Райффайзен БАНК

Разница
в отношении

Merchant Guide
Internet Acquiring API

Версия документа: 1.0

Введение

Настоящий документ описывает процесс пошагового подключения интернет-магазина к системам банка для осуществления приема карт международных платежных систем Visa, MasterCard, а также национальной платежной системы МИР с использованием протокола **3D-Secure**. Документ ориентирован на технических специалистов.

Термины и определения

Эквайер (Acquirer) – Банк, предоставляющий услугу Интернет эквайринга для интернет-магазина.

Эмитент (Issuer) – Банк, выпустивший карту, оплата по которой принимается в интернет-магазине

МПС – Международные платежные системы (Visa, MasterCard)

НПС – Национальная платежная система МИР

3D-Secure – протокол безопасности, основанный на концепции трех доменов (домен Эквайера, домен Эмитента, домен МПС), который используется как дополнительный уровень безопасности при совершении платежей по картам в Интернет. При проведении операции добавляет ещё один шаг аутентификации для онлайн-платежей, позволяющий торговым точкам и банкам дополнительно убедиться, что платеж совершает именно держатель карты, чтобы защититься от мошеннических операций.

Verified By Visa – протокол 3D-Secure реализованный МПС Visa для своих карт.

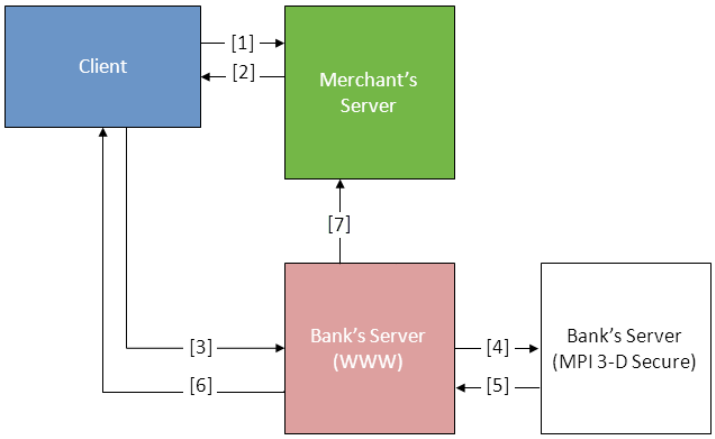
SecureCode – протокол 3D-Secure реализованный МПС MasterCard для своих карт.

МИР Accept – протокол 3D-Secure реализованный НПС МИР для своих карт.

PCI DSS – стандарт безопасности использования, хранения и передачи карточных клиентских данных (Payment Card Industry Data Security Standard). Стандарт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платёжных карт.

Описание порядка обработки 3D-Secure запроса

Ниже описан общий порядок работы системы при осуществлении платежа с использованием схемы 3D-Secure



1 **Клиент магазина оформляет заказ и нажимает кнопку "Оплатить" на странице магазина**

- производится формирование данных с параметрами платежа (*шаг 1 схемы*)

2 **Клиенту передается форма с данными заказа и производится перевод на платежную страницу, находящуюся на сервере банка**

- производится передача данных платежной транзакции, подготовленной магазином через браузер клиента на платежную страницу, находящуюся на сервере банка *(шаг 2 схемы)*

3 **Клиент вводит данные своей карты для проведения авторизации платежной транзакции**

- данные карты пользователя передаются серверу банка (*шаг 3 схемы)*
- Клиент должен обеспечить ввод следующих данных:
  - Номер карты (PAN) – **обязательно**
  - Дата действия карты (Expiry Date) – **обязательно**
  - Секретный код карты (CVV2/CVC2) – **если используется**
  - Секретный код сессии – **обязательно**
  - Имя, фамилию, адрес электронной почты, номер телефона, страну, город, почтовый адрес – **если платежной странице переданы соответствующие параметры**

4 **Производится проверка карты на возможность проведения 3D-Secure аутентификации, после чего данные транзакции передаются серверу MPI 3D-Secure**

5 **После получения результатов проверки 3D-Secure проводится авторизация платежной транзакции посредством передачи данных в МПС и далее в банк эмитент**

6 **По окончании процесса авторизации клиент получает ответ от сервера банка и данные транзакции, подписанные банком**

- Сервер банка передает на браузер клиента результаты авторизации запроса *(шаг 6 схемы)*
- В состав результатов авторизации включены данные транзакции, код завершения, электронная цифровая подпись банка

7 **Так же после завершения сессии с клиентом, банк отправляет магазину уведомление о совершении транзакции по e-mail**

Таблица «Общий порядок обработки запроса 3-D Secure»

Описание процесса подключения интернет-магазина

1 **Получение тестовых параметров для доступа к тестовой среде банка**

- Получение файла с тестовыми настройками для подключения к системе банка. Файл в формате word с перечнем всех необходимых для подключения параметров, предоставляемый техническим специалистом банка.

2 **Добавление вызова платежной страницы банка**

- На последнем шаге формирования заказа на сайте интернет-магазина добавляется форма вызова методом POST платежной страницы банка (*описание на странице 6*)
- Добавьте полученные параметры интернет-магазина в указанные изменяемые поля
- На данной странице так же должны быть размещены сведения о платеже не отличающиеся от передаваемых на платежную страницу, без дополнительных комиссий, наценок и т.д.

3 **Проверка доступа в онлайн консоль просмотра платежей**

- По полученным из файла с тестовыми настройками параметрам для входа логин/пароль, производится вход в консоль просмотра платежей
- В случае возникновения проблем с доступом производится обращение к техническим специалистам банка по предоставленным контактам с описанием проблемы

4 **Проведение тестовых транзакций**

- В файле с тестовыми параметрами есть 3 карты для каждой из подключаемых платежных систем (Visa, MasterCard, МИР)
- Производится последовательный ввод карточных данных и проведение тестовых транзакций.
- После проведения операций производится проверка сформированных транзакций и их статуса через онлайн консоль просмотра платежей
- Так же если банку сообщен электронный адрес для уведомлений то производится проверка получения писем с информацией о платеже

5 **Настройка интернет-магазина для боевых операций**

- После успешного завершения всех тестов, производится замена тестовых параметров интернет-магазина на боевые в форме вызова платежной страницы банка
- С помощью любой боевой карты проводятся платежи в боевых системах для окончательной проверки работоспособности интеграции
- Производится проверка статуса оплаты в онлайн консоли просмотра платежей
- При необходимости совершенные платежи можно отменить непосредственно через онлайн консоль

6

-

Описание формы вызова платежной страницы банка

Запрос магазина на проведение авторизации транзакции

Запрос магазина формируется путем передачи методом POST параметров, указанных в таблице на платежную страницу банка

Поле	Описание	Источник
PurchaseAmt	Сумма заказа, передается в формате: NNNNNNNNN.NN (разделитель: десятичная точка, два знака после запятой, сумма в валюте сделки по договору). Указывается только если платеж в рублях, для другой валюты в это поле проставляется ноль.	Магазин
PurchaseDesc	Уникальный дескриптор заказа (не более 40 символов)	Магазин
CountryCode	Код страны продавца ISO (должен быть установлен **всегда** **643**)	Банк-эквайер
CurrencyCode	Код валюты сделки ISO (должен быть установлен **всегда** **643**)	Банк-эквайер
MerchantName	Имя магазина (не более 25 символов)	Банк-эквайер
MerchantURL	URL сервера магазина	Магазин
MerchantCity	Город магазина (большими буквами на английском языке, например **MOSCOW**)	Банк-эквайер
MerchantID	Идентификатор магазина, передается в формате 00000NNNNNNNNNN-NNNNNNNN (00000**MerchantID-TerminalID**)	Банк-эквайер
SuccessURL	URL ресурса, куда будет перенаправлен клиент в случае успешного платежа	Магазин
FailURL	URL ресурса, куда будет перенаправлен клиент в случае неуспешного платежа	Магазин
Language	Задает язык интерфейса платежной системы на сайте банка по умолчанию, с возможностью смены клиентом (интерфейсом предусмотрены значения: ru-русский, en-английский)	Магазин
CardholderName	Если передается “Y”, то на платежной странице появляется поле для ввода имени и фамилии владельца карты	Магазин
Email	Если передается “Y”, то на платежной странице появляется поле для ввода адреса электронной почты владельца карты	Магазин
Phone	Если передается “Y”, то на платежной странице появляется поле для ввода телефона владельца карты	Магазин
Ext1	Дополнительные параметры, используются для передачи дополнительной информации о заказе для взаимодействия с системой Атол ОНЛАЙН по выполнению требований 54-ФЗ по предоставлению электронного чека покупателю и отправке данных о платеже в ФНС	Магазин
Ext2		Магазин
Примечание:	1. **Синим** шрифтом указаны обязательные параметры 2. Обычным шрифтом указаны необязательные параметры 3. Параметр **PurchaseDesc должен являться уникальным для каждого платежа**. Если по данному номеру заказа уже был успешный платеж, то повторно оплатить с этим же номером нельзя. 4. Параметр MerchantID здесь имеет немного другое значение, нежели обычный **MerchantID**, присвоенный Вашему интернет-магазину. Здесь он состоит из **MerchantID** и **TerminalID**, которые будут выданы вместе с остальными настройками сотрудниками банка.	

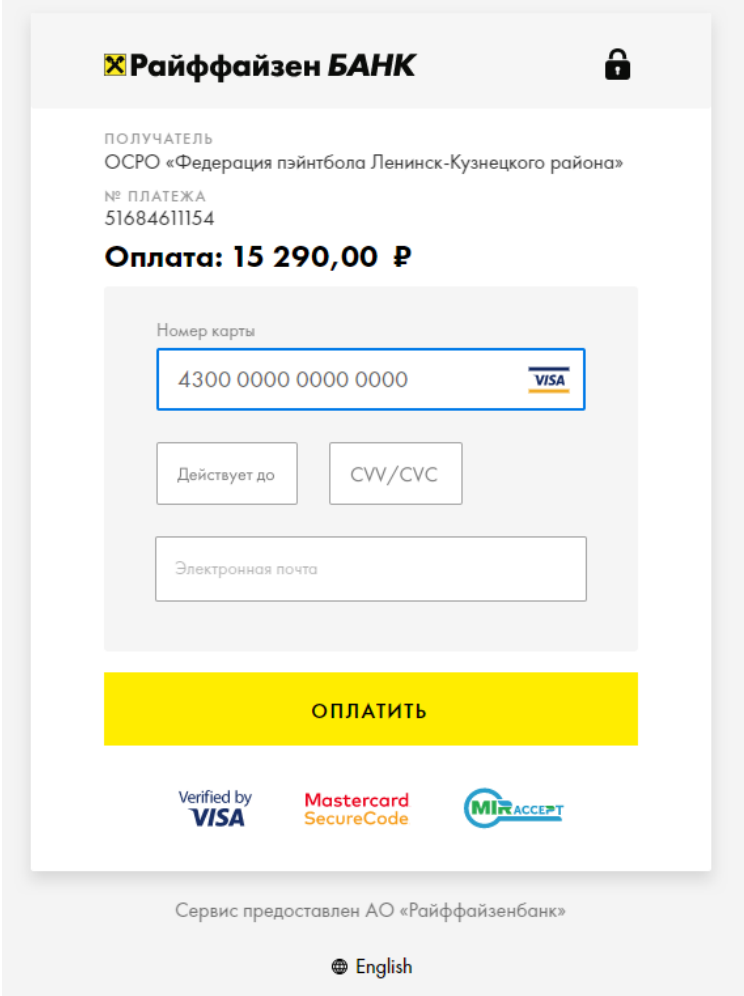
Пример формирования запроса на платежную страницу банка

Запрос магазина формируется путем передачи методом POST параметров, по описанию выше

Стандартный запрос

```
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<title>Pay</title>
<meta content="text/html; charset=UTF-8" http-equiv="Content-Type" />
</head>
<body style="color: #336699 ; font-family: Verdana">
<form action="https://e-commerce.raiffeisen.ru/vsmc3ds_test/pay_new/3dsproxy_init.jsp"
method=POST name="frm">
<input name="PurchaseDesc" type="hidden" value="TestPurchase1" />
<input name="PurchaseAmt" type="hidden" value="10" />
<input name="CountryCode" type="hidden" value="643" />
<input name="CurrencyCode" type="hidden" value="643" />
<input name="MerchantName" type="hidden" value="TestMerchant" />
<input name="MerchantURL" type="hidden" value="https://www.merchantURL.ru" />
<input name="MerchantCity" type="hidden" value="MOSCOW" />
<input name="MerchantID" type="hidden" value="000001680997001-80997001" />
<input type="submit" value="Pay" />
</form>
</body>
</html>
```

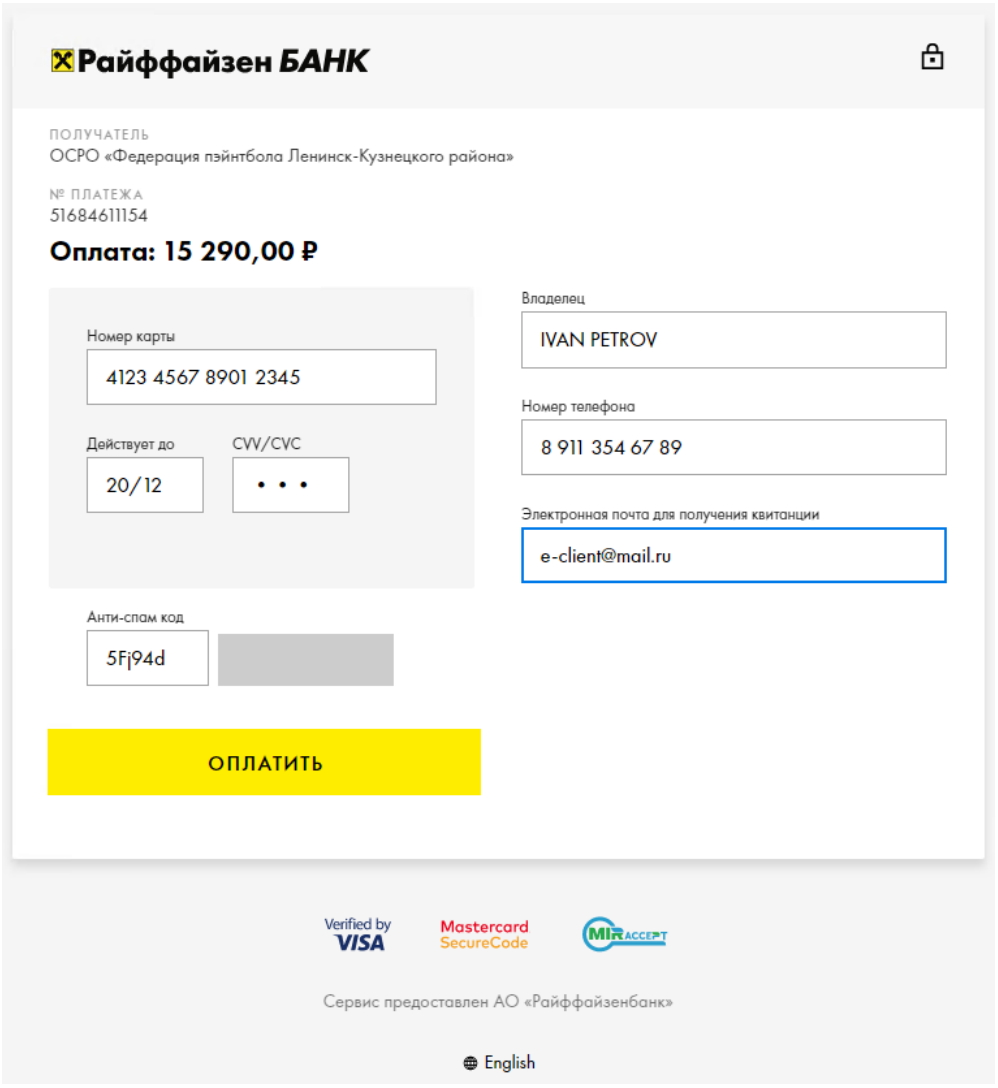
Результатом выполнения подобного запроса будет переадресация клиента на платежную страницу Банка для ввода карточных данных вида:



Запрос с дополнительными параметрами

```
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<title>Pay</title>
<meta content="text/html; charset=UTF-8" http-equiv="Content-Type" />
</head>
<body style="color: #336699 ; font-family: Verdana">
<form action="https://e-commerce.raiffeisen.ru/vsmc3ds/pay_new/3dsproxy_init.jsp"
method=POST name="frm">
<input name="PurchaseDesc" type="hidden" value="TestPurchase1" />
<input name="PurchaseAmt" type="hidden" value="10" />
<input name="CountryCode" type="hidden" value="643" />
<input name="CurrencyCode" type="hidden" value="643" />
<input name="MerchantName" type="hidden" value="TestMerchant" />
<input name="MerchantURL" type="hidden" value="https://www.merchantURL.ru" />
<input name="MerchantCity" type="hidden" value="MOSCOW" />
<input name="MerchantID" type="hidden" value="000001680997001-80997001" />
<input name="CardholderName" type="hidden" value="Y" />
<input name="Email" type="hidden" value="Y" />
<input name="Phone" type="hidden" value="Y" />
<input type="submit" value="Payment" />
</form>
</body>
</html>
```

Результатом выполнения подобного запроса будет переадресация клиента на платежную страницу банка для ввода карточных данных вида:



Описание уведомлений о платеже, доставляемых по e-mail

Формат сообщения

Текст письма содержит строку, содержащую данные, разделенные между собой символом “|” (вертикальная черта). Описание параметров представлено ниже. Для подключения данного сервиса и занесения адреса электронной почты в систему Банка, необходимо обратиться по адресу ecom_support@raiffeisen.ru

Дата совершения операции	MM/DD/YYYY	MM – месяц (1-12) DD – день (1-31) YYYY – год
Время совершения операции	HH:MM:SS	HH – час (0-23) MM – минуты (0-59) SS – секунды (0-59)
Сумма операции	NNNNNNNNN.NN	Сумма операции с разделителем
Код Валюты (числовой)	NNN	Числовой код валюты ISO
Код завершения	S	“Y” – операция успешно завершена “N” – транзакция отклонена
Описание кода	(не более 40 символов)	Код авторизации присвоенный банком эмитентом при подтверждении операции. С данным кодом клиент может обратиться в свой банк для дополнительной информации, если это необходимо
Номер заказа	(не более 40 символов)	Уникальный идентификатор платежа передаваемый интернет-магазином на платежную страницу банка

Пример отправленного уведомления:

01/23/2018|15:10:27|2717.88|643|Y|601707|4KwWYj7FKh

Перечень и описание ошибок, отображаемых на платёжной странице

11010	Отсутствует сессионный атрибут ImgCode	Не отобразился антиспам-код в браузере клиента (отключен JavaScript)
11011	Отсутствует сессионный атрибут UsrCode	Не введен антиспам-код
11012	Значения атрибутов ImgCode и UsrCode не равны	Неверно введён антиспам-код
11020	Платеж не прошел стадию верификации	Отказ по системе фрод-мониторинга, превышен один или несколько лимитов
11030	В результатах 3D-Secure авторизации отсутствует параметр	Ошибка браузера клиента, либо ACS эмитента
11031	В результатах 3D-Secure авторизации отсутствует параметр	Ошибка браузера клиента, либо ACS эмитента
11032	В результатах 3D-Secure авторизации отсутствует параметр	Ошибка браузера клиента, либо ACS эмитента
11040	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11041	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11042	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11043	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11044	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11045	В результатах авторизации запроса процессинговым центром отсутствует параметр	Внутренняя ошибка процессинга
11051	Отсутствует параметр MerchantID	Обязательный параметр
11052	Отсутствует параметр PurchaseDesc	Обязательный параметр
11053	Отсутствует параметр PurchaseAmt	Обязательный параметр
11054	Отсутствует параметр CurrencyCode	Обязательный параметр
11055	Отсутствует параметр CardNumber	Не введен номер карты
11056	Отсутствует параметр CardExpDate	Не введен срок действия карты
11060	Отсутствуют обязательные параметры транзакции	Отсутствуют обязательные поля в платежном запросе от ТСП
11070	Среди входящих параметров отсутствуют обязательные параметры для проведения транзакции	Переданы не все обязательные параметры от магазина или ошибка в формате
11071	Ошибка ввода данных значения входящего параметра CardNumber	Введенный неверный номер карты
9801	Отсутствует один или несколько обязательных параметров для проведения транзакции	Обрыв HTTPS сессии
9802	Отсутствует один или несколько обязательных параметров для валидации	Один или несколько параметров не были возвращены эмитентом после аутентификации