Инструкция пользователя

Gateline

Simple API

Оглавление

1. Общая информация

SimpleAPI – упращенный программный интерфейс Платежного шлюза GateLine (далее – Шлюз), который позволяет торгово-сервисным предприятиям (далее - Организация) за достаточно короткий срок провести интеграцию Интернет-магазина со Шлюзом.

При этом, специалисту Организации для подключения к ПШ GateLine достаточно знать основы HTML. При отправке запросов через SimpleAPI в Шлюз не требуется подписание запроса SSL сертификатом, перенаправление плательщика на платежную форму Шлюза для выбора инструментов платежа и ввода карточных данных происходит автоматически.

2. Работа через SimpleAPI

2.1. Отправка запросов

Оплата инициируется отправкой запроса на специальный URL в ПШ:

- Тестовая среда: https://simpleapi.sandbox.gateline.net:18610/.
- Тип кодировки: application/x-www-form-urlencoded.
- Метод формы: POST

2.2. Подписание запроса

Сумма вычисляется с паролем сайта. Пароль сайта предоставляется Организации после регистрации сайта Организации в Шлюзе GateLine.

Составляющие подписи разделяются символом ";" (точка с запятой).

Пример формирования подписи:

HMAC_SHA1("param1=value1;param2=value2", mypassword)

где mypassword - пароль сайта.

Подпись передается параметром checksum в этой же форме.

2.3. Проверка контрольной суммы

Контрольная сумма передается как параметр checksum.

Контрольная сумма вычисляется как HMAC-SHA1-сумма строки, составленной из пар "имя=значение", отсортированных по имени в алфавитном порядке. Пары разделяются символом ";" (точка с запятой), в качестве пароля для вычисления контрольной суммы используется пароль сайта.

Параметры, которые присутствовали в изначальном URL, обрабатываются при вычислении checksum на общих основаниях.

2.4. Запрос на проведение оплаты (POST/pay)

Формат запроса:

https://simpleapi.sandbox.gateline.net:18610/pay

Параметры запроса:

Имя	Описание	Пример
	Сумма операции	
	Описание заказа	Товар
	Идентификатор сайта Организации в ПШ	
	E-mail клиента	
	Идентификатор заказа в системе клиента	
	Язык платежной формы en, ru	
	Подпись запроса	

* - опциональные поля

При успешной обработке запроса плательщик автоматически перенаправляется (HTTP 302 Redirect) на платежную форму Шлюза GateLine. В случае ошибок клиенту будет сгенерирована страница с описанием ошибок.

2.5. Фискализация покупок

В рамках SimpleAPI Магазин может опционально воспользоваться сервисом ПШ GateLine по автоматической фискализации данной покупки путем направления необходимой информации в онлайн-кассу, открытой в сервисе OrangeData и соответственно ОФД, подключенному к OrangeData. Фискализация через SimpleAPI производится только на всю сумму заказа одной позицией в чеке.

3. Обработка результатов оплаты

При работе через платежную форму ПШ Магазин получает информацию о результате проведения оплаты одним из следующих способов:

1. Переадресацией (Редирект) плательщика на определенные страницы Интернет-магазина с определенными параметрами.
2. Получением уведомления от ПШ.

Несмотря на то, что параметры редиректа содержат всю необходимую информацию о результате проведения операции, использовать их рекомендуется только для отображения пользователю специфических страниц, например, сообщений об ошибках.

Уведомления доставляется более безопасным способом, чем параметры редиректа. Кроме этого, уведомление будет доставлено даже в том случае, если операция выполнилась успешно, а пользователь по какой-либо причине не дождался результата или не проследовал по перенаправлению.

3.1. Обработка ошибок

Сообщения об ошибках отображаются плательщику на стороне ПШ. Возможные ошибки:

- Forbidden – режим SimpleAPI не разрешен для данного сайта.
- Amount/Description/Site required – не все обязательные поля заполнены.

4. Организация ордеров и операций

4.1. Общая информация

В отличие от традиционной схемы транзакций, когда каждая операция содержит в себе все относящиеся к ней данные, в системе реализована схема заказов и связанных с ними операций.

Заказ выступает хранилищем информации о клиенте: номер карты, имя держателя карты, биллинг-адрес. Кроме этого, заказ несет информацию о текущем состоянии процессинга, дате проведения последней операции и т.д.

4.2. Статусы ордера

По статусу ордера можно судить о текущем состоянии заказа.

Статус	Расшифровка	Возможные операции
	Ордер создан, но процессинг еще не начался.	–
	Выполняется процессинг операции	–
	Проведена успешная авторизация (блокировка суммы)	
	Запущена процедура аутентификации через 3D Secure	–
	Проведена успешная операция settle (списание суммы)	
	Авторизация отменена	
	Произведен возврат средств	
	Авторизация отклонена (не удалось заблокировать сумму)	

	В процессе выполнения операции произошла ошибка, возможно, требуется вмешательство службы поддержки.	–
	Был произведен чарджбек (сумма возвращена по инициативе клиента).	–
	Авторизация была отклонена в соответствии с правилами сайта	–

4.3. Статусы операций

По статусу операции можно судить о результате ее выполнения.

Значение	Описание
	Операция проведена успешно.
	Был получен ответ от банка, в котором указано, что операция не завершилась удачно по какойлибо причине (например, произошел отказ в авторизации).
	Возникла проблема, при которой ответ от банка не был получен (например, из-за ошибки подключения к банку или внутренней ошибки системы).

5. Уведомления

5.1. Общая информация

Уведомления предназначены для асинхронной передачи информации от платежного шлюза к магазину.

По умолчанию доставляются после каждой успешной операции, проведенной через пользовательский бэкофис или через API.

5.2. Требования к сайту, принимающему уведомления

Уведомления отправляются по протоколу HTTPS в одном из форматов по выбору:

- XML (Content-Type: text/xml);
- HTML (Content-Type: application/x-www-form-urlencoded).

На сайте партнера на указанном URL должна быть настроена базовая HTTP-аутентификация с реквизитами доступа, соответствующими тем, что указаны в свойствах сайта. Если аутентификация не настроена, уведомление не доставляется.

Перед отправкой уведомления отправляется запрос методом GET для проверки наличия базовой HTTP-аутентификации, после отправляется запрос отправляется методом POST на URL, указанный в свойстве сайта «URL для доставки уведомлений».

5.3. Контроль доставки уведомления

Если сайт принял и обработал уведомление он должен сформировать ответ с HTTP-статусом 200, тело ответа должно состоять из слова «SUCCESS» латиницей в верхнем регистре. Окружающие ответ пробельные символы игнорируются. В этом случае система будет считать, что уведомление доставлено и обработано.

Если первое уведомление не было доставлено, система производит еще 3 попытки через

определенные промежутки времени. Если все 4 попытки доставить уведомление оказались неудачными, система не предпринимает никаких дополнительных действий. Список ошибок доставки уведомлений можно посмотреть в разделе «Журналы -> Ошибки уведомлений».

5.4. Формат уведомления

Формат сообщения соответствует стандартному формату ответа системы. Набор полей зависит от типа операции, на которую передается уведомления и идентичен набору полей, который передается в синхронном ответе на операцию в API

5.5. Верификация настроек уведомлений

Уведомления доставляются только после подтверждения ссылок на стороне тех. поддержки шлюза. После каждого изменения настроек уведомлений требуется повторное подтверждение.

Для продуктивной среды необходимо заранее сообщать URL и ip адрес на который планируется получать уведомления, т.к. адреса добавляются в списки разрешенных на стороне шлюза Gateline.

Тестовое уведомление (xml):

```
<?xml version="1.0" encoding="utf-8"?>
<operation>
  <test>
    <message>test</message>
  </test>
</operation>
```

Тестовое уведомление (urlencoded):

operation=test&message=test

Операции на которые доставляются уведомления: confirmation, authorize, reversal, settle, refund:

Поля ответа:

Имя	Описание	Пример
	Идентификатор заказа в системе клиента	
	Описание результата	
	Уникальный идентификатор заказа в системе	
	Тип провайдера	
	Статус операции	
	Дата выполнения запроса	
	Сумма *Используется в confirmation*	
	Описание заказа *Используется в confirmation*	Товар (#123456789)
	Метод оплаты принимает значение: – оплата выполнена с использованием банковской карты; – оплаты выполнена через СБП	
	Код ответа *Используется в authorize*	

* – Опциональное поле

confirmation

```
<operation>
 <confirmation>
  <amount>500.00</amount>
  <description>TEST-PAY</description>
  <merchant_order_id>12345</merchant_order_id>
  <provider>card</provider>
 </confirmation>
</operation>
```

authorize

```
<operation>
 <authorize>
  <authcode>XXX09X</authcode>
  <descriptor>TEST-TERM</descriptor>
  <merchant_order_id>12345</merchant_order_id>
  <message>Success</message>
  <order_id> rfm50cd3xqa419jp2kn0u2ehm0bzr9rd1</order_id>
  <provider>card</provider>
  <responsecode>000</responsecode>
  <status>success</status>
  <time>2000-01-01 00:00:01</time>
 </authorize>
</operation>
```

settle

```
<operation>
 <settle>
  <merchant_order_id>12345</merchant_order_id>
  <message>Success</message>
  <order_id>rfm50cd3xqa419jp2kn0u2ehm0bzr9rd1</order_id>
  <provider>card</provider>
  <status>success</status>
  <time>2000-01-01 00:00:03</time>
 </settle>
</operation>
```

6. Обработка редиректов

6.1. Общая информация

После некоторых операций пользователь, в зависимости от статуса операции, перенаправляется на один из двух установленных в настройках редиректов URL.

Если в сайте установлено свойство «Передавать параметры при редиректе», к этому адресу добавляется ряд параметров, которые указывают на результат проведения операции, статус, привязку к ордеру и т.д.

Если установленный в сайте URL уже содержит GET-параметры, они будут сохранены при редиректе. Если имя одного из этих параметров совпадает с тем, которое устанавливает система при редиректе, будет возвращен только системный параметр.

URL может быть установлен двумя способами:

- Свойства сайта «URL возврата при успешной операции» и «URL возврата при ошибке». Используются по умолчанию.

- Параметры запроса в API return_success_url и return_failure_url. Эти параметры являются опциональными, и могут перекрывать значения, установленные в сайте.

6.2. Список передаваемых параметров

Название	Описание	Пример
	Описание результата	
	Статус операции	
	ID ордера	
	Идентификатор заказа в системе клиента	
	Код ошибки	

* - поле может не передаваться, если установлен статус error

** - поле передается только для статуса error

6.3. Расшифровка статуса

Поле status может принимать следующие значения:

Значение	Описание
	Операция проведена успешно
	Операция была инициирована, но не завершилась удачно по какой-либо причине.
	Возникла проблема, которая не позволяет запустить проведение операции.

Дополнительная информация о результате операции содержится в поле message.

7. Клиринг

7.1. Автоматический режим

Автоматический клиринг это когда система автоматически проводит операцию settle для каждого ордера.

Клиринг проводится через некоторое время после авторизации. Система позволяет установить время задержки для каждого сайта отдельно, по умолчанию оно составляет 6 часов.

Если блокировка была снята (операция reversal) до того, как был произведен клиринг, операция списания проведена не будет.

8. Проведение тестовых транзакций

8.1. Общая информация

Тестовые транзакции проводятся только через тестовый терминал. Доступ к тестовому терминалу можно получить через службу поддержки. Адрес тестовой среды - https://simpleapi.sandbox.gateline.net:18610/

Номер карты для проведения успешных тестовых транзакций: 5276440065421319. Дата истечения, CVV/CVC код, и прочие требуемые параметры допускаются любые, если они переданы в правильном формате.

Поведением тестового терминала можно управлять, передавая особые метки в поле запроса cardholder.

Поддерживаемые варианты:

Значение поля	Поведение терминала
	Терминал отклоняет транзакцию
decline 2D but not 3D	Терминал отклоняет обычную авторизацию, но пропускает с 3D Secure (используется для тестирования механизма try3d)
	Терминал отклоняет операцию следующую после authorize
	Терминал отклоняет операцию settle
	Терминал генерирует ошибку при проведении операции authorize
	Терминал генерирует ошибку при проведении операций следующей после authorize
	Терминал генерирует ошибку о недостаточности средств на карте
	Эмулируется таймаут при подключении к банку
	Эмулируется ошибка на стороне банка

8.2. Использование 3D Secure

Тестовый терминал поддерживает возможность провести транзакцию с использованием 3D Secure. Указывая специальные значения в полях даты истечения карты (месяц и год), можно эмулировать обработку карт с разной степенью поддержки 3Ds.

Эти значения можно как передавать в API-запросах, так и указывать на платежной странице. Они будут обрабатываться специальным образом только в том случае, если запрошен процессинг с 3-D Secure (запрошена операция authorize3d или передан флаг force3d/try3d соответственно).

Тестовые карты:

MIR: 2200 0000 0000 0053 cvv: 111

Месяц	Год	Ожидаемое поведение
/05	***2	
/	***0	