Руководство администратора по работе с сервисом «Электронная Коммерция» МОСКОВСКОГО КРЕДИТНОГО БАНКА

консультации по юридическим вопросам:
8 (495) 797-42-22, доб. 6716, 8417
ecom@mkb.ru

консультации по техническим вопросам:
8 (495) 797-42-22, доб. 8049, 6816
EcomSupport@mkb.ru

Оглавление

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ 4

1) Требования к сайту 4
2) Рекомендации по размещению правил оплаты в интернет-магазине 4

2. ОСНОВНОЙ ЗАПРОС НА ОПЛАТУ: ФОРМИРОВАНИЕ СТРАНИЦЫ ОПЛАТЫ (MPI) 6

1) Поля, используемые для работы с сервером 8
2) Пример формы для формирования запроса 10
3) Взаимодействие клиента с сервисом 10
4) Формирование поля signature 10
5) Результат обработки транзакции (ответ от сервера) 11
6) Пример ответа от сервера MPI 13
7) Передача и обработка поля resp_url 13
8) Передача и обработка поля directposturl 14
9) Общий пример приёма пакета ответа на Java 14
10) Пример содержимого в ответе от сервера 14
11) Тестовые карты 15

3. СЕРВИС «EXPRESS PAYMENT» 16

1) Демоверсия 16
2) Начало работы 16
3) Формирование заказа 18
4) Проверка статуса платежа 18

4. ЗАВЕРШАЮЩИЙ ЗАПРОС: FINANCIALLINK 19

1) Формирование запроса на сервер 19
2) Формирование поля Signature 20
3) Результат обработки транзакции (ответ от сервера) 20
4) Возможные ответы от сервера в Financial Link 22
5) Адрес боевого сервера 23

5. ДОПОЛНИТЕЛЬНЫЙ ЗАПРОС: СТАТУС ОПЕРАЦИИ 24

1) Формирование HTTPS POST запроса на сервер 24
2) Пример формы для отправки запроса на сервер 24
3) Пример ответа на запрос статуса заказа 25
4) Возможные статусы 25

6. ДОПОЛНИТЕЛЬНОЕ ОПИСАНИЕ В ТРАНЗАКЦИИ 27

7. ОФОРМЛЕНИЕ ПОДПИСКИ (ПОВТОРЯЮЩИЙСЯ ПЛАТЁЖ - RECURRING) 28

Настройка рекуррентных платежей 29
Запрос параметров рекуррентного платежа 30
Запрос на получение статистики по всем рекуррентам за период 31

8. ЧЕКИ 34

1) Стандартный чек 34
2) Чек с дополнительными полями 34

9. ПРИВЯЗКА КАРТ 36

10. ЗАПРОС ОПЕРАЦИЙ ЗА ОПРЕДЕЛЕННУЮ ДАТУ 40

11. ДОПОЛНИТЕЛЬНОЕ ОПИСАНИЕ ТРАНЗАКЦИИ ДЛЯ РЕЕСТРА 42

12. MARKETPLACE. ДОПОЛНИТЕЛЬНЫЕ ПОЛЯ ДЛЯ ПРОВЕДЕНИЯ ПОДТВЕРЖДЕНИЯ. .. 43

13. ДЕМО ВЕРСИЯ ЛК 44

14. ВЛОЖЕНИЯ 44

1) Логотип Visa 44
2) Логотип Mastercard 44

15. КОДЫ ОТВЕТОВ ОТ СЕРВЕРА (RESPONSE, REASON) 46

1) ОРИГИНАЛЬНЫЕ КОДЫ ОТВЕТОВ, КОТОРЫЕ СОГЛАСОВАНЫ С МЕЖДУНАРОДНЫМИ ПЛАТЁЖНЫМИ СИСТЕМАМИ 46

2) РАСШИФРОВКИ И ОПИСАНИЯ НАИБОЛЕЕ ВСТРЕЧАЮЩИХСЯ КОДОВ ОТВЕТОВ ПРИ РАБОТЕ С ОСНОВНОЙ ПЛАТЁЖНОЙ СТРАНИЦЕЙ MPI И СЕРВИСОМ EXPRESS PAYMENT 47

1. 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.

1) 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.**

3. Проверка наличия заголовка Referer в запросе (https://ru.wikipedia.org/wiki/HTTP_referer).
   Данный заголовок заполняется браузером автоматически, при переходе клиентом с одной страницы на другую. При получении запроса на страницу MPI происходит проверка хоста полученного из данного заголовка. Имя хоста привязывается к номеру мерчанта (поле mid из запроса).
   Не допускается указание относительного URI. Заголовок обязательно должен содержать протокол https и имя хоста.
   Возможные последствия:
   Если покупатель самостоятельно выключит передачу данного заголовка в настройках браузера, будет отказ в проведении операции.
   Если магазин использует не стандартные способы для перехода клиентом на платежную страницу, потребуется серьезная доработка со стороны клиента.

2) Рекомендации по размещению правил оплаты в интернет-магазине

Правила оплаты в Интернет-магазине.

К оплате принимаются платежные карты: VISA Inc, MasterCard WorldWide и Мир

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.

2. 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** пункте данного раздела) и с переходом по одному из нижеуказанных адресов:

   Тестовый сервер: **https://mpi.mkb.ru:9443/MPI_payment/**
   «Боевой» сервер: **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=EcomSupport@mkb.ru&resp_url=online.mkb.ru

2. Клиент указывает персональные данные на защищённой странице Банка.
   2.1 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.

3. 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).
   3.1 Также информацию о заказах можно узнать в личном кабинете или с помощью отправки дополнительных запросов (см. **раздел 4**).

***** 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), 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.

1) 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.	600000000000141 (тестовый авто подтверждение) 600000000000505 (тестовый ручное подтверждение) **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 ./|`~!@$^*()-_=+[]{}: кроме & , < > ;# **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 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 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 протокола TLS 1.2** **На сервера с сертификатом «ниже» TLS 1.2 сервер возвращать ответ не будет.**
redirect_url	URL для перенаправления клиента после оплаты. Подробнее о «схеме» перенаправлений ниже в пункте три 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**
frame	Открытие странице во фрейме	При передаче в поле значения **true**, страница открывается во фрейме
receipt_id*	Идентификатор чека.	При передаче данного поля после успешного завершения операции будет запущена процедура отправки фискальных данных

*-используется, если есть интеграция с онлайн кассой и банком.

2) 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='EcomSupport@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.

3) 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 пункте.

2. После заполнения и проверки, данные отправляются на сервер банка для обработки.

3. Клиент получает ответ о состоянии платежа.

4. Формируется и отправляется ответ на сайт.

5. **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

4) Формирование поля signature

Пароль, необходимый для формирования поля signature во время тестирования -
1LsLNYeg(600000000000141- авто подтверждение)
9zrJya7u(600000000000505- ручное подтверждение)

Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров:

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

Например:

kW1dI8Zi5000000000116924432222ORGANIZACIYA-10000000100006433

Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
2c1f1eeef4962d6b9f68966909c30b6bf4a1cfb8ce92a9f1dc7e63c003bf0558

Кодируем полученное значение в BASE64:
LB8e7vSWLWufaJZpCcMLa/Shz7jOkqnx3H5jwAO/BVg=

Например, в PHP, чтобы получить signature, необходимо выполнить следующие операции над строкой:
base64_encode(hex2bin(sha256('kW1dI8Zi5000000000116924432222ORGANIZACIYA-10000000100006433')))

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/WebResource/

5) 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

2) 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

3) 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:

kW1dI8Zi5000000000116924432222ORGANIZACIYA-1111

Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:

2512083bdbaad281369dd3e85cf3726f7707402649bebde642161f47c0e4f6d2

Кодируем полученное значение в BASE64:

JRIIO9uq0oE2ndPoXPNyb3cHQCZJvr3mQhYfR8Dk9tI=

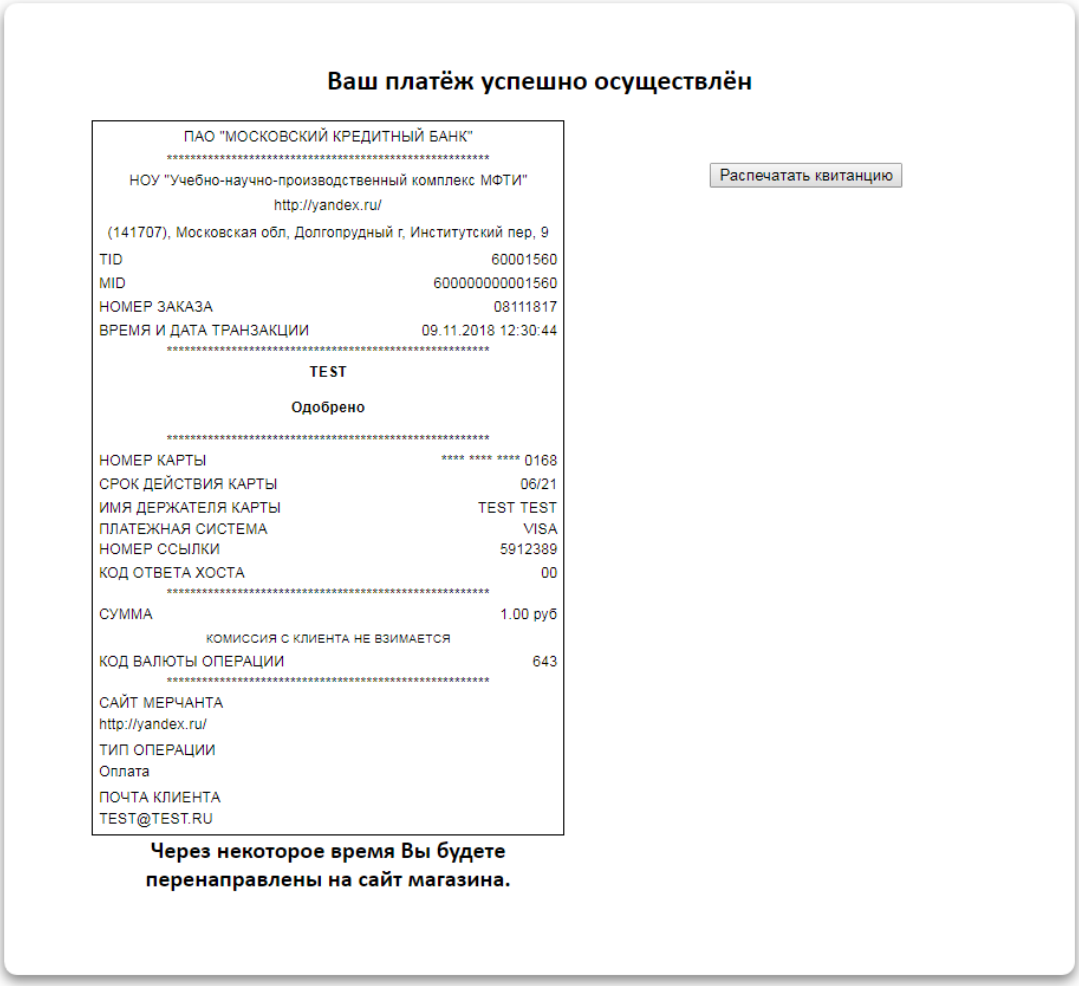
Для окончательного завершения тестирования, подпись необходимо проверить, т.е. рассчитать ее на основании Ваших параметров и сверить с тем, что прислал сервер.
По ошибкам, которыми отвечает сам сервер (например, «неверно сформированная подпись» или «неверный mid»), сервер signature не присваивает.

6) 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.



Ваш платёж успешно осуществлён

ПАО "МОСКОВСКИЙ КРЕДИТНЫЙ БАНК"
****
НОУ "Учебно-научно-производственный комплекс МФТИ"
http://yandex.ru/
(141707), Московская обл, Долгопрудный г, Институтский пер, 9

TID	60001560
MID	600000000001560
НОМЕР ЗАКАЗА	08111817
ВРЕМЯ И ДАТА ТРАНЗАКЦИИ	09.11.2018 12:30:44

****
TEST

Одобрено

****

НОМЕР КАРТЫ	**** **** **** 0168
СРОК ДЕЙСТВИЯ КАРТЫ	06/21
ИМЯ ДЕРЖАТЕЛЯ КАРТЫ	TEST TEST
ПЛАТЕЖНАЯ СИСТЕМА	VISA
НОМЕР ССЫЛКИ	5912389
КОД ОТВЕТА ХОСТА	00

****

СУММА	1.00 руб

КОМИССИЯ С КЛИЕНТА НЕ ВЗИМАЕТСЯ

КОД ВАЛЮТЫ ОПЕРАЦИИ	643

****
САЙТ МЕРЧАНТА
http://yandex.ru/
ТИП ОПЕРАЦИИ
Оплата
ПОЧТА КЛИЕНТА
TEST@TEST.RU

Распечатать квитанцию

Через некоторое время Вы будете перенаправлены на сайт магазина.

7) 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.

8) 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.

9) 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(); }
   }
}
```

10) Пример содержимого в ответе от сервера

Signature=UMdWfapi3lCghp3V4DzptADa3Qg=&SignatureMethod=SHA256&MerID=600000000001834&AcqID=443222&OrderID=843631&amt=000000120000&PaddedCardNo=XXXXXXXXXXXX4089&ResponseCode=1&ReasonCode=1&AuthCode=594523&ReferenceNo=610915982302&ReasonCodeDesc=Transaction is approved.&

11) Тестовые карты

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

Платёжная система: Visa
Номер карты: : 4432 семь три ноль ноль ноль ноль ноль ноль 0168
Срок действия: 10/23
ФИО плательщика (при оплате на тестовом сервере можно указать хоть «Q W», но обязательно минимум в два слова через пробел): TEST 2015 VISA PW 15
Защитный код CVV: 463

Платёжная система: Мир
Номер карты: : 2200 два шесть ноль два ноль ноль два ноль 4075
Срок действия: 07/23
ФИО плательщика (при оплате на тестовом сервере можно указать хоть «Q W», но обязательно минимум в два слова через пробел): NO NAME
Защитный код CVV: 056

Платёжная система: MasterCard
Номер карты: 5218 ноль один ноль ноль ноль один ноль ноль 0054
Срок действия: 11/23
ФИО плательщика (при оплате на тестовом сервере можно указать хоть «Q W», но обязательно минимум в два слова через пробел): TEST PW1
Защитный код CVV: 041

3. 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 (конкретнее)

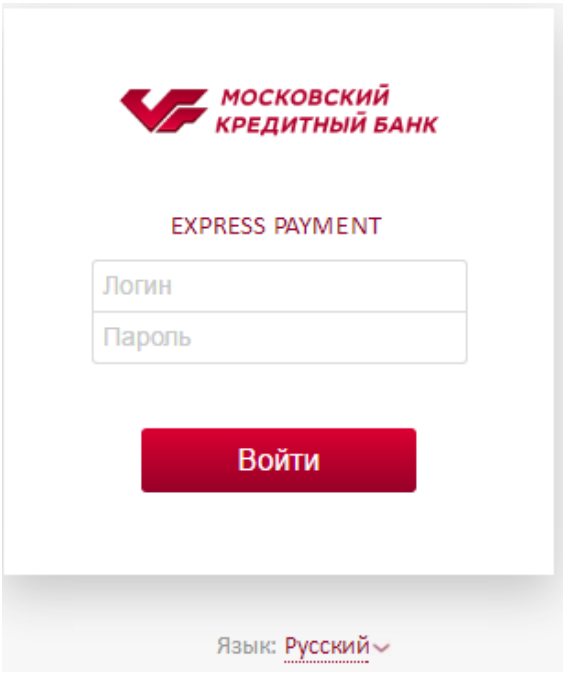
В случае необходимости создания нового пользователя, изменения номера телефона у уже существующих пользователей и в других подобных ситуациях, следует обращаться по электронной почте на EcomSupport@mkb.ru

1) Демоверсия

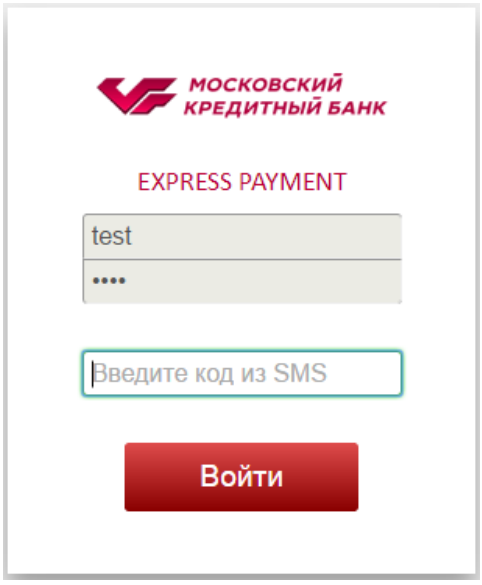
Ссылка на тестовый сервис: https://mpi.mkb.ru:9443/ep/
Логин: test
Пароль: test
Код из СМС: 00000

2) Начало работы

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

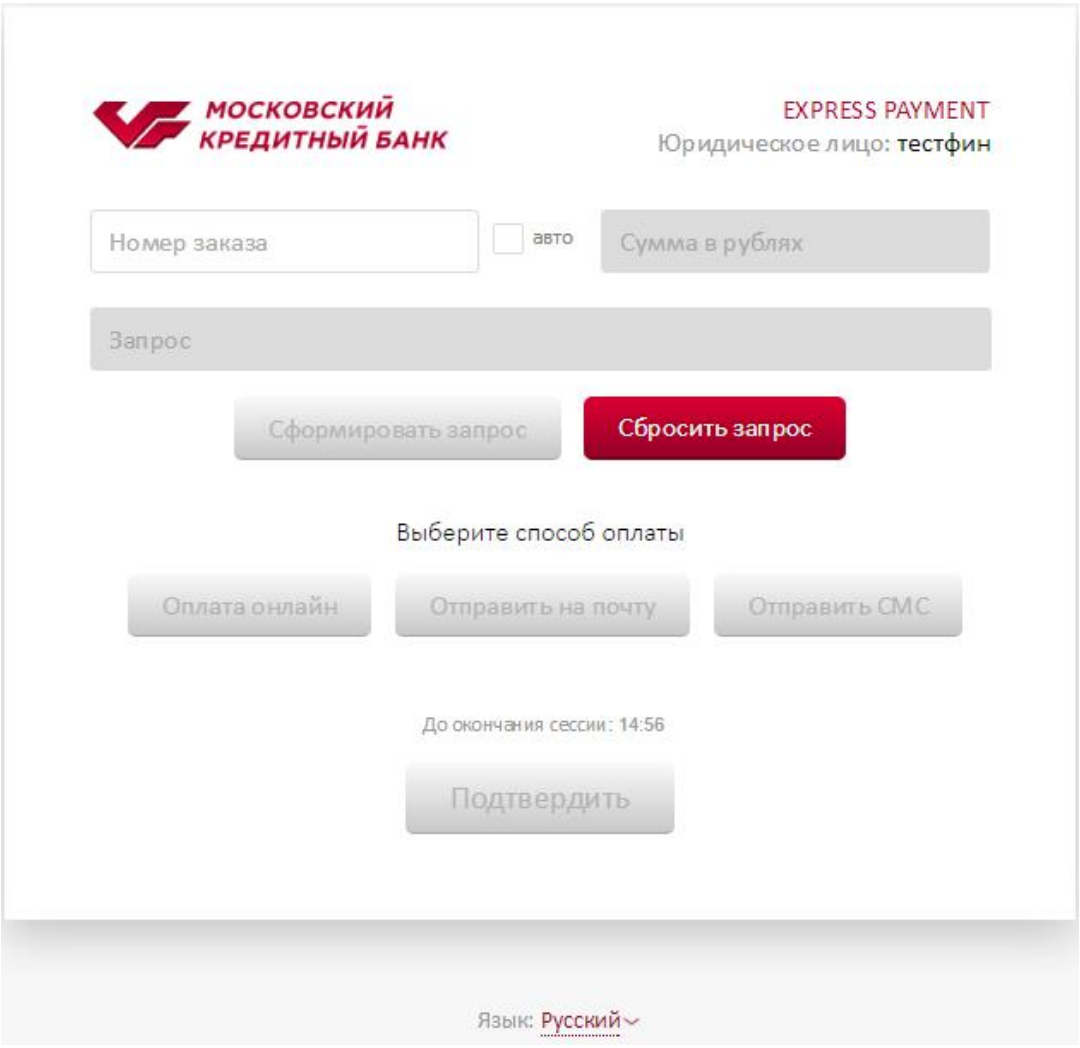


Для входа в сервис используйте выданные Вам логин и пароль. Если комбинация логина и пароля корректна, то Вам отобразиться поле для ввода кода из СМС.



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

После ввода кода Вам отобразится основное меню сервиса.



3) 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:
   ,./\|<>`~!@#$%^*()-_=+[]{}‘“;:

   Номер заказа должен быть уникальным для каждой транзакции. Допускается повторная отправка ранее использованного номера заказа, если операция завершилась с ошибкой.

2. Укажите сумму в рублях.

3. Нажмите «сформировать запрос». Станет активен выбор способа оплаты.

4. 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.

4) 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/lk

4. Завершающий 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.

1) 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	SHA256	Метод генерации подписи. Значение статично.

Адрес тестового сервера, на который отправляются данные:

https://mpi.mkb.ru:9443/finoperate/dofinancialoperationservlet

2) Формирование поля Signature

Принцип формирования подписи аналогичен стандартной оплате.

Для формирования цифровой подписи, необходимо посчитать хэш SHA-256 от строки в которую входят значения следующих параметров:

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

Например:

3G7Kgu3N500000000003285443222ORGANIZACIYA-1000000017600643

Считаем SHA-256, получаем хэш в шестнадцатиричной кодировке:

012017e144046ddceeb45eb4b271d1ed5783c76470f514a434b418f6d06756f4

Кодируем полученное значение в BASE64:

ASAX4UQEbdzutF60snHR7VeDx2Rw9RSkNLQY9tBnVvQ=

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

base64_encode(hex2bin(sha256('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/WebResource/

3) 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

2) 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

3) 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-256, получаем хэш в шестнадцатеричной кодировке:

77bd8d99571e0ca7b30dd7b7dc9ef3a77894d292f5c13fb4aa332223106ef6b7

Кодируем полученное значение в BASE64:

d72NmVceDKezDde33J7zp3iU0pL1wT+0qjMiIxBu9rc=

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

4) Возможные ответы от сервера в Financial Link

Reverse:

1) Response Code = 1

Reason Code	Описание
1	Успешная отмена

2) 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

2) Response Code = 3

Reason Code	Описание
11	Списание уже подтверждено
12	Сумма превышает оригинальную
24	Информация по заказу не найдена
26	Время на проведение операции вышло.
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

2) Response Code = 3

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

5) Адрес боевого сервера

Адрес сервера, на который отправляются данные:

https://mpi.mkb.ru:8443/finoperate/dofinancialoperationservlet

5. Дополнительный запрос: статус операции

Данный функционал позволяет запросить с сервера текущий статус проведения операции.

1) 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

   «На бою» используется порт 8443.

3. Система обработает транзакцию и отправит в ответ результат.

Данные для тестирования:

Login = test_test
Password = 4e7fbe

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.**

2) 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">  
POST<input type="radio" name="RedirectMethod" value="POST"  checked>
<input type="submit" value="Submit">
```

```
</form>
</body>
</html>
```

3) 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>

4) 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.

6. 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.

Все данные, которые были переданы в поле «AdditionalDetails», возможно выгрузить при формирование отчета в Личном кабинете

7. Оформление подписки (повторяющийся платёж - recurring)

Рекуррент – от англ. «Recurring Payment», в общем понимании так называется платёж, по которому оформляется подписка или автоматическое повторение платежа. По рекуррентным платежам не требуется ввод персональных и карточных данных клиента повторно.

Возможность оформления подписки задаётся на сервере платёжного шлюза МКБ для каждого номера продавца (mid) индивидуально. Для включения необходимо предварительно обратиться к Вашему менеджеру в Банке или на почту EcomSupport@mkb.ru

Возможны две схемы проведения рекуррентных платежей:

1. При подписке со списанием раз месяц/квартал/год следующий платеж будет через 30/90/365 дней
   Пример: подписка на месяц родительский платеж был 02.10 следующий платеж будет списан 1.11
2. При подписке со списанием раз месяц/квартал/год следующий платеж будет через один календарный месяц/календарный квартал/календарный год
   Пример: подписка на месяц родительский платеж был 02.10 следующий платеж будет списан 2.11

   По дефолту мерчанту выставляется вторая схема, для изменения необходимо написать на EcomSupport@mkb.ru

Процедура формирования подписки выглядит следующим образом:

1. Клиент организации при проведении первого платежа соглашается с условиями оформления подписки.
2. На сайте организации формируется запрос на шлюз Московского Кредитного Банка, в котором передаётся ряд полей с настройками данной подписки: сумма, количество списаний, периодичность.
3. Сайт перенаправляет клиента на платёжный шлюз МКБ, клиент указывает персональные и карточные данные, вводит защитный код 3D Secure и завершает операцию.
4. В базе данных платёжного шлюза делается запись о подписке с присланными настройками.
5. В указанную в настройках подписки дату производится автоматический платёж.

Примечания:

1. Подписка будет автоматически оформлена во всех ситуациях, когда платёж был полностью завершён без ошибок (от платёжного шлюза МКБ был получен ответ с Response=1 или Response=2) – даже в случаях, если оригинальная операция была отклонена эмитентом.
2. Все платежи, связанные с подписками, всегда автоматически подтверждаются сервером. Т.е. возможность оформить подписку только по холдированию средств на карте без фактического списания – отсутствует.
3. Первый платёж происходит как обычная оплата по интернет эквайрингу, а все последующие платежи происходят в фоновом для клиента и организации режиме согласно настройкам подписки.
4. Изменить настройки подписки или отменить её можно в личном кабинете организации на странице «Рекурренты».
5. По каждому проведенному рекуррентному платежу, организации будет отправляться ответ на directposturl/ resp_url, по аналогии с родительским платежом, а клиенту письмо со слипом и ссылкой для отключения подписки.

Если Вам требуется оформление подписки к оригинальному платежу, Вы можете добавить в запрос ряд полей.

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

Name:	Format:	Value:	Данные для теста:
Recurring	**Varchar2(1)**	Y или N	Признак отправки. При =N поля игнорируются.
ExecutionDate	**Number(8)**	YYYYMMDD	Дата первого платежа, т.е. фактически текущая дата

Frequency	**Varchar2(1)**	D,W,F,M,E,Q,Y	Периодичность списания: D – раз в день, W – раз в неделю (7 дней), F – раз в 2 недели (14 дней), M – раз в месяц (30 дней), E – раз в 2 месяца (60 дней), Q – раз в квартал (90 дней), Y – раз в год (365 дней). Отсчёт начинается от даты первого платежа.
NumberOfRecurrences	**Number(3)**	от 1 до 365 или 999	Количество списаний по подписке. От 1 до 365- максимально допустимые значения зависят от Frequency, если подписка не до окончания срока действия карты. 999-до окончания срока действия карты

Настройка рекуррентных платежей

Адрес для создания тестового запроса: https://mpi.mkb.ru:9443/eCom_api/finOperate/recurring
Адрес для создания боевой запроса: https://mpi.mkb.ru:8443/eCom_api/finOperate/recurring
Метод: POST

Формирование поля signature

Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров **Password** & **MerchantID (mid)** & **AcquirerID (aid)** & **OrderID (oid)** & **Валюта**

Например:
kW1dI8Zi500000000011692443222ORGANIZACIYA-1643
Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
18faf2b351008fb4456ddfe48dd4813ce69671e700954f72208d20732dff8acc
Кодируем полученное значение в BASE64:
GPrys1EAj7RFbd/kjdSBPOaWcecAlU9yII0gcy3/isw=

Параметр запроса:

Имя	Описание	Формат	Обязательное
mid	Идентификатор магазина	[0-9]{15}	Да
oid	Идентификатор заказа	[a-zA-Z0-9,-/(){}]{1,200}	Да
signature	Подпись запроса		Да
Recurring*	Признак отправки рекуррентного платежа (вкл/откл).	^[N||Y]$	Нет
ExecutionDate*	Изменение даты списание. Отчет идет от дата первого платежа.**	^[0-9]{8}$	Нет
Frequency*	Периодичность списания: D – раз в день, W – раз в неделю (7 дней), F – раз в 2 недели (14 дней), M – раз в месяц (30 дней), E – раз в 2 месяца (60 дней), Q – раз в квартал (90 дней), Y – раз в год (365 дней). Отсчёт начинается от даты первого платежа.	^[D||W||F||M||E||Q||Y|$	Нет

* Обнулить поля нельзя. Передача пустого поля не вносит никаких изменений.

** Для изменения даты списание необходимо изменять дату родительского платежа. Пример: Родительский рекуррентный платеж был 01.01.20 списание раз в квартал, в запросе ExecutionDate был передан 20200101, следующий планируется 01.04.20, но клиент хочет списание 04.04.20, для этого не обходимо изменить дату родительского рекуррента на 3 дня, соответственно необходимо отправить в запросе ExecutionDate=20200104

Параметры ответа:

response_code	Код ответа	[0-9]{1}
reason_code	Код причины отказа	[0-9]{1,2}
description	Описание ответа	[a-zA-Z0-9,.!]{1,500}

Пример запроса:

```
>> POST /eCom_api/finOperate/recurring HTTP/1.1
>> Content-Type: application/json;charset=UTF-8
>> Content-Length: 167
>> Host: mpi.mkb.ru:9443
>> Connection: Keep-Alive
>> User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
>> {
 "mid": "600000000001560",
 "oid": "testOrder_10.12.2019_LtSq4",
  "signature" : "gkSGgkm45TcTFvR4Q9FNMXEbGvoIy/sZDkMDZ6AaQ8k=",
  "Recurring" : "Y",
  "ExecutionDate" : "20200401",
   "Frequency" : "D"
}
```

Пример ответа:

```
<< HTTP/1.1 200 OK
<< Server: Apache-Coyote/1.1
<< Content-Type: application/json;charset=UTF-8
<< Date: Mon, 30 Sep 2019 13:49:00 GMT
<< Content-Length: 95
<<{"reason_code":"1","description":"Approved","response_code":"1"}
```

Запрос параметров рекуррентного платежа

С помощью данного запроса возможно получить информацию по ранее проведенному реккуренту

Адрес для создания тестового запроса: https://mpi.mkb.ru:9443/finoperate/getRecurringInfo
Адрес для создания боевой запроса: https://mpi.mkb.ru:8443/finoperate/getRecurringInfo
Метод: GET

Формирование поля signature

Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров **Password** & **MerchantID (mid)** & **AcquirerID (aid)** & **OrderID (oid)** & **Валюта**

Например:
kW1dI8Zi500000000011692443222ORGANIZACIYA-1643
Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
18faf2b351008fb4456ddfe48dd4813ce69671e700954f72208d20732dff8acc
Кодируем полученное значение в BASE64:
GPrys1EAj7RFbd/kjdSBPOaWcecAlU9yII0gcy3/isw=

Параметр запроса:

Имя	Описание	Формат	Обязательное
mid	Идентификатор магазина	[0-9]{15}	Да
oid	Идентификатор заказа	[a-zA-Z0-9,-/(){}]{1,200}	Да
signature	Подпись запроса		Да

Параметры ответа:

recurring	Признак отправки рекуррентного платежа (вкл/откл).	^[N||Y]$
executionDate	Дата родительского платежа	^[0-9]{8}$
frequency	Периодичность списания	^[D||W||F||M||E||Q||Y|$
nextDataPay	Дата следующего платежа	^[0-9]{8}$
quantityPay	Кол-во оставшихся платежей	^[0-9]{3}$
amount	Сумма	^[0-9]{12}$

Пример запроса:

GET
https://mpi.mkb.ru:9443/finoperate/getRecurringInfo?mid=600000000001560&oid=090920anton&signature=RsLFE87GmDwR%2BpWlGruHB8RKBx4V9ZudpZhWLZzd49s%3D HTTP/1.1
Accept-Encoding: gzip,deflate
Host: mpi.mkb.ru:9443
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

Пример ответа:

HTTP/1.1 200
Server: nginx
Date: Thu, 10 Sep 2020 14:07:46 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 115
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
{"recurring":"Y","executionDate":"20200909","frequency":"M","nextDataPay":"20201009","quantityPay":5,"amount":5100}

Запрос на получение статистики по всем рекуррентам за период

С помощью данного запроса возможно получить информацию по ранее проведенным реккурентам

Адрес для создания тестового запроса:
https://mpi.mkb.ru:9443/eCom_api/recurring/infoByPeriod?mid=<mid>&period_start=<period_start>&period_end=<period_end>&signature=<signature>
Адрес для создания боевой запроса:
https://mpi.mkb.ru:8443/eCom_api/recurring/infoByPeriod?mid=<mid>&period_start=<period_start>&period_end=<period_end>&signature=<signature>
Метод: GET

Формирование поля signature

Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров **Password** & **MerchantID (mid)**

Например:
nXkG847p600000000001560
Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
6183e49b231a4faac7222d6a1acba258d04b649f04aac3e0876e8eab494a8cbf
Кодируем полученное значение в BASE64:
YYPkmyMaT6rHIi1qGsuiWNBLZJ8EqsPgh26Oq0lKjL8=

Параметр запроса:

Имя	Описание	Формат	Обязательное
mid	Идентификатор магазина	[0-9]{15}	Да
period_start	Дата начала поиска по родительскому платежу (из	[0-9]{8}	Да

	executionDate). Шаблон: yyyyMMdd		
period_end	Дата окончания поиска по родительскому платежу (из executionDate). Шаблон: yyyyMMdd	[0-9]{8}	Да
status	Признак включенного/отключенного платежа - Если в запросе поле status отсутствует, отправлять данные по всем рекуррентам и включенным и отключенным за выбранные период. - Если в поле status передано значение Y отправлять данные по включенным рекуррентам. - Если в поле status передано значение N отправлять данные по отключенным рекуррентам.	^[N||Y]$	нет
signature	Подпись запроса		Да

Параметры ответа:

Имя	Описание	Формат
oid	Номер заказа родительского платежа	[a-zA-Z0-9,-/(){}]{1,200}
status	Признак отправки рекуррентного платежа (вкл/откл).	^[N||Y]$
status_code	Код статуса	
disconnection_date	Дата отключения рекуррента	^[0-9]{8}$
executionDate	Дата родительского платежа	^[0-9]{8}$
frequency	Периодичность списания	^[D||W||F||M||E||Q||Y|$
nextDataPay	Дата следующего платежа	^[0-9]{8}$
quantityPay	Кол-во оставшихся платежей	^[0-9]{3}$
amount	Сумма	^[0-9]{12}$

Возможные статусы:

Код	Расшифровка
9	Рекуррент включен и ждет обработки
25	Рекуррент отключен мерчантом
79	Срок действия карты закончился
80	Превышен лимит неуспешных операций
81	Закончен срок действия рекуррента
82	Рекуррент отключен клиентом

Пример запроса:

GET
https://mpi.mkb.ru:9443/eCom_api/recurring/infoByPeriod?mid=600000000001560&period_start=20201001&period_end=20201026&signature=YYPkmyMaT6rHIi1qGsuiWNBLZJ8EqsPgh26Oq0lKjL8%3D&status=N HTTP/1.1
Accept-Encoding: gzip,deflate
Host: mpi.mkb.ru:9443
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)

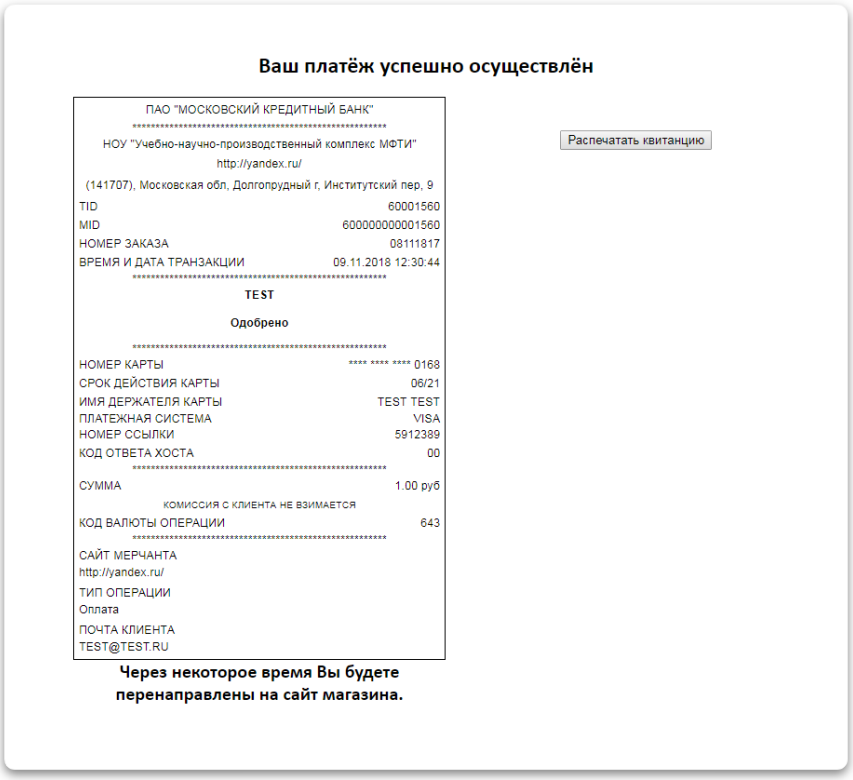
Пример ответа:

TTP/1.1 200
Server: nginx
Date: Mon, 26 Oct 2020 14:09:36 GMT
Content-Type: application/json;charset=UTF-8
Connection: keep-alive
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
Content-Length: 753

{"recurrents":[{"oid":"test_081020-14410","status":"N","frequency":"D","amount":100,"status_code":80,"disconnection_date":null,"execution_date":"20201008","next_pay_date":"20201008","quantity_pay":13},{"oid":"test_081020-14411","status":"N","frequency":"D","amount":100,"status_code":80,"disconnection_date":null,"execution_date":"20201008","next_pay_date":"20201008","quantity_pay":13},{"oid":"test_081020-14412","status":"N","frequency":"D","amount":100,"status_code":80,"disconnection_date":null,"execution_date":"20201008","next_pay_date":"20201008","quantity_pay":13},{"oid":"231020002","status":"N","frequency":"M","amount":31000,"status_code":25,"disconnection_date":"20201026","execution_date":"20201023","next_pay_date":null,"quantity_pay":6}]}

8. Чеки

1) Стандартный чек



Ваш платёж успешно осуществлён

ПАО "МОСКОВСКИЙ КРЕДИТНЫЙ БАНК"
****
НОУ "Учебно-научно-производственный комплекс МФТИ"
http://yandex.ru/
(141707), Московская обл, Долгопрудный г, Институтский пер, 9

TID	60001560
MID	600000000001560
НОМЕР ЗАКАЗА	08111817
ВРЕМЯ И ДАТА ТРАНЗАКЦИИ	09.11.2018 12:30:44

****
TEST

Одобрено

****

НОМЕР КАРТЫ	**** **** **** 0168
СРОК ДЕЙСТВИЯ КАРТЫ	06/21
ИМЯ ДЕРЖАТЕЛЯ КАРТЫ	TEST TEST
ПЛАТЕЖНАЯ СИСТЕМА	VISA
НОМЕР ССЫЛКИ	5912389
КОД ОТВЕТА ХОСТА	00

****

СУММА	1.00 руб

КОМИССИЯ С КЛИЕНТА НЕ ВЗИМАЕТСЯ

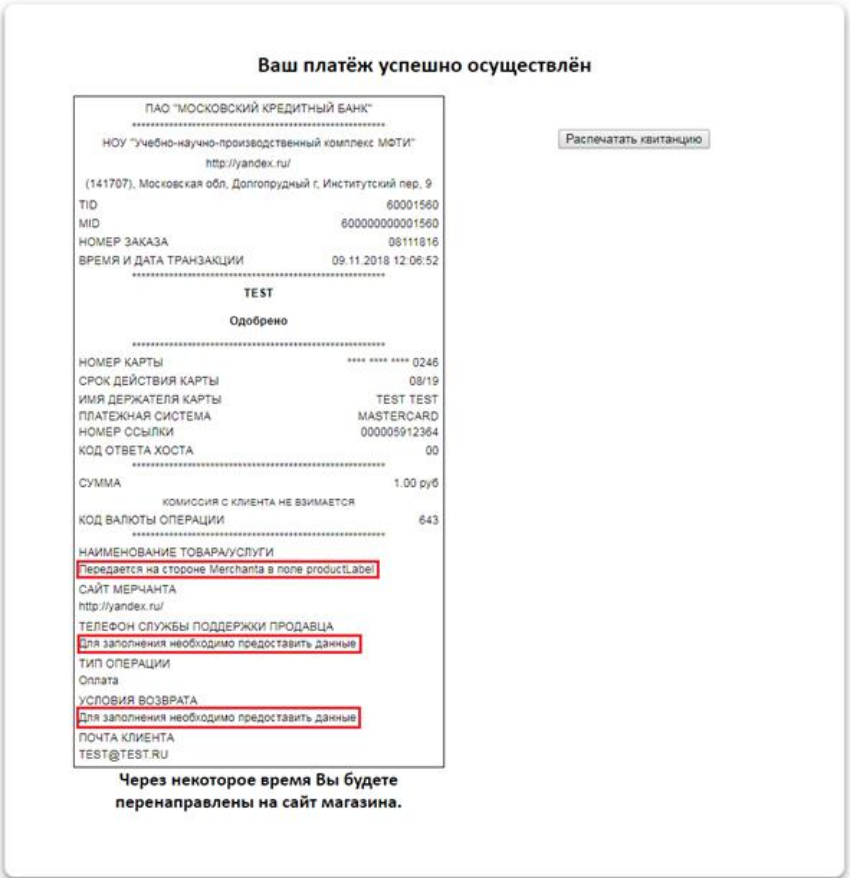
КОД ВАЛЮТЫ ОПЕРАЦИИ	643

****
САЙТ МЕРЧАНТА
http://yandex.ru/
ТИП ОПЕРАЦИИ
Оплата
ПОЧТА КЛИЕНТА
TEST@TEST.RU

Распечатать квитанцию

Через некоторое время Вы будете перенаправлены на сайт магазина.

2) Чек с дополнительными полями



Ваш платёж успешно осуществлён

ПАО "МОСКОВСКИЙ КРЕДИТНЫЙ БАНК"
****
НОУ "Учебно-научно-производственный комплекс МФТИ"
http://yandex.ru/
(141707), Московская обл, Долгопрудный г, Институтский пер, 9

TID	60001560
MID	600000000001560
НОМЕР ЗАКАЗА	08111816
ВРЕМЯ И ДАТА ТРАНЗАКЦИИ	09.11.2018 12:06:52

****
TEST

Одобрено

****

НОМЕР КАРТЫ	**** **** **** 0246
СРОК ДЕЙСТВИЯ КАРТЫ	08/19
ИМЯ ДЕРЖАТЕЛЯ КАРТЫ	TEST TEST
ПЛАТЕЖНАЯ СИСТЕМА	MASTERCARD
НОМЕР ССЫЛКИ	000005912364
КОД ОТВЕТА ХОСТА	00

****

СУММА	1.00 руб

КОМИССИЯ С КЛИЕНТА НЕ ВЗИМАЕТСЯ

КОД ВАЛЮТЫ ОПЕРАЦИИ	643

****
НАИМЕНОВАНИЕ ТОВАРА/УСЛУГИ
Передается на стороне Merchanta в поле productLabel
САЙТ МЕРЧАНТА
http://yandex.ru/
ТЕЛЕФОН СЛУЖБЫ ПОДДЕРЖКИ ПРОДАВЦА
Для заполнения необходимо предоставить данные
ТИП ОПЕРАЦИИ
Оплата
УСЛОВИЯ ВОЗВРАТА
Для заполнения необходимо предоставить данные
ПОЧТА КЛИЕНТА
TEST@TEST.RU

Распечатать квитанцию

Через некоторое время Вы будете перенаправлены на сайт магазина.

Поля выделенные красными премоугольниками можно дополнительно передавать на чеки, следующие поля

Название строки на чеке	Название поля	Описание поля	Значение
Наименование товара/ услуги	productLabel	В данном поле, возможно передавать значения оплачиваемого товара/услуги.	Допускаются буквы кирилицы и латиницы, цифры и все стандартные клавиатурные символы кроме: «?», «:» Максимальное значение- 50 символов **Обязательно один символ должен быть буквенным.** Пример: Телефон Nokia 3310
Телефон службы поддержки продавца		В данном поле, возможно передавать телефон, по которому покупатель может задать вопросы продавцу. По дефолту будет стоять телефон из анкеты.	Данные необходимо предоставить в Банк Значение статичное
Условия возврата		В данном поле, возможно передавать условия для возврата товара/услуги	Данные необходимо предоставить в Банк Значение статичное

3) API для отправки ссылки на чек

Если Вам требуется повторно отправить чек себе/клиенту или получить данные чек необходимо отправить запрос (методом GET) со следующими параметрами :

Имя параметра	Значение	Описание
mid	500000000003285	ID магазина.
oid	Test123	Номер заказа, по которому необходим чек
case	full – все поля чека в формате JSON basic- основные параметры чека в формате JSON html- перенаправит на страничку с чеком email- отправит чек на email	Формат передачи чека
address*	test@mkb.ru	Почтовый адрес на который необходимо направить чек *данное поле необходимо передавать, если значение поля case= email

Адрес тестового сервера, на который отправляются данные:

https://mpi.mkb.ru:9443/finoperate1/getReceipt

Адрес боевого сервера, на который отправляются данные:

https://mpi.mkb.ru:8443/finoperate/getReceipt

9. Привязка карт

Привязка карты при оплате:

Данный функционал включается в личном кабинете клиента, по дефолту данный функционал отключен.

Запоминание карты возможно только при запросе методом POST.

Client_id и Card_id формируется на стороне банка.

Если функционал включён , клиент при оплате на страничке поставил запомнить карту и совершил успешный платеж:

В ответе будет передан его client_id и card_id, пример ответа:

ResponseCode=1&AuthCode=946276 A&cardName=VISA MKB&AcqID=443222&amt=000000002100&CardID=BD939CBA094B4F65E0530F00E60AAB8B&OrderID=1503210191&fio=CZKCZ+CZ&ReasonCode=1&Signature=hLcrILVHqsPKnteVOkKbuw4PvG0%3D&MerID=600000000000141&ClientID=BD939CBA094A4F65E0530F00E60AAB8B&SignatureMethod=SHA1&PaddedCardNo=XXXXXXXXXXXX0168&ReasonCodeDesc=Approved&ReferenceNo=000006892918

Для оплаты уже привязанной картой в теле запроса необходимо дополнительно передавать, либо поле client_id, тогда будут загружены все карты клиента и будет возможность привязать новую, либо client_id и card_id, тогда будет загружена только конкретная карта и оплата будет возможна только по ней, без возможности оплатить или привязать другую карту, со значение, которое было прислано в ответе.
Параметры полей:

Имя	Описание	Формат
client_id	Идентификатор клиента	[a-zA-Z0-9,-/(){}]
card_id	Идентификатор карты	[a-zA-Z0-9,-/(){}]

Пример запроса с client_id:
https://mpi.mkb.ru:9443/MPI_payment/?mid=600000000000141&oid=090321001&amount=000000002100&aid=443222&signature=jBpLofvyCAwMhu4DwJpmAMB8PWk%3D&merchant_mail=&client_mail=&redirect_url=&directposturl=https%3A%2F%2Fmpi.mkb.ru%3A9443%2FMPI_Utilities1%2F&client_id=BD93344BDAD0463BE0530F00E60AF65F

Пример запроса с client_id и card_id:
https://mpi.mkb.ru:9443/MPI_payment/?mid=600000000000141&oid=090321001&amount=000000002100&aid=443222&signature=jBpLofvyCAwMhu4DwJpmAMB8PWk%3D&merchant_mail=&client_mail=&redirect_url=&directposturl=https%3A%2F%2Fmpi.mkb.ru%3A9443%2FMPI_Utilities1%2F&client_id=BD93344BDAD0463BE0530F00E60AF65F&card_id=BD939CBA094B4F65E0530F00E60AAB8B

Регистр букв ВАЖЕН!

Если у клиента три раза подряд будет отказ в проведении операции по любой причине, все карты будут автоматически удалены.

Привязка карты с автоотменой операции.

Формирование поля signature

В запросе присутствует цифровая подпись. Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров **Password & MerchantID (mid) & AcquirerID (aid) & OrderID (oid) & Валюта**
Например:

q63XzIUa600000000001560443222123456643
Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
7512891d88b45af146b6f6db255fe80b93f7c677a3c5589f4633675d822a0923
Кодируем полученное значение в BASE64:
dRKJHYi0WvFGtvbbJV/oC5P3xnejxVifRjNnXYIqCSM=

Пароль, необходимый для формирования поля signature во время тестирования - q63XzIUa (600000000003004)

Адрес отправки запроса:

Тестовый сервер: **https://mpi.mkb.ru:9443/MPI_payment/**
«Боевой» сервер: **https://mpi.mkb.ru/MPI_payment/**

Перечень полей запроса:

Название поля	Описание поля	Необходимые значения и данные для тестирования
mid	Идентификатор Мерчанта (магазина). Статичное значение.	600000000003004 (тестовый) **Индивидуальный «боевой» присваивается после заключения договора.**
aid	Идентификатор Банка-Эквайера. Статичное значение. Для теста и боя используется одинаковый номер.	443222
oid	Номер заказа на сервере (до 150 символов). Допускаются латинские буквы, цифры и следующие клавиатурные символы ./|`~!@$^*()-_=+[]{}: кроме & , < > ;# **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
resp_url*	Поле для получения ответа от сервера, **отправляемого на указанный web-сервер**. Нужно указывать доменное имя или IP сервера. Подробнее в пункте семь 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.	URL страницы сайта, на которую будет передаваться **ответ методом POST**. **На странице обязательно должен быть валидный SSL сертификат протокола TLS 1.2** **На сервера с сертификатом «ниже» TLS 1.2 сервер возвращать ответ не будет.**

	Подробнее в пункте восемь 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.**	
redirect_url*	URL для перенаправления клиента после оплаты. Подробнее о «схеме» перенаправлений ниже в пункте три 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.	Электронный почтовый адрес клиента.
merchant_mail*	E-mail оператора/магазина/администратора.	Электронный почтовый адрес, на который Вам будут приходить уведомления о транзакциях. **Чеки абсолютно идентичные чекам клиентов.**
client_id*	Идентификатор клиента. Поле передается только для существующих клиентов. Если клиент новый, данное поле не заполняется.	

* Не обязательные поля

Пример запроса:

https://mpi.mkb.ru:9443/MPI_payment/?mid=600000000003004&oid=999543&aid=443222&signature=ezqlxnMlqLNrj3mQVe3HWRBuddO9tfJBCfj3bZT7iuQ=&merchant_mail=test@mkb.ru&client_mail=test@mkb.ru&directposturl=https://test.ru&bind_card=true

Пример ответа:

ResponseCode=1&AuthCode=465241&cardName=VISA MKB&AcqID=443222&amt=000000000100&CardID=BB9BDB6D002B683AE0530F00E60AA624&OrderID=999543&fio=SE+S&ReasonCode=1&Signature=Uc6NCvdKnCHRhfo%2BM4XKdpyzG36FwfmsXGmwQDRG1B0%3D&MerID=600000000003004&ClientID=BB9BDB6D002A683AE0530F00E60AA624&SignatureMethod=SHA256&PaddedCardNo=443273XXXXXX0168&ReasonCodeDesc=Approved&ReferenceNo=689092 4

Пароль для прохождения 3DS

Для всех тестовых карт пароль для прохождения 3DS- 1234

Административные запросы для привязанных карт:

Формирование поля signature

Во всех запросах присутствует цифровая подпись. Для формирования цифровой подписи необходимо посчитать хэш SHA-256 от строки, в которую входят значения следующих параметров **Password & MerchantID (mid) & AcquirerID (aid)**

Например:
q63XzIUa600000000001560443222
Считаем SHA-256, получаем хэш в шестнадцатеричной кодировке:
80257f6e42df43bc2fedb42bd416da6e08f17a567f9f774511860b860944086f

Кодируем полученное значение в BASE64:
gCV/bkLfQ7wv7bQr1BbabgjxelZ/n3dFEYYLhglECG8=

Запрос на удаление клиента

Адрес: https://mpi.mkb.ru:9443/eCom_api/client_identification/client/{mid}/{client_id}
Метод: DELETE

Параметры запроса:

Имя	Описание	Формат
mid	Идентификатор магазина	[0-9]{15}
client_id	Идентификатор клиента	[a-zA-Z0-9,-/(){}]
signature	Подпись запроса	

Пример:

https://mpi.mkb.ru:9443/eCom_api/client_identification/client/600000000001560/948A685273C84330A0ED7D408C70DCAD?signature=MdoDRjfN3Z7uGa9P+UKB7nWDGsCqririfoQJJ2+0/tE=

Если удаление прошло успешно, в ответ придет статус 200 OK

Запрос на удаление одной карты клиента

Адрес: https://mpi.mkb.ru:9443/eCom_api/client_identification/card/{mid}/{client_id}/{card_id}
Метод: DELETE

Параметры запроса:

Имя	Описание	Формат
mid	Идентификатор магазина	[0-9]{15}
client_id	Идентификатор клиента	[a-zA-Z0-9,-/(){}]
card_id	Идентификатор карты	[a-zA-Z0-9,-/(){}]
signature	Подпись запроса	

Пример:

https://mpi.mkb.ru:9443/eCom_api/client_identification/card/600000000001560/948A685273C84330A0ED7D408C70DCAD/475724574asdgfasdg?signature=MdoDRjfN3Z7uGa9P+UKB7nWDGsCqririfoQJJ2+0/tE=

Если удаление прошло успешно, в ответ придет статус 200 OK

Запрос на удаление всех карт клиента

Адрес: https://mpi.mkb.ru:9443/eCom_api/client_identification/card/{mid}/{client_id}/
Метод: DELETE

Параметры запроса:

Имя	Описание	Формат
mid	Идентификатор магазина	[0-9]{15}
client_id	Идентификатор клиента	[a-zA-Z0-9,-/(){}]
signature	Подпись запроса	

Пример:
https://mpi.mkb.ru:9443/eCom_api/client_identification/card/600000000001560/948A685273C84330A0ED7D408C70DCAD?signature=MdoDRjfN3Z7uGa9P+UKB7nWDGsCqririfoQJJ2+0/tE=

Если удаление прошло успешно, в ответ придет статус 200 OK

Запрос на получение всех карт клиента
Адрес: https://mpi.mkb.ru:9443/eCom_api/client_identification/{mid}/{client_id}
Метод: GET

Параметры запроса:

Имя	Описание	Формат
mid	Идентификатор магазина	[0-9]{15}
client_id	Идентификатор клиента	[a-zA-Z0-9,-/(){}]
signature	Подпись запроса	

Пример:
https://mpi.mkb.ru:9443/eCom_api/client_identification/600000000001560/948A685273C84330A0ED7D408C70DCAD?signature=MdoDRjfN3Z7uGa9P+UKB7nWDGsCqririfoQJJ2+0/tE=

В ответ придет JSON в следующем формате:


```
{
"mid": "600000000001560",
"oid": null,
"client_id": "96BBCB9A39AD4039B8125D7BFE6BCDFB",
"Response": true,
"ResponseDesc": "Successfully",
"LinkedCards": {
"7B9C98C6B0964385A39043BE175C89E6": {
"exp_date": "**/**",
"pan": "**** **** **** 5555 ",
"cardholder_name": "TEST 2015 VISA PW 15",
"pay_system": "VISA"
}
```


На бою используеться порт 8443

10. Запрос операций за определенную дату

1) Формирование запроса на сервер

Перечень обязательных полей

Имя параметра	Значение	Описание
mid	600000000003285	ID магазина. (указан пример, необходимо использовать боевой ID)
date	01.01.2019	Дата, за которую необходимы операции **Обязательно предаётся в формате 'dd.mm.yyyy'**
signature	nFetcgHG16fyFTT7ctc5tMPmvIQ=	Цифровая подпись, необходимая для аутентификации магазина (формирование см. ниже).

Запрос формируется методом GET!

Адрес сервера, на который отправляются данные:

https://mpi.mkb.ru:8443/finoperate/getOperations

2) Формирование поля Signature

Для формирования цифровой подписи, необходимо посчитать хэш SHA-256 от строки в которую входят значения следующих параметров:
Password & **MerchantID**

Например:

3G7Kgu3N500000000003285

Считаем SHA-256, получаем хэш в шестнадцатиричной кодировке:

7c25e51710b155cd104f6fa1bdef9fabda8d97b989247d5784756b691bd9f3eb

Кодируем полученное значение в BASE64:

fCXlFxCxVc0QT2+hve+fq9qNl7mJJH1XhHVraRvZ8+s=

3) Результат обработки запроса (ответ от сервера)

Ответ включает в себя все операции за выбранную дату и содержит следующие параметры:

Имя параметра	Описание
operationDate	Дата операции
orderId	Номер заказа
operationType	тип операции (оплата, возврат и тп)
sum	Сумма в копейках
payment	Признак операции. Возможные значения: common – обычная операция, recurrent – рекуррент, auto – авто платеж.
pan	Номер карты (маскированный)
cardholder	Имя держателя карты

Ответ передается в формате JSON!
Пример ответа:

[{"operationDate":"11.02.2019","orderId":"jafhg7asfg","operationType":"Оплата","sum":"100000","payment":"auto","pan":"123456******7890","cardholder":"TEST TESTING"},{"operationDate":"11.02.2019","orderId":"453LDFG8FGH","operationType":"Оплата","sum":"116500","payment":"auto","pan":"123456******7890","cardholder":"QWERTY ASDFGH"},{"operationDate":"11.02.2019","orderId":"gg54689sdfDFG","operationType":"Оплата","sum":"216500","payment":"common","pan":"123456******7890","cardholder":"UIOP JKLZXCV"}]

11.Дополнительное описание транзакции для реестра

Для передачи дополнительного описания для реестра необходимо в запросе на оплату передавать дополнительный параметр в виде json обеъкта. Предварительно этот json должен быть преобразован с **URL Encoded**

Перечень полей

Имя параметра	Значение	Описание
twpg_params	{"param_1":"val_1"," param_2":"val_2"} Пример: {"FIO":"Ivanov Ivan Ivanovich"," Dorovor":" ND-123/2"}	Параметр для передачи json обеъкта с данными для реестра.

Правила заполнения параметров в json объекте:
Значение переменной **param** может быть заполнено только буквами латинского алфавита, цифрами и допускается только символ **_** , но **БЕЗ ПРОБЕЛОВ**. Примеры: Dogovor, zadanie_1
Значение переменной **val** может быть заполнено только буквами латинского алфавита, цифрами и допускаются символы: ./\|`~!@^*()-_[]{}:. Примеры: Ivanov Ivan Ivanovich, ND-123/2

Пример запроса:
https://mpi.mkb.ru:9443/MPI_payment/?site_link=ya.ru&mid=600000000001560&oid=test_27-08-20_1246&aid=443222&amount=000000010000&merchant_mail=test@mkb.ru&signature=cftY/8UZ0r+xamW+KmAVomw6TlE=&client_mail=pos@mkb.ru&resp_url=online.mkb.ru&twpg_params=%7B%22FIO%22%3A%22Ivanov Ivan Ivanovich%22%2C%22Dorovor%22%3A%22ND-123/2%22%7D

12. MarketPlace. Дополнительные поля для проведения подтверждения.

Для проведения подтверждения операций сразу после холдирования или в оперделенное время, с параметрами сабмерчантов необходимо дополнительно в запросе передавать следующие поля:

Название поля	Описание поля	Необходимые значения и данные для тестирования	Обязательно для заполнения
SID_1	ID субмерчанта. Если их несколько, то необходимо увеличь цифру в названии поля: SID_2, SID_3 и т.д.	Номер магазина marketplace, которому будет перечислена необходимая сумма.	да
SUMMSID_1	Сумма возмещения, которая будет перечислена субмерчант. Если было передано несколько SID, то необходимо и столько же передавать SUMMSID.	Пример: SID_1=1003 SID_2=1004 SUMMSID_1=10 SUMMSID_2=20	да
PURPOSEOFPAY_1*	Доп. описание перечисления Состоит из кириллицы, пробела, цифр и следующих символов: ( ) , . ‘ ? : - + / №. Максимальное количество символов 210.	Пример: PURPOSEOFPAY_1=товар1	нет
CAPTURESUMM	Общая сумма подтверждения	Пример: CAPTURESUMM=50	да
PURPOSEOFPAY*	Расширенное назначение платежа Состоит из кириллицы, пробела, цифр и следующих символов: ( ) , . ‘ ? : - + / №. Максимальное количество символов 210.	Пример: PURPOSEOFPAY=заказ 123	нет
CAPTUREDATETIME	Дата и время подтверждения в формате YYYY MM DD HH:II:SS Если данное поле не передать, то подтверждение пройдет сразу.	Пример: CAPTUREDATETIME=2020 10 30 15:45:00	нет

*Значение данных полей необходимо предварительно преобразовывать в **URL Encoded**

Пример запроса:

https://mpi.mkb.ru:9443/MPI_payment/?mid=600000000001560&oid=09112004&amount=000000004100&aid=443222&directposturl=https://mpi.mkb.ru:9443/MPI_Utilities1/&SID_1=1003&SID_2=1003&SID_3=1003&SUMMSID_1=20&SUMMSID_2=10&SUMMSID_3=5&PURPOSEOFPAY_1=%D1%82%D0%B5%D1%81%D1%82&PURPOSEOFPAY_2=%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D0%BA%D0%B0&PURPOSEOFPAY_3=%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85&CAPTURESUMM=41&CAPTUREDATETIME=2020+10+30+15%3A45%3A00&PURPOSEOFPAY=%D0%BF%D0%BE%D0%BA%D1%83%D0%BF%D0%BA%D0%B0&signature=GcVPcJywaDnKiV28fUBEUILUBqzY3OejbOQSUrDweMA%3D

13. Демо версия ЛК

Для входа в демо-версию личного кабинет перейдите по ссылке:

https://office-demo.mkb.ru/lk/new_Login

Пользователь для ECom:

Login testE
Pass test

Пользователь для POS-терминалов:

Login testP
Pass test

14.Вложения

1) Логотип Visa

Visa.zip

2) Логотип Mastercard

mastercard.zip

3) Логотип MIR

MIR.zip

15.Коды ответов от сервера (Response, Reason)

1) 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.

2) 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 ECOMSUPPORT@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 ECOMSUPPORT@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 ECOMSUPPORT@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 EcomSupport@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 EcomSupport@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 EcomSupport@mkb.ru