка, должна быть защищена SSL (ссылка должна начинаться HTTPS://...).\*
2. Не должно быть посторонних включений – все элементы страницы должны размещаться на том же ресурсе. Исключение – счётчики, рекламные объявления и активное содержимое для обратной связи (звонок с сайта, чаты, информеры). Но все обязательно с известных, проверенных площадок.

**\* SSL сертификат должен быть с меткой доверия (соответствие домену), т.е. на сайте должно быть уведомление «соединение защищено». Подойдет сертификат с проверкой только доменного имени от любого лицензированного центра сертификации.**

## Рекомендации по размещению правил оплаты в интернет-магазине

**Правила оплаты в Интернет-магазине.**

К оплате принимаются платежные карты: VISA Inc, MasterCard WorldWide.

Для оплаты товара банковской картой при оформлении заказа в интернет-магазине выберите Способ оплаты: банковской картой.

При оплате заказа банковской картой, обработка платежа происходит на авторизационной странице ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК», где Вам необходимо ввести данные Вашей банковской карты:

1. тип карты
2. номер карты,
3. срок действия карты (указан на лицевой стороне карты)
4. Имя держателя карты (латинскими буквами, точно также как указано на карте)
5. CVC2/CVV2 код

Далее нажать на кнопку «ОПЛАТИТЬ».

Для дополнительной аутентификации держателя карты используется протокол 3D Secure. Если Ваш Банк поддерживает данную технологию, Вы будете перенаправлены на сервер Вашего Банка для дополнительной идентификации. Информацию о правилах и методах дополнительной идентификации уточняйте в Банке, выдавшем Вам банковскую карту.

Безопасность обработки интернет-платежей через ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» гарантирована международным сертификатом безопасности PCI DSS.

Передача информации происходит с применением технологии шифрования SSL.

**Советы и рекомендации по необходимым мерам безопасности проведения платежей с использованием банковской карты:**

1. берегите свои пластиковые карты так же, как бережете наличные деньги. Не забывайте их в машине, ресторане, магазине и т.д.
2. никогда не передавайте номер своей кредитной карты по телефону каким-либо лицам или компаниям
3. всегда имейте под рукой номер телефона для экстренной связи с банком, выпустившим вашу карту, и в случае ее утраты немедленно свяжитесь с банком
4. вводите реквизиты карты только при совершении покупки. Никогда не указывайте их по каким-то другим причинам.
5. проверьте, установлено ли защищенное SSL-соединение: адрес в адресной строке должен начинаться с https:// и в правом нижнем углу браузера должно появиться изображение замка.

# Основной запрос на оплату: формирование страницы оплаты (MPI)

**MPI – платёжная страница для ввода персональных данных карты.**

Данная страница обеспечивает возможность проведения операции **холдирования\*** средств, с использованием защищённого web-интерфейса Банка.

В общих чертах процедура работы со страницей выглядит следующим образом:

1. Сайт-продавец отправляет запрос на сервер Банка и переводит клиента на защищённую страницу оплаты.

Для проведения операции необходимо инициировать **HTTPS POST/GET** запрос с передачей необходимых полей (список которых приведён ниже, в [**первом**](#_Поля,_используемые_для_1) пункте данного раздела) и с переходом по одному из нижеуказанных адресов:

Тестовый сервер: [**https://mpi.mkb.ru:9443/MPI\_payment/**](https://mpi.mkb.ru:9443/MPI_payment/)

«Боевой» сервер: [**https://mpi.mkb.ru/MPI\_payment/**](https://mpi.mkb.ru/MPI_payment/)

**Рекомендуется отправка запроса методом GET.**

**Пример «готового» запроса на тестовый сервер методом GET:**

[**https://mpi.mkb.ru:9443/MPI\_payment/?site\_link=test-api.html&mid=500000000011692&oid=12341236&aid=443222&amount=000000010000&merchant\_mail=test@mkb.ru&signature=coo0re7VuwMFnY%2Bsc4EmhWEvejc%3D&client\_mail=pos@mkb.ru&resp\_url=online.mkb.ru**](https://mpi.mkb.ru:9443/MPI_payment/?site_link=test-api.html&mid=500000000011692&oid=12341236&aid=443222&amount=000000010000&merchant_mail=test@mkb.ru&signature=coo0re7VuwMFnY%2Bsc4EmhWEvejc%3D&client_mail=pos@mkb.ru&resp_url=online.mkb.ru)

1. Клиент указывает персональные данные на защищённой странице Банка.
   1. Если карта, которой оплачивает клиент, поддерживает технологию 3D-Secure, то сервер перед проведением холдирования автоматически переводит клиента на страницу Банка, выпустившего карту клиента, для ввода данного кода.
2. После холдирования сервер передаёт данные о транзакции на сайт организации (при указании соответствующих полей, см. перечень необязательных полей в таблице ниже), а также отправляет чек на почту клиенту (если почта была указана).
   1. Также информацию о заказах можно узнать в личном кабинете или с помощью отправки дополнительных запросов (см. [**раздел 4**](#_Дополнительный_запрос:_статус)).

**\*** первым этапом оплаты является именно холдирование средств (не снятие средств), т.е. деньги **не будут** зачислены на счёт организации до тех пор, пока операция не будет подтверждена.

Если подтверждение не было произведено в течение **семи календарных дней**, то средства автоматически разблокируются.

По стандартной настройке банка установлено, что все операции автоматически подтверждаются сразу после холдирования.

**Если Вам требуется подтверждать операции вручную (например, в личном кабинете или по API из** [**раздела 3**](#_Дополнительный_запрос:_FinancialLin)**), то необходимо сообщить об этом банковскому менеджеру, чтобы Вам была установлена данная настройка.**

**Внимание!**

**Страница сайта (не обязательно весь сайт, достаточно только конкретной директории, например, «корзины покупателя»), с которой клиент будет перенаправляться на страницу оплаты (MPI), должна быть защищена валидным сертификатом SSL!**

Подойдёт любой сертификат с проверкой доменного имени (на сайте должен быть значок «соединение защищено»).

**Также необходимо обратить внимание на следующие моменты:**

1. Все параметры и ссылки, указанные в данной инструкции, являются тестовыми, т.е. оплата нашими тестовыми картами на сайте будет проходить, но деньги на счет Вашей Организации зачислены не будут.

2. Значение поля **oid** для каждого заказа должно быть уникальным в рамках **одного номера продавца** (далее **mid**). Если на Вашем сайте в зависимости от региона используются разные юр. лица с разными **mid** соответственно, то для разных **mid** номер заказа может повторяться. Сервер будет отвечать ошибкой на запросы, содержащие повторяющиеся **oid** в рамках одного **mid**.

Если Вам требуется провести несколько оплат в рамках одного заказа, то самым простым способом будет использование префикса/суффикса для номера заказа. Т.е. на примере заказа oid=12345

Первая оплата будет oid=12345-1

Вторая =12345-2

При ответе от нашего сервера последние 2 символа можно «опускать» (например, ограничить по длине или до знака препинания) и записывать себе только сам номер заказа.

## Поля, используемые для работы с сервером

**РЕГИСТР БУКВ В НАЗВАНИЯХ ПОЛЕЙ ДОЛЖЕН СОБЛЮДАТЬСЯ!**

**Перечень обязательных полей (без которых сервер будет возвращать ошибку):**

|  |  |  |
| --- | --- | --- |
| Название поля | Описание поля | Необходимые значения и данные для тестирования |
| mid | Идентификатор Мерчанта (магазина).  Статичное значение. | 500000000011692 (тестовый)  **Индивидуальный «боевой» присваивается после заключения договора.** |
| aid | Идентификатор Банка-Эквайера.  Статичное значение. Для теста и боя используется одинаковый номер. | 443222 |
| amount | Сумма (в копейках). | Записывается как 12-тизначное число, дополняемое нулями с левой стороны.  Например: 000000155020 = 1,550р. 20к. |
| oid | Номер заказа на сервере (до 150 символов).  Допускаются латинские буквы, цифры и следующие клавиатурные символы ,./\|<>`~!@$^\*()-\_=+[]{};:  **При использовании символов в данном поле, рекомендуется перед отправкой кодировать значения в URL Encode.** | Можно указывать различные значения, например:  oid=dogovor-010116-1  oid=zakaz12  oid=#102030  oid=123456-3  **Должен быть уникальным для каждой успешной транзакции!**  **Если транзакция завершилась любым Response-кодом, кроме 1 (единицы), то допускается отправка данного oid повторно.** |
| signature | Цифровая подпись транзакции. | Метод генерации описан ниже в четвёртом пункте данного раздела. |

**Перечень необязательных полей (поля для кастомизации):**

|  |  |  |
| --- | --- | --- |
| Название поля | Описание поля | Необходимые значения и данные для тестирования |
| resp\_url | Поле для получения ответа от сервера, **отправляемого на указанный web-сервер**.  Нужно указывать доменное имя или IP сервера.  Подробнее в пункте [семь](#_Передача_и_обработка) данного раздела. | Доменное имя или IP сервера.  Ответ передаётся **TCP пакетом (не POST и не GET!)**  Например:  mkb.ru или 11.22.33.44 |
| directposturl | Поле для получения ответа от сервера, **отправляемого на указанную директорию сервера**.  Нужно указывать полную ссылку на страницу приёма ответа.  Подробнее в пункте [восемь](#_Передача_и_обработка_1) данного раздела.  **Ответ (callback) отсылается в момент вывода чека конечному клиенту (клиенту организации).**  Если сервер МКБ не получил 200-е HTTP сообщение от URL, указанного в запросе, на первый отправленный ответ, то сервер МКБ делает ещё 6 попыток отправки:   1. Через 1 минуту 2. Через 15 минут 3. Через 60 минут 4. Через 4 часа 5. Через 8 часов 6. Через 24 часа   **Если нет 200-го сообщения после отправки через 24 часа, то попыток больше не делается.** | URL страницы сайта, на которую будет передаваться **ответ методом POST**.  **На странице обязательно должен быть валидный SSL сертификат.** |
| redirect\_url | URL для перенаправления клиента после оплаты.  Подробнее о «схеме» перенаправлений ниже в пункте [три](#_Взаимодействие_клиента_с) данного раздела.  Перенаправление производится для всех транзакций, независимо от результата (успешная/неуспешная). | URL, на который после оплаты (после страницы с чеком) будет перенаправлен клиент.  **Ссылка должна быть с указанием протокола (http/https), например, http://www.mkb.ru !** |
| client\_mail | E-mail клиента.  Если данное поле передавать в запросе, то соответствующее поле на странице оплаты будет заполнено автоматически (можно передавать email зарегистрированного на сайте пользователя – конечным клиентам это удобно). | Электронный почтовый адрес клиента.  **Даже при передаче поля, клиенту доступно изменение email на странице оплаты (непосредственно перед оплатой) и чек будет отправлен на изменённую почту!** |
| site\_link | URL сайта.  **Доменное имя** данного URL будет отображено на странице оплаты, а также непосредственно на чеке. | URL сайта, в пользу которого производится платёж.  **Ссылка должна быть с указанием протокола (http/https), например, http://www.mkb.ru !** |
| merchant\_mail | E-mail оператора/магазина/администратора. | Электронный почтовый адрес, на который Вам будут приходить уведомления о транзакциях.  **Чеки абсолютно идентичные чекам клиентов.** |
| cancel\_link | URL, на который будет перенаправлен клиент в случае нажатия на первой странице кнопки «Отмена». | При наличии поля клиент будет перенаправляться на данный URL при нажатии «отмена».  Если поля нет, то логика аналогичная **redirect\_url** |

## Пример формы для формирования запроса

<form id='FrmHtmlCheckout' name='FrmHtmlCheckout' action='https://mpi.mkb.ru:9443/MPI\_payment/' method='post'>

<input id='mid' type='hidden' value='500000000011692' name='mid' >

<input id='aid' type='hidden' value='443222' name='aid' >

<input id='amount' type='hidden' value='000000000100' name='amount'>

<input id='oid' type='hidden' value='TESTOVIY-ZAKAZ' name='oid' >

<input id='signature' type='hidden' value='xLVDcdENzPdGpzkIXM/6T1xIYoY=' name='signature'>

<input id='redirect\_url' type='hidden' value='www.mkb.ru' name='redirect\_url'>

<input id='directposturl' type='hidden' value='www.mkb.ru' name='directposturl'>

<input id='merchant\_mail' type='hidden' value='pos@mkb.ru' name='merchant\_mail'>

<input id='resp\_url' type='hidden' value=’mkb.ru’ name='resp\_url'>

<input type="submit" value="Oplata">

</form>

**Для проверки работы на тестовом сервере желательно использовать GET (будут видны поля), но на бою лучше использовать POST.**

## Взаимодействие клиента с сервисом

1. На защищённой SSL странице пользователь вводит данные, необходимые для оплаты: номер карты, срок действия карты, фамилию и имя владельца карты, код CVV2.

**Данные для формирования запроса приведены в таблице выше. Персональные данные тестовой карты приведены в** [**одиннадцатом**](#_Тестовая_карта) **пункте.**

1. После заполнения и проверки, данные отправляются на сервер банка для обработки.
2. Клиент получает ответ о состоянии платежа.
3. Формируется и отправляется ответ на сайт.
4. **Далее происходит редирект на ссылку из поля redirect\_url.**

**Если поле не задано, то редирект происходит на URL из поля site\_link.**

**Если и site\_link не задано, то редирект происходит на** [**www.mkb.ru**](http://www.mkb.ru)

## Формирование поля signature

**Пароль, необходимый для формирования поля signature во время тестирования** - SD13ag03

Для формирования цифровой подписи необходимо посчитать хэш SHA-1 от строки, в которую входят значения следующих параметров:

**Password** & **MerchantID (mid)** & **AcquirerID (aid)** & **OrderID (oid)** & **Amount** & **Валюта**

Например:

**SD13ag03500000000011692443222ORGANIZACIYA-1000000010000643**

Считаем SHA-1, получаем хэш в шестнадцатеричной кодировке:

**babb1188407a81d2a6fca85fed8cb2bbe8868488**

Кодируем полученное значение в BASE64:

**ursRiEB6gdKm/Khf7Yyyu+iGhIg=**

Например, в PHP, чтобы получить signature, необходимо выполнить следующие операции над строкой:

**base64\_encode(hex2bin(sha1('SD13ag03500000000011692443222ORGANIZACIYA-1000000010000643')))**

**Настоятельно рекомендуется перед первой отправкой запроса на сервер проверить формирование подписи через ресурсы, доступные в сети Интернет или через нашу страницу:**

[**https://mpi.mkb.ru:9443/MPI\_payment/Signature.jsp**](https://mpi.mkb.ru:9443/MPI_payment/Signature.jsp)

## Результат обработки транзакции (ответ от сервера)

После переключения клиента на страницу MPI с чеком, на сайт автоматически передаётся ответ от сервиса. В следующем пункте описан ответ и как его можно получить.

Самый главный параметр в ответе – это Response Code (Код ответа):

|  |  |
| --- | --- |
| **Response Code** | **Описание** |
| 1 | Одобрено |
| 2 | Отклонено |
| 3 | Ошибка |

В зависимости от него сообщение может включать в себя дополнительные параметры:

1. Response Code = 1

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| Signature | Цифровая подпись ответа |
| SignatureMethod | Метод шифрование |
| MerID | ID магазина **(mid)** |
| AcqID | ID банка эквайера **(aid)** |
| OrderID | ID заказа **(oid)** |
| amt | сумма |
| PaddedCardNo | Маскированный номер карты |
| ResponseCode | Статус операции |
| ReasonCode | Причина прохождения/отклонения |
| AuthCode | Код авторизации |
| ReferenceNo | Номер ссылки RRN |
| ReasonCodeDesc | Расшифровка ответа (одобренно/ отказано /какая ошибка ) |
| fio | ФИО клиента, которую он указал на платёжной странице |

1. Response Code = 2

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| ResponseCode | Код ответа |
| ReasonCode | Код причины ответа |
| ReasonCodeDesc | Описание причины ответа |
| MerID | ID магазина |
| AcqID | ID банка эквайера |
| OrderID | ID заказа |

1. Response Code = 3

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| ResponseCode | Код ответа |
| ReasonCode | Код причины ответа |
| ReasonCodeDes | Описание причины ответа |
| OrderID | ID заказа |

По операциям, проведённым через процессинг, т.е. которые имеют конкретный ответ от Международной Платёжной Системы и/или Банка-Эмитента, сервер в ответе добавляет поле signature. Принцип ее формирования аналогичен формированию в запросе от сайта интернет-магазина.

В подпись включаются следующие поля:

**Password** & **MerchantID** & **AcquirerID** & **OrderID** & **ResponseCode** & **ReasonCode**

Например:

**SD13ag03500000000011692443222ORGANIZACIYA-111**

Считаем SHA-1, получаем хэш в шестнадцатеричной кодировке:

**3f66b9a21bb36ce3f0509cd36087eb1fa443f98f**

Кодируем полученное значение в BASE64:

**P2a5ohuzbOPwUJzTYIfrH6RD+Y8=**

**Для окончательного завершения тестирования, подпись необходимо проверить, т.е. рассчитать ее на основании Ваших параметров и сверить с тем, что прислал сервер.**

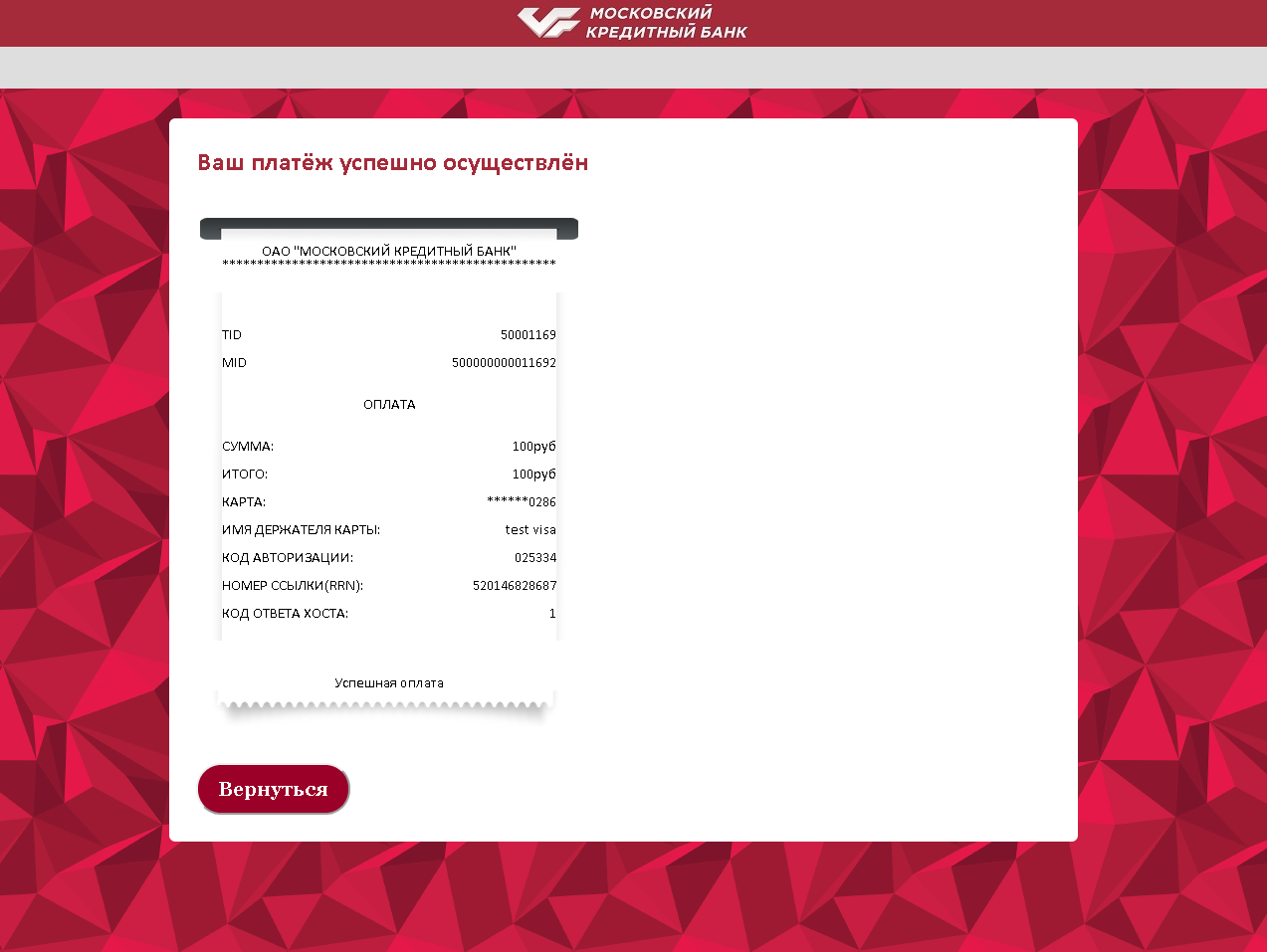
**По ошибкам, которыми отвечает сам сервер (например, «неверно сформированная подпись» или «неверный mid»), сервер signature не присваивает.**

## Пример ответа от сервера MPI

В момент, когда клиент переключается на страницу с чеком, сервис MPI отправляет чеки на почту, а также отправляет пакет с информацией об оплате по одному из полей: **resp\_url** или **directrespurl.**

**Ответ отправляется с IP: 191.191.76.137**

Ниже пример страницы с чеком.

****

## Передача и обработка поля resp\_url

Если Вы передаёте поле resp\_url , то в обработке на сервере Вам необходимо постоянно «слушать» соединение.

Передавать в данное поле необходимо либо IP адрес сервера, либо адрес основной страницы (без указания протокола).

Т.е. если у Вас адрес, например, **https://online.mkb.ru/secure/login.aspx?ReturnUrl=%2fsecure%2f** , то передавать надо просто **resp\_url=online.mkb.ru**

От сервиса MPI отправляется стандартный TCP пакет, который **приходит на порт 443 указанного сервера**.

Для его приёма необходимо «слушать» 443 порт и в момент, когда приходит пакет – принимать данные и далее обрабатывать их.

## Передача и обработка поля directposturl

Если Вы передаёте поле directposturl , то в обработке на сервере Вам необходимо постоянно «слушать» соединение.

Передавать в данное поле необходимо полный адрес основной страницы (с указанием протокола).

Например, **directposturl=https://online.mkb.ru/secure/login.aspx?ReturnUrl**

От сервиса MPI отправляется пакет методом POST по порту 443.

Для его приёма необходимо «слушать» 443 порт и в момент, когда приходит пакет – принимать данные и далее обрабатывать их.

## Общий пример приёма пакета ответа на Java

package listener;

import java.net.\*;

import java.io.\*;

public class Listener {

/\*\*

\* @param args the command line arguments

\*/

public static void main(String[] args) {

int port = 443;

try {

ServerSocket ss = new ServerSocket(port);

System.out.println("Waiting for a client...");

Socket socket = ss.accept();

System.out.println("Got a client :) ... Finally, someone saw me through all the cover!");

System.out.println();

InputStream sin = socket.getInputStream();

OutputStream sout = socket.getOutputStream();

DataInputStream in = new DataInputStream(sin);

DataOutputStream out = new DataOutputStream(sout);

String line = null;

while(true) {

line = in.readUTF();

System.out.println("The dumb client just sent me this line : " + line);

System.out.println("I'm sending it back...");

out.writeUTF(line);

out.flush();

System.out.println("Waiting for the next line...");

System.out.println();

break;

}

} catch(Exception x) { x.printStackTrace(); }

}

}

## Пример содержимого в ответе от сервера

Signature=UMdWfapi3lCghp3V4DzptADa3Qg=&SignatureMethod=SHA1&MerID=600000000001834&AcqID=443222&OrderID=843631&amt=000000120000&PaddedCardNo=XXXXXXXXXXXX4089&ResponseCode=1&ReasonCode=1&AuthCode=594523&ReferenceNo=610915982302&ReasonCodeDesc=Transaction is approved.&

## Тестовая карта

Ниже приведены параметры карты, с помощью которой Вы можете протестировать все необходимые Вам операции.

**Платёжная система:** Visa

**Номер карты:** 4037 восемь ноль ноль ноль четыре ноль один семь 0245

**Срок действия:** 06/17

**ФИО плательщика (при оплате на тестовом сервере можно указать хоть «Q W», но обязательно минимум в два слова через пробел):** TEST VISA MAG 1

**Защитный код CVV:** 860

# Сервис «EXPRESS PAYMENT»

Данная инструкция описывает методы работы с электронной коммерцией МОСКОВСКОГО КРЕДИТНОГО БАНКА с использованием сервиса «EXPRESS PAYMENT».

Сервис «EXPRESS PAYMENT» предоставляет организации возможность приёма оплат по картам без непосредственного взаимодействия с сайтом организации.

Для подключения данного сервиса необходимо обратиться в Банк (контакты указаны на титульной странице).

В заявке важно указать электронную почту организации и сотовые телефоны сотрудников, которые будут пользоваться сервисом.

После заключения договора организация получает по электронной почте параметры для работы с сервисом - персональные логин и пароль для каждого пользователя.

К каждому логину будет привязан номер телефона сотрудника, который будет пользоваться сервисом. На данный номер телефона будет присылаться по СМС защитный код, который необходимо будет ввести в момент входа в личный кабинет.

Более подробно описано на сайте [www.mkb.ru](http://www.mkb.ru) ([конкретнее](https://mkb.ru/facility/business/acquiring/express_payment/))

В случае необходимости создания нового пользователя, изменения номера телефона у уже существующих пользователей и в других подобных ситуациях, следует обращаться по электронной почте на [pos@mkb.ru](mailto:pos@mkb.ru)

## Демоверсия

Ссылка на тестовый сервис: <https://mpi.mkb.ru:9443/ep/>

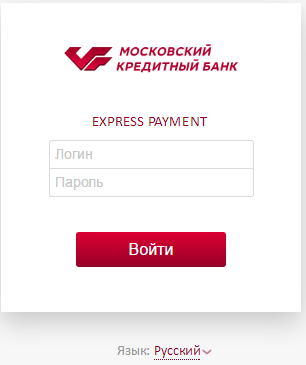
Логин: test

Пароль: test

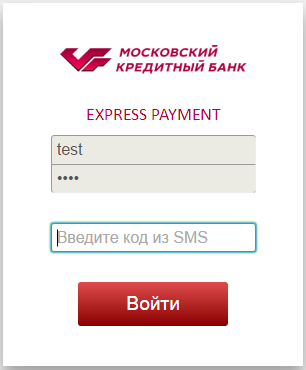
Код из СМС: 00000

## Начало работы

Ссылка на «боевой» сервис: <https://mpi.mkb.ru/ep/>

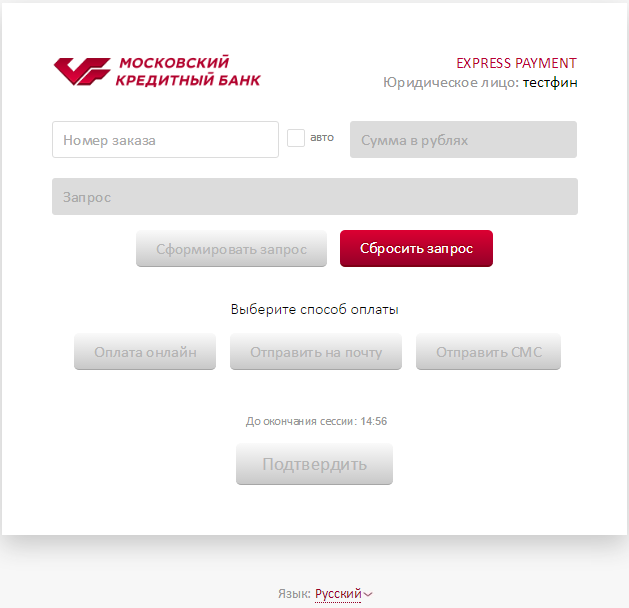


Для входа в сервис используйте выданные Вам логин и пароль. Если комбинация логина и пароля корректна, то Вам отобразиться поле для ввода кода из СМС.



Код отправляется отдельно для каждого логина на номер, указанный в заявке на подключение.

После ввода кода Вам отобразится основное меню сервиса.



## Формирование заказа

1. На основной странице сервиса укажите номер заказа

Если в Вашей организации отсутствует внутренний учёт номеров заказов, то активируйте галочку «авто» и система автоматически присвоит текущему заказу последовательный номер.

Допускается латиница, а также цифры и следующие символы:

,./\|<>`~!@#$%^\*()-\_=+[]{}‘“;:

1. Укажите сумму в рублях.
2. Нажмите «сформировать запрос». Станет активен выбор способа оплаты.
3. Выберите способ оплаты.

**Оплата онлайн:** Вы будете немедленно перенаправлены на страницу оплаты.

**Отправить на почту:** при активации данного пункта меню, Вам будет отображено поле для указания электронной почты клиента. На данную электронную почту клиенту будет автоматически отправлено письмо со ссылкой на оплату.

**Отправить СМС:** при активации данного пункта меню, Вам будет отображено поле для указания номера телефона клиента. На данный номер телефона клиенту будет автоматически отправлено сообщение со ссылкой на оплату.

## Проверка статуса платежа

После того как клиент оплатит заказ, на электронную почту, указанную в заявке на подключение, будет отправлена копия чека оплаты. Абсолютно такой же чек получит клиент, если указал на странице оплаты электронную почту.

Также проверить статус платежей можно в личном кабинете <https://office.mkb.ru/>

# Дополнительный запрос: FinancialLink

FinancialLink - метод проведения операций расхолдирования (Reverse), подтверждения списания (Capture) и возврата денежных средств по уже подтверждённой операции (Refund). Персональные данные карт не требуются.

Своего рода, данный линк – альтернатива личному кабинету office.mkb.ru , который Банк предоставляет Организации.

## Формирование запроса на сервер

Данные, которые направляются в запросе от интернет-магазина на сервер (Все поля являются обязательными!):

|  |  |  |
| --- | --- | --- |
| **Имя параметра** | **Значение** | **Описание** |
| MerID | 500000000003285 | ID магазина.  **В схеме MPI указывался как mid** |
| AcqID | 443222 | ID Банка эквайера.  **В схеме MPI указывался как aid** |
| PurchaseAmt | 000000017600 | Сумма оригинальной операции (12 символов).  В примере 176руб 00коп.  **В схеме MPI указывалась как amount** |
| PurchaseCurrency | 643 | ISO-код валюты заказа. |
| PurchaseCurrencyExponent | 2 | Кол-во знаков после запятой для суммы заказа. |
| OrderID | ORGANIZACIYA-1 (для тестирования рекомендуется использовать название компании и символ, чтобы миновать ошибку повторных номеров заказов). Допускаются латинские буквы, цифры и все стандартные клавиатурные символы ,./\|<>`~!@#$%^\*()-\_=+[]{}‘“;: кроме & | Номер заказа (должен быть уникальным для каждого заказа).  **В схеме MPI указывался как oid** |
| Signature | nFetcgHG16fyFTT7ctc5tMPmvIQ= | Цифровая подпись, необходимая для аутентификации магазина (формирование см. ниже).  **В схеме MPI указывалась как signature** |
| Action | Для подтверждения списания – Capture  Для отмены холдирования – Reverse  Для возврата подтверждённой операции – Refund | Тип функции. Для каждой функции необходимо отправлять своё значение. |
| AuthorizationNumber | 123456 | Код авторизации изначальной операции. Присутствует в ответе от сервера. Шесть символов. |
| Amount | 000000017600 | Проводимая сумма (12 символов). Сумма, на которую будет завершена оплата или произведены отмена/возврат.  **Для Capture и Reverse значение данного поля должно совпадать с полем PurchaseAmt !**  В примере 176руб 00коп |
| MerRespURL | https://yoursite.ru/form.php | URL, на который сервер возвращает результат транзакции. Страница **должна быть защищена сертификатом SSL** с меткой доверия (проводится только проверка соответствия домену). |
| Version | 1.0.0 | Версия на сервере. Значение статично. |
| SignatureMethod | SHA1 | Метод генерации подписи. Значение статично. |

Адрес тестового сервера, на который отправляются данные:

<https://ts-ecomweb-test.mcb.ru/SENTRY/PaymentGateway/Application/FinancialProcessing.aspx>

## Формирование поля Signature

***Принцип формирования подписи аналогичен стандартной оплате.***

Для формирования цифровой подписи, необходимо посчитать хэш SHA-1 от строки в которую входят значения следующиx параметров:

**Password** & **MerchantID** & **AcquirerID** & **OrderID** & **Purchase Amount** & **PurchaseCurrency**

Например:

**3G7Kgu3N500000000003285443222ORGANIZACIYA-1000000017600643**

Считаем SHA-1, получаем хэш в шестнадцатиричной кодировке:

**9c57ad7201c6d7a7f21534fb72d739b4c3e6bc84**

Кодируем полученное значение в BASE64:

**nFetcgHG16fyFTT7ctc5tMPmvIQ=**

Например в PHP, чтобы получить signature, необходимо выполнить следующе операции над строкой:

**base64\_encode(hex2bin(sha1('3G7Kgu3N500000000003285443222ORGANIZACIYA-1000000017600643')))**

**Настоятельно рекомендуется перед первой отправкой запроса на сервер проверить формирование подписи через ресурсы, доступные в сети Интернет или через нашу страницу:**

[**https://mpi.mkb.ru:9443/MPI\_payment/Signature.jsp**](https://mpi.mkb.ru:9443/MPI_payment/Signature.jsp)

## Результат обработки транзакции (ответ от сервера)

После обработки запроса, сервер возвращает ответ на адрес, указанный в поле MerRespURL.

Самый главный параметр в ответе – это Response Code (Код ответа):

|  |  |
| --- | --- |
| **Response Code** | **Описание** |
| 1 | Одобрено |
| 2 | Отклонено |
| 3 | Ошибка |

В зависимости от него сообщение может включать в себя дополнительные параметры:

1. Response Code = 1

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| Response Code | Код ответа |
| Reason Code | Код причины ответа |
| Reason Description | Описание причины ответа |
| Merchant Id | ID магазина |
| Acquirer Id | ID банка эквайера |
| Merchant Order Id | ID заказа |
| Signature | Цифровая подпись ответа |
| Reference Number | Номер ссылки RRN |
| Card Number (padded) | Маскированный номер карты |
| Authorization Code | Код авторизации |
| BillToToFirstName | Имя владельца карты |
| BillToLastName: | Фамилия владельца карты |

1. Response Code = 2

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| Response Code | Код ответа |
| Reason Code | Код причины ответа |
| Reason Description | Описание причины ответа |
| Merchant Id | ID магазина |
| Acquirer Id | ID банка эквайера |
| Merchant Order Id | ID заказа |
| BillToToFirstName | Имя владельца карты |
| BillToLastName: | Фамилия владельца карты |

1. Response Code = 3

|  |  |
| --- | --- |
| **Имя параметра** | **Описание** |
| Response Code | Код ответа |
| Reason Code | Код причины ответа |
| Reason Description | Описание причины ответа |
| Merchant Order Id | ID заказа |

Если транзакция одобрена (ResponseCode = 1), сервер подписывает ответ цифровой подписью. Принцип ее формирования аналогичен вышеописанному. В подпись включаются следующие поля:

**Password** & **MerchantID** & **AcquirerID** & **OrderID** & **ResponseCode** & **ReasonCode**

Например:

**3G7Kgu3N500000000003285443222ORGANIZACIYA-111**

Считаем SHA-1, получаем хэш в шестнадцатеричной кодировке:

**6bb6afbe78958b954cf9da57fb0af361500315ec**

Кодируем полученное значение в BASE64:

**a7avvniVi5VM+dpX+wrzYVADFew=**

**Для окончательного завершения тестирования, подпись необходимо проверить, т.е. рассчитать ее на основании Ваших параметров и сверить с тем, что прислал сервер.**

## Возможные ответы от сервера в Financial Link

Reverse:

1. Response Code = 1

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 1 | Успешная отмена |

1. Response Code = 3

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 24 | Информация по заказу не найдена |
| 38 | Сумма превышает оригинальную |
| 41 | Отмена уже произведена ранее |
| 51 | Отмена не доступна |

Capture:

1. Response Code = 1

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 17 | Успешное подтверждение |

1. Response Code = 3

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 11 | Списание уже подтверждено |
| 12 | Сумма превышает оригинальную |
| 24 | Информация по заказу не найдена |
| 27 | Частич. подтверждение не доступно |
| 57 | Транзакция была отменена ранее |
| 60 | Частичная сумма не поддерживается |
| 201 | Неверно заполнен Action |

Refund:

1. Response Code = 1

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 1 | Успешный возврат |

1. Response Code = 3

|  |  |
| --- | --- |
| **Reason Code** | **Описание** |
| 24 | Информация по заказу не найдена |
| 36 | Возврат не доступен |

## Адрес боевого сервера

Адрес сервера, на который отправляются данные:

<https://ts-ecomweb.mcb.ru/SENTRY/PaymentGateway/Application/FinancialProcessing.aspx>

# Дополнительный запрос: статус операции

Данный функционал позволяет запросить с сервера текущий статус проведения операции.

## Формирование HTTPS POST запроса на сервер

Для вызова операций необходимо:

1. Подготовить данные.
2. Инициировать HTTPS POST запрос к сервлету финансового процессинга:

[**https://mpi.mkb.ru:9443/finoperate/dogetorderstatusservlet**](https://mpi.mkb.ru:9443/finoperate/dogetorderstatusservlet)

**«На бою» используется порт 8443.**

1. Система обработает транзакцию и отправит в ответ результат.

**Данные для тестирования:**

Login = testfin

Password = d96a4c1

MerID = 500000000003285 / 500000000011692 / 500000000022152

Данные, которые направляются в запросе от интернет-магазина на сервер:

|  |  |  |
| --- | --- | --- |
| Name | Format | Value |
| login | **Varchar2(32)** | login |
| password | **Varchar2(32)** | password |
| Status | **Varchar2** | «Short» or «Full» |
| MerID | **Number(15)** | Your Merchant ID |
| OrderID | **Varchar2(99)** | Order id |
| Type | **Varchar2(32)** | Purchase – выводит информацию по оплате  Refund – выводит информацию по крайнему в рамках заказа возврату |
| RedirectURL | **Varchar2(32)** | URL для перенаправления ответа\* |
| RedirectMethod | **Varchar2(32)** | Метод ответа (POST / GET)\* |

**\* Необязательные поля. Без них вывод ответа будет на странице сервлета.**

## Пример формы для отправки запроса на сервер

<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

</head>

<body>

<form method=*"Post"* action = *"*<https://mpi.mkb.ru:9443/finoperate/dogetorderstatusservlet>*"*>

Login: <input id="login" name="login" type='text' SIZE="32" MAXLENGTH="16"><br>

Password: <input id="password" name="password" type='password' SIZE="32" MAXLENGTH="16"><br>

Status: <select size="1" id="Status" name="Status" style="width:209px; height: 24px">

<option value="Short" selected="selected">Short</option>

<option value="Full">Full</option>

</select><br>

MerID: <input id='MerID' type='text' name='MerID' MAXLENGTH="15" ><br>

OrderId: <input id='OrderID' type='text' name='OrderID' MAXLENGTH="99"><br>

Redirect URL: <input id='RedirectURL' type='text' value=https://mpos-app-preprod:8443/testfinoperateredirectapp/getanswerservlet name='RedirectURL'><br>

GET<input type="radio" name="RedirectMethod" value="GET">&nbsp;&nbsp;

POST<input type="radio" name="RedirectMethod" value="POST" checked>

<input type="submit" value="Submit">

</form>

</body>

</html>

## Пример ответа на запрос статуса заказа

В ответ сервер присылает поля с информацией по заказу, где

**<amount>** - сумма

**<auth\_id>** - код авторизации по операции

**<auth\_responsedata>** - расшифровка статуса по операции

**<count>** - количество операций данного типа.

Например если при Type=Refund выводится <count>5</count><, значит было проведено 5 возвратов по данному заказу. Информация отображается только по крайнему.

**<date>** - дата и время проведения транзакции

**<orderId>** - номер заказа

**<rrn>** - код RRN по операции

**<secure3D>** - признак наличия проверки кода 3D Secure по данной операции.

Yes – проверялся, No – карта «не запрашивала» 3D Secure.

**<status>** - статус операции (ниже таблица с описанием. Пункт 4).

**Для запроса краткой информации Status = Short:**

<order><orderId>20150525\_04</orderId><status>5 - Возврат</status></order>

**Для запроса полной информации Status = Full:**

<order><amount>100</amount><auth\_id>028761</auth\_id><auth\_responsedata>Transaction is approved.</auth\_responsedata><count>1</count><date>2017-02-06 14:50:20.987</date><orderId>test060217</orderId><rrn>703727848784</rrn><secure3D>No</secure3D><status>1 - Авторизация</status></order>

## Возможные статусы

В ответе отображается сообщение, которое выделено только жирным шрифтом.

Например, **1 - Авторизация**.

**0 – Web запрос**

Клиент проводит в данный момент операцию или ответ по операции не получен (клиент закрыл браузер)

**1 – Авторизация**

Транзакция со статусом Approved, т.е. успешное холдирование, которое нужно завершить с помощью Capture.

**2 – Отказ**

Транзакция со статусом Declined, т.е. операция была проведена через процессинг, но отклонена. Отображается для таких случаев, как «недостаточно средств» и т.д.

**3 – Завершено**

Полностью завершённая транзакция, по которой была произведена Capture.

**4 – Отменено**

Операция, по которой выполнен Reverse, т.е. деньги расхолдированы.

**5 – Возврат**

Операция, по которой выполнен Refund, т.е. начата/выполнена процедура возврата средств по полностью завершённой операции. Возврат денег на карту клиента может производиться в течение 30 календарных дней (зависит от Платёжной Системы и Банка-Эмитента)!

**6 – Ошибка 3DSecure**

С данным статусом возвращаются все операции, по которым цикл работы сервера завершен и вернулся ответ с ошибкой Response=3. Ошибка может быть не связана с 3DSecure!

**7 – Операция не завершена клиентом**

Клиент нажал кнопку «отмена» на странице для ввода номера карты и подобные случаи.

# Дополнительное описание в транзакции

Если Вам требуется передавать дополнительное описание к платежу (например, указание об участии в акции и т.д.), Вы можете добавить в запрос ряд полей.

Описание можно посмотреть в личном кабинете:

1. выбрать необходимую операцию.

2. пройти во вкладку Additional Details.

Также данные поля отображены на чеке оплаты, т.е. клиент будет проинформирован.

Данные, которые направляются в запросе от интернет-магазина на сервер:

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | Format: | Value: | Данные для теста: |
| AdditionalDetails | **Varchar2(1)** | Y или N | Признак отправки. При =N поля игнорируются. |
| NoOfFields | **Number(1)** | От 1 до 9 | Количество строк в описании. Максимум девять. |
| FieldDescription1 \* | **Varchar2(20)** | Uchastie v Aktsii | Левый столбец описания. Как правило, это общее поле в котором передаётся общее обозначение, например «Nomer Dogovora».  **Поддерживается только латиница!** |
| FieldValue1 \* | **Varchar2(50)** | Sezonnie Skidki | Правый столбец описания. Как правило, используется для самого названия акций и т.д.  **Поддерживается только латиница!** |

**\* цифра – обозначение номера строки. Основано на поле NoOfFields.**

Если передаётся NoOfFields=9, должны отправляться поля FieldDescription2, FieldValue2, FieldDescription3, FieldValue3 и т.д.

# Вложения

## Логотип Visa



## Логотип Mastercard



# Коды ответов от сервера (Response, Reason)

## Оригинальные коды ответов, которые согласованы с Международными Платёжными Системами

|  |  |  |
| --- | --- | --- |
| **System Reason Codes for Response Code 2**  **Reason Code** | **Name** | **Description** |
| 2 | Transaction is declined. | Normal Decline |
| 3 | Transaction is declined | Referral. Call for further details on this transaction. |
| 4 | Transaction is declined. | Pick up card (if possible) or report to authorities. |
| 35 | Unable to process your request. Please try later. | Merchant exceeds allowed amount. |
| 38 | Transaction processing terminated. Please try again later. | Transaction is not permitted to merchant. |
| 39 | Issuer or switch not available. Please try again later | Issuing bank or switch not available. Transaction has timed-out. |

|  |  |  |
| --- | --- | --- |
| **System Reason Codes for Response Code 3**  **Reason Code** | **Reason Text** | **Description** |
| 5 | Connection not secured. | Connection was not secured. |
| 6 | HTTP Method not POST | HTTP Method not POST |
| 7 | *Field* is missing. | *Field* is missing |
| 8 | *Field* format is invalid. | *Field* format is invalid. |
| 10 | Invalid Merchant | Not such merchant. |
| 11 | Authentication Failed (Signature computed incorrectly). | Merchant was found but computed signature does not match one included in the request |
| 12 | Merchant is inactive. | Merchant is not enabled for processing |
| 14 | Merchant is not allowed to process this currency | Currency supplied is not permitted. |
| 15 | Merchant settings are not valid. | Merchant record is not correctly setup in the system. |
| 16 | Unable to process transaction | Unable to authenticate merchant now. Try later. |
| 36 | Credit Card holder canceled the request. | Credit Card holder canceled the request. |
| 37 | Card Entry Retry Count Exited Allowed Limit. | Card Entry Retry Count Exited Allowed Limit. |
| 40 | Duplicate Order Not Allowed | Merchant order identification numbers must be unique |
| 41 | Card Holder Session Expired. | Card Holder’s Session expired while performing a 3DS Transaction. Possibly because he/she closed the window, or pressed the back button in the middle of the transaction. |
| 42 | Illegal Operation by Card holder. Check Order Status. | Card Holder Pressed the back button while the transaction was processing. Check the status of that order. |
| 60 | Duplicate Order Not Allowed | FAC Custom based on amount |
| 90 | General Error during processing. Please try again later. | An unexpected error occurred in the system. |

|  |  |  |
| --- | --- | --- |
| **System Reason Codes for 3D-Secure Errors for Response Code 3**  **Reason Code** | **Reason Text** | **Description** |
| 13 | Merchant is not allowed to process cards in this Payment system. | Merchant is blocked. |
| 17 | Unable to process transaction | System cannot process a Card Range Request |
| 18 | Unable to process transaction | System cannot build a Verify Enrollment Request. |
| 19 | Unable to process transaction | System cannot contact Visa Directory. |
| 20 | Unable to process transaction. | System cannot build a Payment Authentication. |
| 21 | Unable to process transaction | System could not contact Issues ACS Server. |
| 22 | Unable to process transaction | Issuer ACS responded with invalid data or returned data failed. |
| 23 | Unable to process transaction | System cannot process a Verify Enrollment Request. |
| 31 | Authentication successful | 3-D Secure Payment Authentication successful |
| 32 | Authentication failed | 3-D Secure Payment Authentication failed. |
| 33 | Authentication successful with attempt. | Attempt authentication was performed. |
| 34 | Authentication failed with error. | Authentication result not expected. |
| 50 | Verify Enrollment Response Unavailable | The VeRes message came back from the MPI as a “U”. This may be returned during an Authentication only request. |
| 51 | Bin not Enrolled | The VeRes message came back from the MPI as an “N” bin not enrolled. This may be returned during an Authentication only request. |
| 52 | Card not Enrolled | The VeRes message came back from the MPI as an “N” card not enrolled. This may be returned during an Authentication only request. |
| 53 | Payer Authentication Response Unavailable | The PaRes message came back from the MPI as “U”. This may be returned during an Authentication only request. |

## Расшифровки и описания наиболее встречающихся кодов ответов при работе с основной платёжной страницей MPI и сервисом Express Payment

|  |  |
| --- | --- |
| **Ответ от сервера содержит Response=2**  **Reason Code=** | **Описание причины ответа** |
| 2 | Банк-Эмитент, выпустивший карту клиента, прислал сообщение с Общим отказом, т.е. «недостаточно средств на карте клиента», «запрещены Online-платежи», «отказ в обслуживании» и прочее. |
| 4 | Банк-Эмитент, выпустивший карту клиента, прислал сообщение о попытке проведения операции по заблокированной/украденной карте. |
| 38 | Банк-Эмитент, выпустивший карту клиента, запретил проведение операции. |
| 39 | Шлюз взаимодействия с Банком-Эмитентом, выпустившим карту клиента, в данный момент недоступен. Неработоспособность может возникать как на стороне МКБ, так и на стороне конечного эмитента. |

|  |  |
| --- | --- |
| **Ответ от сервера содержит Response=3**  **Reason Code=** | **Описание причины ответа** |
| 7 | Отсутствует одно из основных полей. Если у Вас возникают трудности с самостоятельной диагностикой, необходимо сформировать запрос на оплату методом HTTP GET, скопировать полученную ссылку из адресной строки браузера и отправить на почту отдела эквайринга [POS@MKB.RU](mailto:POS@MKB.RU) вместе с кратким описанием ситуации. |
| 8 | Ошибка в одном из основных полей. Если у Вас возникают трудности с самостоятельной диагностикой, необходимо сформировать запрос на оплату методом HTTP GET, скопировать полученную ссылку из адресной строки браузера и отправить на почту отдела эквайринга [POS@MKB.RU](mailto:POS@MKB.RU) вместе с кратким описанием ситуации. |
| 10 | В поле mid (MerchantID) указан некорректный номер продавца. Если у Вас возникают трудности с самостоятельной диагностикой, необходимо сформировать запрос на оплату методом HTTP GET, скопировать полученную ссылку из адресной строки браузера и отправить на почту отдела эквайринга [POS@MKB.RU](mailto:POS@MKB.RU) вместе с кратким описанием ситуации. |
| 11 | Значение поля подписи (signature) не проходит расшифровку. Поле неверно сформировано или отсутствует. Перепроверьте формирование и отправку данного поля.  Основные ошибки:  А) Подпись формируется не по 12-тизначной сумме и/или без учёта копеек.  Б) Неправильно отрабатывает вызов номера заказа из БД сайта, т.е. подпись формируется одна и та же.  В) Название поля отправлено с опечаткой в символе или в уровне регистра, например Signature (верно только signature с маленькой буквы). |
| 13 | Мерчант заблокирован. Обратитесь на [pos@mkb.ru](mailto:pos@mkb.ru) |
| 14 | Банк-Эмитент, выпустивший карту клиента, вернул сообщение об ошибке конвертации валюты. |
| 15 | Настройки mid (MerchantID) некорректны или имеют особые условия. Обратитесь на [pos@mkb.ru](mailto:pos@mkb.ru) |
| 18 | Сервис не может выполнить проверку наличия на 3D Secure. |
| 23 | Получено сообщение с отказом от Платёжной Системы |
| 32 | Банк-Эмитент, выпустивший карту, прислал сообщение о том, что клиент ввёл некорректный защитный код 3D Secure. |
| 34 | Банк-Эмитент, выпустивший карту, прислал отказ в проведении технологии 3D Secure. |
| 36 | Банк-Эмитент, выпустивший карту, прислал сообщение о том, что клиент закрыл страницу для ввода защитного кода 3D Secure. |
| 40 | Дублёр номера заказа oid (OrderID). Допускается повторная отправка значения номера заказа для неуспешных операций с Response=2 и Response=3.  Если сервер по данному заказу отвечал Response=1 , то допускается выполнение только завершающих операций (capture, reverse, refund). |
| 50 | Получено сообщение от Платёжной Системы о том, что карта не поддерживает платежи по интернет-эквайрингу.  Общий случай – попытка оплаты по картам с припиской Electron (Visa Electron, MasterCard Electronic, Maestro Electron). |
| 51 | Получено сообщение от Платёжной Системы о том, что БИН карты не зарегистрирован в Платёжной Системе. |
| 52 | Получено сообщение от Платёжной Системы о том, что операция возможна только с вводом защитного кода 3D Secure, но карта не поддерживает данную технологию. |
| 53 | Отсутствует конечный ответ от страницы ввода защитного кода 3D Secure.  Общий случай – клиент закрыл браузер в момент ввода защитного кода и после таймаута отображён данный Reason-код. |
| 90 | Операция завершена с ошибкой.  Необходимо либо попробовать провести операцию ещё раз, либо другой картой. В случае повторения ошибки организации необходимо обратиться на [pos@mkb.ru](mailto:pos@mkb.ru) |