Протокол EACQ Мультирасчеты

13.11.2025

БИЗНЕС

Версия документа: 1.8

Оглавление

История изменений

Версия	Описание	Дата
1.0	Документ создан	09.08.2024
1.1	Обновлена схема проведения платежа и список статусов Обновлена обязательность параметров CreateDealWithType и DealId	21.03.2025
1.2	Обновлен параметр LevelOfConfidence Добавлен блок ответа в методе Init	19.05.2025
1.3	Обновлено описание параметра Amount в методе Init	14.08.2025
1.4	Обновлено примечание по блоку DATA в методе Init	21.08.2025
1.5	Обновлено описание для тестовой карты ***0831	04.09.2025
1.6	Обновлена Таблица 4.2.1	11.09.2025
1.7	Обновлен URL в примере ответа метода Init	18.09.2025
1.8	Обновлен сценарий рекуррентного платежа по одностадийной схеме	13.11.2025

Термины и сокращения

Термин	Определение
Сайт (Приложение, Площадка)	Интернет-ресурс, предоставляющий возможность размещения Продавцами Объявлений о продаже Товаров, а также предоставляющий Покупателям возможность поиска, просмотра предложений Продавцов с целью последующего приобретения Товара с использованием Сервиса.
Продавец	Зарегистрированный пользователь Сайта (Приложения), размещающий там Объявления с предложением заключить Сделку в отношении Товара с использованием Сервиса
Покупатель	Зарегистрированный пользователь Сайта (Приложения), осуществляющий просмотр размещенного Продавцом Объявления, взаимодействие с Продавцом в отношении Товара, заключивший с Продавцом Сделку с использованием Сервиса.
PCI DSS	Стандарт безопасности данных индустрии платёжных карт. Стандарт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платёжных карт. Данные 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
3-D Secure	Протокол, который используется как дополнительный уровень безопасности для онлайн-кредитных и дебетовых карт. 3-D Secure добавляет ещё один шаг аутентификации для онлайн-платежей
Терминал	Точка приема платежей Площадки (в общем случае привязывается к сайту, на котором осуществляется прием платежей) Далее в этой документации описан протокол для терминала мерчанта

Рекомендации при интеграции

Ниже мы расписали несколько рекомендаций, которые необходимо соблюдать при интеграции с MAPI через фронтенд сайта мерчанта, а именно:

1.1. Наиболее безопасный способ передачи данных от мерчанта в MAPI — прямая интеграция бэкенда мерчанта с бэкендом Т-Банк Бизнес. В этом случае злоумышленник сможет перехватить запрос только, если окажется в локальной сети мерчанта;

1.2. Получение нотификаций:

- **По e-mail:** на указанную почту придет письмо при переходе платежа в статус «CONFIRMED»;
- **По http:** MAPI будет отправлять POST-запрос при каждом изменении статуса платежа на URL, указанный в настройках терминала.

2.0. Вызов метода GetState, который возвращает основные параметры и текущий статус платежа

1. Параметры приема платежей

Параметры приема платежей настраиваются отдельно на каждый терминал.

Таблица 1.1.Параметры приема платежей

Название параметра	Формат	Описание
TerminalKey	20 символов (чувствительно к регистру)	Уникальный символьный ключ терминала. Устанавливается банком
Success URL	250 символов (чувствительно к регистру)	URL на веб-сайте Площадки, куда будет переведен покупатель в случае успешной оплаты *
Fail URL	250 символов (чувствительно к регистру)	URL на веб-сайте Площадки, куда будет переведен покупатель в случае неуспешной оплаты *
Success Add Card URL	250 символов (чувствительно к регистру)	URL на веб-сайте Площадки, куда будет переведен покупатель после успешной привязки карты *
Fail Add Card URL	250 символов (чувствительно к регистру)	URL на веб-сайте Площадки, куда будет переведен покупатель после неуспешной привязки карты *
Notification URL	250 символов (чувствительно к регистру)	URL на веб-сайте Площадки, куда будет отправлен POST запрос о статусе выполнения вызываемых методов. Только для методов Authorize, FinishAuthorize, Confirm, Cancel
Валюта терминала	3 символа	Валюта, в которой будут происходить списания по данному терминалу, если иное не передано в запросе
Активность терминала	Рабочий / Неактивный / Тестовый	Определяет режим работы данного терминала
Password	20 символов (чувствительно к регистру)	Используется для подписи запросов/ответов. Является секретной информацией, известной только Площадке и банку. Пароль находится в личном кабинете мерчанта https://business.tbank.ru
Отправлять нотификацию на Authorize	Да/Нет	Определяет, будет ли отправлена нотификация на выполнение метода Authorize (по умолчанию нет)

Отправлять нотификацию на FinishAuthorize	Да/Нет	Определяет, будет ли отправлена нотификация на выполнение метода FinishAuthorize (по умолчанию да)
Отправлять нотификацию на Completed	Да/Нет	Определяет, будет ли отправлена нотификация на выполнение метода AttachCard (по умолчанию Да)
Отправлять нотификацию на Reversed	Да/Нет	Определяет, будет ли отправлена нотификация на выполнение метода Cancel (по умолчанию Да)

***** в URL можно указать необходимые параметры в виде ${<параметр>}, которые будут переданы на URL методом GET.

Таблица 1.2. Параметры Success URL и Fail URL

Наименование	Описание
Success	Возможные значения: – true – запрос завершился успешно; – false – запрос не завершился.
ErrorCode	Код ошибки (0 – если ошибки не было)
OrderId	Номер заказа в системе Площадки
Message	Заголовок ошибки (заполняется только в случае ошибки)
Details	Детальное описание ошибки (заполняется только в случае ошибки)

Например:
http://tcsbank.ru/success.html?Success=${Success}&ErrorCode=${ErrorCode}&OrderId=${OrderId}&Mes sage=${Message}&Details=${Details}

2. Методы приема платежей

2.1. Общая информация

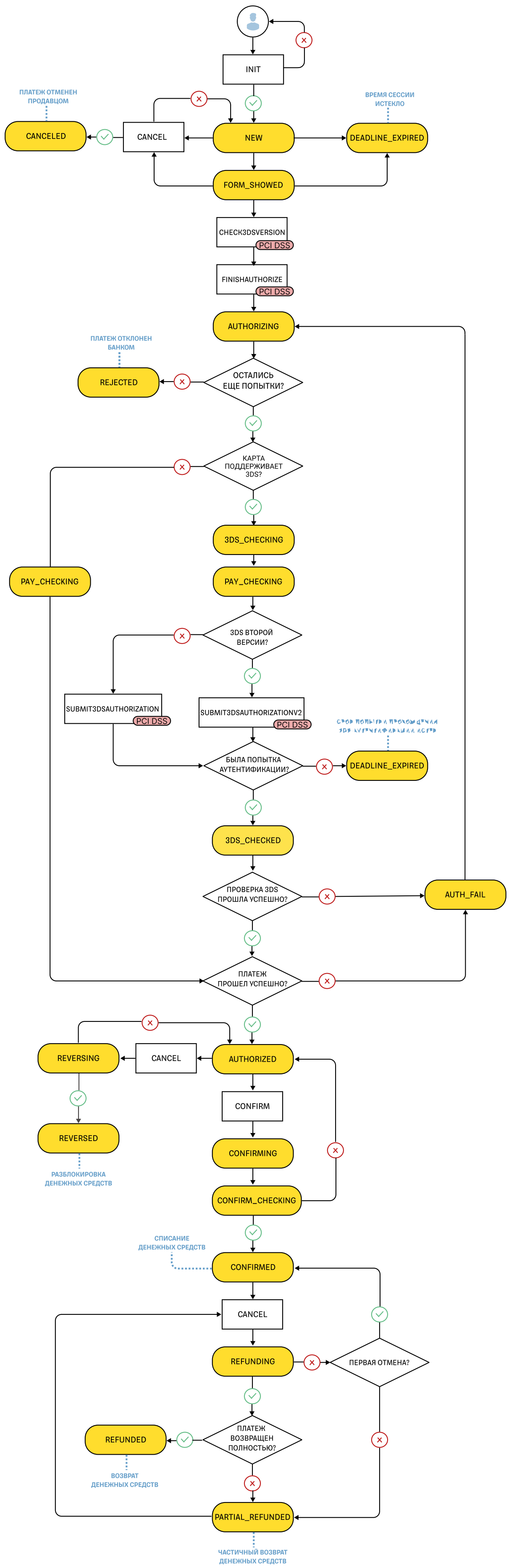
Прием платежей осуществляется вызовом методов с передачей параметров методом POST в формате JSON. Все методы и передаваемые параметры являются чувствительными к регистру.
Для POST запроса в заголовке должен присутствовать **Content-Type: application/json.**

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/

Боевой URL: https://securepay.tinkoff.ru/v2/
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала.

2.2. Схема проведения платежа

На схеме показаны статусы платежа и возможные методы, которые могут быть вызваны, если платеж находится в данном статусе.


INIT
ПЛАТЕЖ ОТМЕНЕН ПРОДАВЦОМ
CANCELED
CANCEL
NEW
ВРЕМЯ СЕССИИ ИСТЕКЛО
DEADLINE_EXPIRED
FORM_SHOWED
CHECK3DSVERSION
PCI DSS
FINISHAUTHORIZE
PCI DSS
AUTHORIZING
ПЛАТЕЖ ОТКЛОНЕН БАНКОМ
REJECTED
ОСТАЛИСЬ ЕЩЕ ПОПЫТКИ?
КАРТА ПОДДЕРЖИВАЕТ 3DS?
3DS_CHECKING
PAY_CHECKING
PAY_CHECKING
3DS ВТОРОЙ ВЕРСИИ?
SUBMIT3DSAUTHORIZATION
PCI DSS
SUBMIT3DSAUTHORIZATIONV2
PCI DSS
БЫЛА ПОПЫТКА АУТЕНТИФИКАЦИИ?
DEADLINE_EXPIRED
3DS_CHECKED
ПРОВЕРКА 3DS ПРОШЛА УСПЕШНО?
AUTH_FAIL
ПЛАТЕЖ ПРОШЕЛ УСПЕШНО?
REVERSING
CANCEL
AUTHORIZED
REVERSED
РАЗБЛОКИРОВКА ДЕНЕЖНЫХ СРЕДСТВ
CONFIRM
CONFIRMING
CONFIRM_CHECKING
СПИСАНИЕ ДЕНЕЖНЫХ СРЕДСТВ
CONFIRMED
CANCEL
REFUNDING
ПЕРВАЯ ОТМЕНА?
REFUNDED
ПЛАТЕЖ ВОЗВРАЩЕН ПОЛНОСТЬЮ?
ВОЗВРАТ ДЕНЕЖНЫХ СРЕДСТВ
PARTIAL_REFUNDED
ЧАСТИЧНЫЙ ВОЗВРАТ ДЕНЕЖНЫХ СРЕДСТВ

Возможные статусы платежа:

- **NEW** — MAPI получил запрос Init. После этого он создает новый платеж со статусом NEW и возвращает его идентификатор в параметре PaymentId, а также ссылку на платежную форму в параметре PaymentURL.
- **FORM_SHOWED** — Мерчант перенаправил клиента на страницу платежной формы PaymentURL, и страница загрузилась у клиента в браузере.
- **AUTHORIZING** — Платеж обрабатывается MAPI и платежной системой.
- **3DS_CHECKING** — Платеж проходит проверку 3D-Secure.
- **3DS_CHECKED** — Платеж успешно прошел проверку 3D-Secure.
- **AUTHORIZED** — Платеж авторизован, деньги заблокированы на карте клиента.
- **PAY_CHECKING** — Платеж обрабатывается. В течение 60 минут статус сменится на конечный.
- **CONFIRMING** — Подтверждение платежа обрабатывается MAPI и платежной системой.
- **CONFIRMED** — Платеж подтвержден, деньги списаны с карты клиента.
- **REVERSING** — Мерчант запросил отмену авторизованного, но еще неподтвержденного платежа. Возврат обрабатывается MAPI и платежной системой.
- **PARTIAL_REVERSED** — Частичный возврат по авторизованному платежу завершился успешно.
- **REVERSED** — Полный возврат по авторизованному платежу завершился успешно.
- **REFUNDING** — Мерчант запросил отмену подтвержденного платежа. Возврат обрабатывается MAPI и платежной системой.
- **PARTIAL_REFUNDED** — Частичный возврат по подтвержденному платежу завершился успешно.
- **REFUNDED** — Полный возврат по подтвержденному платежу завершился успешно.
- **CANCELED** — Мерчант отменил платеж.
- **DEADLINE_EXPIRED** — 1. Клиент не завершил платеж в срок жизни ссылки на платежную форму PaymentURL. Этот срок мерчант передает в методе Init в параметре RedirectDueDate.
- 2. Платеж не прошел проверку 3D-Secure в срок.
- **REJECTED** — Банк отклонил платеж.

AUTH_FAIL — Платеж завершился ошибкой или не прошел проверку 3D-Secure.

2.3. Метод Init

Метод для схем PCI DSS \ Без PCI DSS

Описание: Инициирует платежную сессию.
Примечание: При оплате по СБП не требуется использовать метод Confirm. Оплата происходит в рамках одного метода **Init**.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Init
Боевой URL: https://securepay.tinkoff.ru/v2/Init
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.3.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
Amount	Number	Да	Сумма в копейках. Минимальное значение: • для карточных операций — 100 (1 руб.); • для операций по СБП— 1000 (10 руб.).
OrderId	String	Да	Номер заказа в системе Площадки
Token	String	Нет***	Подпись запроса
IP	String	Нет	IP-адрес клиента
Description	String	Нет	Краткое описание
PaymentRecipientId	String	Да	Идентификатор будущего получателя выплаты (номер телефона в формате "+79606747611").
DealId	Number	Нет, если передан CreateDealWithType	Идентификатор сделки
CreateDealWithType	String	Нет, если передан DealId	Флаг о необходимости создания сделки при выполнении запроса. Вариант заполнения: NN
LevelOfConfidence	String	Нет	Уровень проверки получателя выплаты. Параметр необходим только в том случае, если его передачу потребовал отдел рисков на этапе подключения. Возможные значения: "low", "moderate", "high"

Currency	Number	Нет	Код валюты ISO 421. Если Currency передан и валюта разрешена для Площадки, транзакция будет инициирована в переданной валюте. Иначе будет использована валюта по умолчанию для данного терминала. В текущей версии допустимы только рубли - код 643
CustomerKey	String	Да, если передан Recurrent	Идентификатор покупателя в системе Площадки. Если передается и Банком разрешена автоматическая привязка карт к терминалу, то для данного покупателя будет осуществлена привязка карты. Тогда в нотификации на AUTHORIZED будет передан параметр CardId (подробнее см. 5.7. Метод GetCardList)
Recurrent	String	Для регистрации автоплатежа	Если передается и установлен в Y, то регистрирует платеж как рекуррентный. В этом случае после оплаты в нотификации на AUTHORIZED будет передан параметр RebillId для использования в методе Charge.
PayType	Enum	Нет	Определяет тип проведения платежа – двухстадийная или одностадийная оплата. – "O" - одностадийная оплата; – "T"- двухстадийная оплата
Language	String	Нет	Язык платёжной формы. ru – форма оплаты на русском языке; en – форма оплаты на английском языке. По умолчанию (если параметр не передан) - форма оплаты на русском языке
NotificationURL*	String	Нет	URL на веб-сайте Площадки, куда будет отправлен POST запрос о статусе выполнения вызываемых методов. Если параметр передан – используется его значение. Если нет – значение в настройках терминала.
SuccessURL*	String	Нет	URL на веб-сайте Площадки, куда будет переведен покупатель в случае успешной оплаты. Если параметр передан – используется его значение. Если нет – значение в настройках терминала.

FailURL*	String	Нет	URL на веб-сайте Площадки, куда будет переведен покупатель в случае неуспешной оплаты. Если параметр передан – используется его значение. Если нет – значение в настройках терминала.
RedirectDueDate	Datetime	Нет	Срок жизни ссылки или динамического QR-кода СБП (если выбран данный способ оплаты)****. Если текущая дата превышает дату, переданную в данном параметре, ссылка для оплаты или возможность платежа по QR-коду становятся недоступными и платёж выполнить нельзя. Максимальное значение: 90 дней от текущей даты. Минимальное значение: 1 минута от текущей даты. Формат даты: YYYY-MM-DDTHH24:MI:SS+GMT Пример даты: 2016-08-31T12:28:00+03:00
DATA**	Object	Нет	JSON объект, содержащий дополнительные параметры в виде “ключ”:”значение”. Данные параметры будут переданы на страницу оплаты (в случае ее кастомизации). Максимальная длина для каждого передаваемого параметра: ключ – 20 знаков; значение – 100 знаков Максимальное количество пар «ключ-значение» не может превышать 20
Descriptor	String	Нет	Динамический дескриптор точки

Структура объектов DATA

Ключ	Тип	Обязательность	Значение
StartSpAccumulation	String	Нет	Флаг о необходимости создания сделки при выполнении запроса. Игнорируется при наличии параметра DealId Вариант заполнения: NN

SpAccumulationId	String	Нет	Идентификатор сделки
BasicFieldKey	String	Нет	Идентификатор будущего получателя выплаты (номер телефона в формате "+79606747611").
Confidant	String	Нет	Уровень проверки получателя выплаты

* Для настройки параметра напишите в службу технической поддержки на acq_help@tbank.ru.
** Если у терминала включена опция привязки покупателя после успешной оплаты и передается параметр CustomerKey, то в передаваемых параметрах DATA могут присутствовать параметры метода AddCustomer. Если они присутствуют, то автоматически привязываются к покупателю.

Например, если указать: "DATA": {"Phone":"+71234567890", "Email":"a@test.com"}, к покупателю автоматически будут привязаны данные Email и телефон, и они будут возвращаться при вызове метода GetCustomer.

Дополнительные параметры DATA:

– Параметр notificationEnableSource позволяет отправлять нотификации только если Source (также присутствует в параметрах сессии) платежа входит в перечень указанных в параметре. Возможные варианты: TinkoffPay, sbpqr, YandexPay.
  Пример: notificationEnableSource=TinkoffPay

– Для MCC 4814 обязательно передать значение в параметре "Phone". Требования по заполнению параметра «Phone»:
  - минимум 7 символов;
  - максимум 20 символов;
  - разрешены только цифры, исключение – первый символ может быть «+».

– Если используется функционал сохранения карт на платежной форме, то при помощи опционального параметра "DefaultCard" можно задать, какая карта будет выбираться по умолчанию. Возможные варианты:
  - Оставить платежную форму пустой. Пример: "DATA": {"DefaultCard":"none"};
  - Заполнить данными передаваемой карты. В этом случае передается CardId. Пример: "DATA": {"DefaultCard":"894952"};
  - Заполнить данными последней сохраненной карты. Применяется, если параметр "DefaultCard" не передан, передан с некорректным значением или в значении null.

  По умолчанию возможность сохранения карт на платежной форме может быть отключена. Для активации обратитесь в службу технической поддержки.

– Для привязки и одновременной оплаты по СБП передавайте параметр QR в значении true:
  "DATA": { "QR": "true"}

– При реализации подключения оплаты **T-Pay Web** на сайте мерчанта необходимо обязательно передавать следующие параметры в объекте DATA:
  "DATA": {
   "TinkoffPayWeb": "true",
   "Device": "Desktop",
   "DeviceOs": "iOS",

```
  "DeviceWebView": "true",
 "DeviceBrowser": "Safari"
}
```

где следует передать параметры устройства, с которого будет осуществлен переход

– Для привязки и одновременной оплаты по СБП передавайте параметр “QR”: true: "DATA": { "YandexPayWeb": "true"}

Таблица 2.3.1.1 Параметры запроса для T-Pay

Наименование	Тип	Обязательность	Описание
Device	String	Нет	Тип устройства • SDK (вызов из мобильных приложений) • Desktop (вызов из браузера с десктопа) • Mobile (вызов из браузера с мобильных устройств)
DeviceOs	String	Нет	ОС устройства
DeviceWebView	Boolean	Нет	Признак открытия в WebView
DeviceBrowser	String	Нет	Браузер
TinkoffPayWeb	Boolean	Нет	Признак проведения операции через T-Pay по API

В случае, если не удается определить параметр гарантированно (режим инкогнито и пр.) – не передавать параметр.

*** Для включения обязательности подписи запроса (token) напишите в службу технической поддержки на acq_help@tbank.ru. Описание алгоритма формирования подписи доступно по ссылке.

**** В случае, если параметр RedirectDueDate не был передан, проверяется настроечный параметр платежного терминала REDIRECT_TIMEOUT, который может содержать значение срока жизни ссылки в часах. Если его значение больше нуля, то оно будет установлено в качестве срока жизни ссылки или динамического QR-кода. Иначе устанавливается значение по умолчанию - 24 часа.

Примеры передачи параметров в запросах

/v2/Init метод POST **Content-Type : json**	/v2/Init метод POST **Content-Type : json**

{
"TerminalKey": "TerminalKey ",
"Amount": "15000",
"OrderId": "sp123",
"Description": "Мультирасчеты",
"DATA": {
"Phone": "+71234567777",
"Email": "a@test.com",
"StartSpAccumulation": "NN",
"SpAccumulationId": "2332112",
"BasicFieldKey": "7921324234",
"Confidant": 1
}
}
	{
	"TerminalKey": "TerminalKey ",
	"Amount": "15000",
	"OrderId": "sp123",
	"Description": "Мультирасчеты",
	"DATA": {
	"Phone": "+71234567777",
	"Email": "a@test.com"
	},
	"PaymentRecipientId": "asdasdad",
	"DealId" : "23123123",
	"CreateDealWithType": "NN"
	"LevelOfConfidence": "moderate"
	}

Ответ

Таблица 2.3.2 Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
Amount	Number	Да	Сумма в копейках
OrderId	String	Да	Идентификатор заказа в системе мерчанта
Status	String	Да	Статус транзакции
PaymentId	String	Да	Идентификатор платежа в системе Т-Бизнеса
PaymentURL	String	Нет	Ссылка на платежную форму. Параметр возвращается только для мерчантов без PCI DSS
Success	Bool	Да	Успешность запроса (true/false)

ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:


```
{
  "Success": true,
  "ErrorCode": "0",
  "TerminalKey": "TerminalKey",
  "Status": "NEW",
  "PaymentId": "7277900132",
  "OrderId": "sp123",
  "Amount": "15000",
  "PaymentURL": "https://pay-test.tbank.ru/kwVvZY9L"
}
```

2.4. Метод Check3dsVersion

Метод для схемы PCI DSS

Описание: Проверяет поддерживаемую версию 3DS протокола по карточным данным из входящих параметров.
При определении второй версии возможно в ответе получение данных для прохождения дополнительного метода “3DS Method”, который позволяет эмитенту собрать данные браузера пользователя – это может быть полезно при принятии решения в пользу Frictionless Flow (аутентификация клиента без редиректа на страницу ACS).

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Check3dsVersion
Боевой URL: https://securepay.tinkoff.ru/v2/Check3dsVersion
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.4.1 Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
CardData	String	Да	Данные карты*
Token	String	Да	Подпись запроса

* Объект CardData описан в пункте 2.5 Метод FinishAuthorize

Пример запроса:


```
{
 "TerminalKey": "TinkoffBankTest",
 "PaymentId": "777",
 "CardData":"b3tSlUYwsf3Erdv5ReB7WpWK3/NBWLIwDiSLjQGOcBxAOMgs7ALd7ediORbVlORsyGZEUJSlRynQ9zLMyHYzWP3z2sQYGAvzOqufoVPe2AozhW3pZV+dN5s7oGcpXd39NDCOMa/Zw6oa3dJROZh8QYjv/sGOzUllMjXl5aHgTpxk37q6OxUakxuG7euhvSN71JqxHsNEuoJELAqLq7U+3tuh9AjTuiBpmEH99maK9e7gnVXgZd1Nk8vachs97xj9cL/O23qYMk7CMjldBfG4VOsYVqcHsKfbbJJ8CZXIJgmXhCYns1hmRD/kf3OhEZrO38LghC7IioOyxHYMhZyJoQ==",
"Token": "daab60d01863965284f1db558ff37534715afd0f1e726ca9611b1f90720ad03b",
}
```

Ответ

Таблица 2.4.2 Параметры ответа

Наименование	Тип	Обязательность	Описание
Version	String	Да	Версия протокола 3DS. Пример: “1.0.0” – первая версия “2.1.0” – вторая версия
TdsServerTransID	String	Нет	Уникальный идентификатор транзакции, генерируемый 3DS-Server, обязательный параметр для 3DS второй версии. Пример: 17d3791b-5cfa-4318-bc233d949e8c4b7e
ThreeDSMethodURL	String	Нет	Дополнительный параметр для 3DS второй версии, который позволяет пройти этап по сбору данных браузера ACS-ом
PaymentSystem	String	Да	Платежная система карты
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:


```
{
   "Success": true,
   "ErrorCode": "0",
   "Message": "OK",
   "Version": "2.1.0",
   "TdsServerTransID": "17d3791b-5cfa-4318-bc23-3d949e8c4b7e",
   "ThreeDSMethodURL": "https://acs.vendorcert.mirconnect.ru/ds/6300"
   "PaymentSystem": "mir"
}
```

Процесс прохождения этапа “3DS Method”:

Если в ответе метода был получен параметр ThreeDSMethodURL, то необходимо отправить запрос на стороне браузера по полученному ThreeDSMethodURL. для сбора информации ACS-ом о девайсе пользователя. Отправка запроса 3DS Method в браузере должна происходить в скрытом frame.

Тайм-аут ожидания ответа выполнения запроса 3DS Method перед выполнением запроса FinishAuthorize должен быть 10 секунд.

Формат запроса: x-www-form-urlencoded

Таблица 2.4.3. Описание параметров запроса 3DS Method

Название параметра	Тип	Обязательность	Описание
*threeDSMethodData	String	Y	JSON с параметрами threeDSMethodNotificationURL, threeDSServerTransID, закодированный в формат base-64

* Запрещено использовать padding

threeDSMethodNotificationURL, threeDSServerTransID

Название параметра	Тип	Обязательность	Описание
threeDSMethodNotificationURL	String	Y	Обратный адрес, на который будет отправлен запрос после прохождения threeDSMethod
threeDSServerTransID	String	Y	Идентификатор транзакции из ответа метода

Пример запроса на 3DS Method Url:

```
<body onload="document.form.submit()">
<form name="form" action="{ThreeDSMethodURL}" method="post" >
  <input type="hidden" name=" threeDSMethodData "
value="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjU2ZTcxMmE1LTE5MGEtNDU4OC05MWJjLWUwODYy
NmU3N2M0NCIsInRocm
VlRFNNZXRob2ROb3RpZmljYXRpb25VUkwiOiJodHRwczovL3Jlc3QtYXBpLXRlc3QudGlua29mZi5ydS92
Mi9Db21wbGV0ZTNEU0 1ldGhvZHYyIn0">
</form>
</body>
```

Пример декодированного значения threeDSMethodData

```
{
"threeDSServerTransID":"56e712a5-190a-4588-91bc-e08626e77c44",
"threeDSMethodNotificationURL":https://rest-api-test.tinkoff.ru/v2/Complete3DSMethodv2”
}
```

2.5. Метод FinishAuthorize

Метод для схемы PCI DSS

Описание: Подтверждает инициированный платеж передачей карточных данных. При использовании одностадийного проведения осуществляет списание денежных средств с карты покупателя. При двухстадийном проведении осуществляет блокировку указанной суммы на карте покупателя.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/FinishAuthorize
Боевой URL: https://securepay.tinkoff.ru/v2/FinishAuthorize
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.5.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
CardData	String	Да	Данные карты*
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента Обязательный параметр для 3DS второй версии DS платежной системы требует передавать данный адрес в полном формате, без каких-либо сокращений (8 групп по 4 символа) Данный формат регламентируется на уровне спецификации EMVCo. Пример правильного адреса: 2011:0db8:85a3:0101:0101:8a2e:0370:7334 Пример неправильного адреса: 2a00:1fa1:c7da:9285:0:51:838b:1001
Amount	Number	Нет	Сумма в копейках
SendEmail	boolean	Нет	true – отправлять клиенту информацию на почту об оплате

deviceChannel	String	Нет	Канал устройства.Поддерживается следующий канал устройства: 01 = Application (APP) 02 = Browser (BRW)
Route	Enum	Нет	Способ платежа. Возможные значения: – ACQ; – MC; – EINV; – WM.
Source	Enum	Нет	Источник платежа. Значение параметра зависит от параметра Route – ACQ - cards (также поддерживается написание Cards); – MC - beeline / mts/ tele2 / megafon; – EINV - einvoicing; – WM - webmoney.
InfoEmail	String	Нет (Обязателен при передаче SendEmail)	Email для отправки информации об оплате
DATA***	Object	Нет	JSON объект, содержащий дополнительные параметры в виде “ключ”:”значение”. Данные параметры будут переданы на страницу оплаты (в случае ее кастомизации). Максимальная длина для каждого передаваемого параметра: ключ – 20 знаков; значение – 100 знаков Максимальное количество пар «ключ-значение» не может превышать 20

* Объект CardData собирается в виде списка «ключ=значение» (разделитель «;»), зашифровывается открытым ключом (X509 RSA 2048), получившееся бинарное значение кодируется в Base64. Открытый ключ генерируется Банком и выдается при регистрации терминала. Все поля обязательны.

Для YandexPay (расшифровка токена происходит на стороне Мерчанта) надо:

1. Передавать Route=ACQ и Source=YandexPay;
2. Передавать в DATA.transactionId значение PaymentToken.messageId
3. Передавать в DATA.YandexPayWeb значение true
4. Передавать параметр CardData

Размапить параметры из расшифрованного токена event.token

- paymentMethodDetails.pan в pan
- paymentMethodDetails,expirationMonth + paymentMethodDetails.expirationYear в ExpDate
- paymentMethodDetails.cryptogram в CAVV (если есть)
- paymentMethodDetails.eci в ECI (если есть)

Таблица 2.5.2. Параметры CardData

Наименование	Тип	Обязательность	Описание
PAN	Number	Да	Номер карты
ExpDate	Number	Да	Месяц и год срока действия карты в формате MMYY
CardHolder	String	Нет	Имя и фамилия держателя карты (как на карте)
CVV	String	Нет	Код защиты (с обратной стороны карты)
ECI	String	Нет	Electronic Commerce Indicator. Индикатор, показывающий степень защиты, применяемую при предоставлении покупателем своих данных ТСП.
CAVV	String	Нет	Cardholder Authentication Verification Value или Accountholder Authentication Value

Пример значения элемента формы CardData:
PAN=4300000000000777;ExpDate=0519;CardHolder=IVAN PETROV;CVV=111

Пример запроса:

{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"CardData":"b3tSlUYwsf3Erdv5ReB7WpWK3/NBWLIwDiSLjQGOcBxAOMgs7ALd7ediORbVlORsyGZEUJSl
RynQ9zLMyHYzWP3z2s
QYGAvzOqufoVPe2AozhW3pZV+dN5s7oGcpXd39NDCOMa/Zw6oa3dJROZh8QYjv/sGOzUlIMjXI5aHgTp
xk37q6OxUakxuG7euhvS
N71JqxHsNEuoJELAqLq7U+3tuh9AjTuiBpmEH99maK9e7gnVXgZd1Nk8vachs97xj9cL/O23qYMk7CMj
IdBfG4VOsYVqcHsKfbbJ
J8CZXIJgmXhCYns1hmRD/kf3OhEZrO38LghC7IioOyxHYMhZyJoQ==",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}

*** Для 3DS второй версии в параметрах DATA необходимо передавать следующие параметры.

Таблица 2.5.3. DATA для 3DS v2

Наименование	Тип	Обязательность	deviceChannel	Описание
threeDSCompInd	String	Да	02 - BRW	Идентификатор выполнения 3DS Method 'Y' - выполнение метода успешно завершено 'N' - выполнение метода завершено неуспешно или метод не выполнялся
javaEnabled	String	Нет	02 - BRW	Поддерживает ли браузер пользователя Java: true/false. По умолчанию значение "false".
language	String	Да	02 - BRW	Язык браузера по формату IETF BCP47 Рекомендация по получению значения в браузере (из глобального объекта navigator): navigator.language
colorDepth	String	Нет	02 - BRW	Глубина цвета в битах. Допустимые значения: 1/4/8/15/16/24/32/48 Рекомендация по получению значения в браузере (из глобального объекта screen): screen.colorDepth По умолчанию значение будет 48
timezone	String	Да	02 - BRW	Time-zone пользователя в минутах. Пример для UTC +5 hours: "timezone": "-300" Рекомендация по получению значения в браузере: вызов метода getTimezoneOffset()
screen_height	String	Да	02 - BRW	Высота экрана в пикселях Рекомендация по получению значения в браузере (из глобального объекта screen): screen.height
screen_width	String	Да	02 - BRW	Ширина экрана в пикселях Рекомендация по получению значения в браузере (из глобального объекта screen): screen.width

cresCallbackUrl	String	Да	02 - BRW	URL который будет использоваться для получения результата(CRES) после завершения Challenge Flow(аутентификаци с дополнительным переходом на страницу ACS)
sdkAppID	String	Да	01 – APP	Уникальный идентификатор приложения 3DS Requestor, который формируется 3DS SDK при каждой установке или обновлении приложения
sdkEncData	String	Да	01 – APP	Данные, собранные SDK. JWE объект, полученный от 3DS SDK, должен быть дополнительно закодирован в base64 строку
sdkEphemPubKey	String	Да	01 – APP	Компонент public key пары ephemeral key, сгенерированный 3DS SDK. JWE объект, полученный от 3DS SDK, должен быть дополнительно закодирован в base64 строку
sdkMaxTimeout	String	Да	01 – APP	Максимальное количество времени (в минутах) Значение должно быть больше либо равно 5 символов.
sdkReferenceNumber	String	Да	01 – APP	Поставщик и версия 3DS SDK
sdkTransID	String	Да	01 – APP	Уникальный идентификатор транзакции, назначенный 3DS SDK для идентификации одной транзакции
sdkInterface	String	Да	01 – APP	Список поддерживаемых интерфейсов SDK Поддерживаемые значения: • 01 = Native • 02 = HTML • 03 = Both
sdkUiType	String	Да	01 – APP	Список поддерживаемых типов UI Значения для каждого интерфейса: • Native UI = 01–04 • HTML UI = 01–05 Поддерживаемые значения: • 01 = Text • 02 = Single Select

				• 03 = Multi Select • 04 = OOB • 05 = HTML Other (valid only for HTML UI) Пример значения: "01,02,03,04,05"

Для 3DS Version 2 в HttpHeaders запроса обязательно должны присутствовать заголовки: “User-Agent” и “Accept”.

Ответ

Формат ответа: JSON

Таблица 2.5.4. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
Amount	Number	Да	Сумма в копейках
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки
RebillId	String	Нет	Идентификатор рекуррентного платежа
CardId	String	Нет	Идентификатор карты в системе банка. Передается только для сохраненной карты

Статус платежа:

– при успешном сценарии и одностадийном проведении платежа: CONFIRMED;

– при успешном сценарии и двухстадийном проведении платежа: AUTHORIZED;

– при неуспешном: REJECTED;

– при необходимости прохождения проверки 3-D Secure: 3DS_CHECKING.

Пример ответа:

{
"Success": true,
"ErrorCode": "0",
"TerminalKey": "1485466639730",
"Status": "AUTHORIZED",
"PaymentId": "2181311",
"OrderId": "PAYMENT11750",
"Amount": 120
}

Пример ответа для статуса 3DS_CHECKING (3DS Version 1):

{
"Success": true,
"ErrorCode": "0",
"TerminalKey": "Test",
"Status": "3DS_CHECKING",
"PaymentId": "1993052",
"OrderId": "86d9d441-6685-43fd-b800-ded79290bd33",
"Amount": 100,
"ACSUrl": "https://secure.tcsbank.ru/acs/auth/start.do",
"MD": "ACQT-563587431",
"PaReq":
"eJxVUl1TwjAQ/CtM3Os+KLTDHGHQwsiogFhO9C2kp1RpC2nLh7/eBAtqnnYvN3ubvUD/kK4bO9RFkm
c9hzWpO8BM5XGSvfecRTRyA6cvIFppxPARVaVRwDOWhXzHRhL3HMUU73itwKVtyl1Pcs8Nli3pymUQK
+z2Sww6joDZYI5bAfUgYeYOOZAzNYparWRWCpBqezWeiDZnLe3BqSmkqMeh4PRy2pO2BfJThkymKCI
sSiAnCCqvslIfhXEG5Eyg0muxKstNOSVkv983yyT7zN/emroiQOwlkF8js8qiwogdklg8rEfT5WKOjj6G7D4c
epNo8TWNBmwSDXtAbAfEskTjkPkOoF6DeV3a6jLj8VQHmVoXglFTqTFs7IjBn4u/BTBZa7OK8yPODPCw
yTMOHSbACwby6/f6xsaoSpNMMN89+uHdV/iUPz2nyat/uxrPXz5nuX/c2nBPTVYxMflwzthJOhIgVobUey
P1yg469xW+AedOuuM="
}

! Если в ответе метода FinishAuthorize возвращается статус 3DS_CHECKING, мерчанту необходимо сформировать запрос на URL ACS банка, выпустившего карту (в ответе параметр ACSUrl) и вместе с этим перенаправить клиента на эту же страницу ACSUrl для прохождения 3DS.

URL: ACSUrl (возвращается в ответе метода FinishAuthorize)

Метод: POST

Формат запроса: x-www-form-urlencoded

Таблица 2.5.5. Параметры запроса

Наименование	Тип	Обязательность	Описание
MD	String	Да	Уникальный идентификатор транзакции в системе банка (возвращается в ответе на FinishAuthorize)
PaReq	String	Да	Результат аутентификации 3-D Secure (возвращается в ответе на FinishAuthorize)
TermUrl	String	Да	Адрес перенаправления после аутентификации 3-D Secure (URL обработчик на стороне мерчанта, принимающий результаты прохождения 3-D Secure)

Пример запроса на ACS:

```
<body onload="document.form.submit()" >
<form name="form" action="{ACSUrl}" method="post" >
  <input type="hidden" name="TermUrl" value="{TermUrl}" >
  <input type="hidden" name="MD" value="{MD}" >
  <input type="hidden" name="PaReq" value="{PaReq}" >
</form>
</body>
```

Формат ответа: JSON

Таблица 2.5.6. Параметры ответа

Наименование	Тип	Обязательность	Описание
MD	String	Да	Уникальный идентификатор транзакции в системе банка (возвращается в ответе на FinishAuthorize)
PaRes	String	Да	Шифрованная строка, содержащая результаты 3-D Secure аутентификации (возвращается в ответе от ACS)
FallbackOnTdsV1	Boolean	Нет	В случае невозможности прохождения аутентификации по 3DS v2, делается принудительный Fallback на 3DS v1 и данный атрибут выставляется в true, в противном случае не передается в ответе

Пример ответа для статуса 3DS_CHECKING (3DS Version 2) для 02-BRW:

```
{
   "Success": true,
   "ErrorCode": "0",
   "TerminalKey": "1562766106114",
   "Status": "3DS_CHECKING",
   "PaymentId": "1993052",
```

"OrderId": "86d9d441-6685-43fd-b800-ded79290bd33",
"Amount": 700000,
"ACSUrl": "https://acs.vendorcert.mirconnect.ru/mdpayacs/creq",
"TdsServerTransId": " d7171a06-7159-4bdd-891a-a560fe9938d2",
"AcsTransId": " e176d5d3-2f19-40f5-8234-46d3464e0b08"
}

! Если в ответе метода FinishAuthorize возвращается статус 3DS_CHECKING, мерчанту необходимо сформировать запрос на URL ACS банка, выпустившего карту (в ответе параметр ACSUrl) и вместе с этим перенаправить клиента на эту же страницу ACSUrl для прохождения 3DS.

URL: ACSUrl (возвращается в ответе метода FinishAuthorize/AttachCard)

Пример ответа для статуса 3DS_CHECKING (3DS Version 2) для 01-APP:

{
"Success": true,
"ErrorCode": "0",
"TerminalKey": "1489677025749",
"Status": "3DS_CHECKING",
"PaymentId": "3114697365",
"OrderId": "1647850270",
"Amount": 8000,
"TdsServerTransId": "d93f7c66-3ecf-4d10-ba62-46046e7b7596",
"AcsTransId": "aceca6af-56ee-43f0-80ef-ea8d30d5c5b0",
"AcsInterface": "02",
"AcsUiTemplate": "03",
"AcsSignedContent":
"eyJ4NWMiOlsiTUlJRGtUQ0NBbm1nQXdJQkFnSVVRU1VEV05VZEFicWozS1UyaOMOVHpaSEpVVHd3R
FFZSktvWklodmNOQVFFTEJRQXdXREVMTUFrR0ExVUVCaE1DVWxVeER6QU5CZO5WQkFnTUJrMXZjMk
52ZHpFUE1BMEdBMVVFQnd3R1RXOXpZMjkzTVJJd0VBWURWUVFLREFsVGIyMWxJR0poYm1zeEV6Q
VJCZO5WQkFNTUNtUnpMbTF2WTJzdWNuVXdIaGNOTWpBd056RTRNVFExT1RNM1doY05NakV3TnpFN
E1UUTFPVEOzV2pCWU1Rc3dDUVlEVlFRR0V3SlNWVEVQTUEwR0ExVUVDQXdHVFc5elkyOTNNUTh3RF
FZRFZRUUhEQVpOYjNOamIzY3hFakFRQmdOVkJBb01DVk52YldVZ1ltRnVhekVUTUJFR0ExVUVBd3dL
WkhNdWJXOWpheTV5ZFRDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBREND0VFvQ2dnRUJ
BTUhNdXB1Wlg3VUFWR3Z5dm9uZ1o4U3BJcisrRDRnMjBRaFwvZONGb3JUN1pDUkRaVWhRamlDSzdX
SWpiVHRKQUFKVG1yelhcLzlMSGJIdHpIcFFvRFVTNXZPTnRqVWFaVGVQUE91SklMRWl6NDBBVjJCUVZR
dOxnRzBjbm9oK21QaOdNMEZ4VmJFcHFEVHk3SHBOdFAwdm96cGxHNjdFWk1HTXdKSUpESmlDYUdG
0GZOaTlYR3M4MXB3NUhWZElmOHNpQnFaWW94cGtOQWJ1dnpBTFJEUnp3dFBhclFHOTZyQStPMOdJa
E53VDhZXC9pallwSOhWNkJCWDBKNmxZdFdoaVY5blhBVktYNTNlVTJ4M1E2Njh4U3BLa2dwSVh1N2xi
NUN2M2dDTlIrelVqKOlTODNZYjJhUlR2WkF6MFI1V3dBNW5Zb2J6V3Vta1wvdE5iV1FYdzBWTUNBdOV
BQWFOVE1GRXdIUVlEVlIwT0JCWUVGRmVWNOdzROtCSzhUTDljaVk4UFF2NORhY29OTUI4ROExVWRJd
1FZTUJhQUZGZVY3R3NHSOJLOFRMOWNpWThQUXY3RGFjb3RNQThHQTFVZEV3RUJcL3dRRk1BTUJB
Zjh3RFFZSktvWklodmNOQVFFTEJRQURnZOVCQUZqVGppUkxKOFpaWld5dXFLNTZHVkR6dnJiXC9uRlVD
THVjVXZEV2toKO9lRWkxWUFPOUJZV3RFVTVzdmRNNTlsOWVTMGtjbGxrRzVDTklcL1U4S2dKSnUzVOtE
VXp5cU8OeVRNU3g3RWZDXC9qVE1oT2d2YUJubktWK2hvV3FQZTlKNHZVYzZ2ROwzWE1cLOFNeWpo
VDlBRko1ZjZBaVdZMk5QYkxHczQ2NOZPY2Vwb1RJMkdseHBtcWdaMFVGKzlsblNZbDUOWEg2dGNZYU
szWjcxS2NESOlOQkUySWVmV1Y3MUM3anBVdjFFSlFsNTY4XC8xaGpsZktXUExWcE5NTzVlTlNMR1ZKd1
VmdFAOVOtKU2Y2VmdtbG5XOU1yVStiK3hvZW44MFF1dUxrSWs1ZXBIM2l1ZDV4a1IxcVVXQU1aTUZ
TQW4yUHJJDdjQrZFFMRDd2OG83d3BrPSJdLCJhbGciOiJQUzI1NiJ9.eyJhY3NFcGhlbVB1YktleSI6eyJrd

HkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IlRoRjNJY3BIMVVLanliQW5lNWhHcy1BNnpyYXo2aUxiYVkOWmVE
OU1oSUOiLCJ5IjoidOVuVXNvNlRLZDlfbjZSc2NjUXRCeFc2Q1gzLXFSTGkOUWJBU3pNbm4tTSJ9LCJzZ
GtFcGhlbVB1YktleSI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6Ikp6R2tGM2w3WGxnclJ6NU1PTl9ncD
g3WUxfdONkVVJpVUlxOXJmNnVyR2MiLCJ5IjoiTnI4UmllTE9vVzJXUkhiX2RFazFmdHRoWEZXTHdYaWZ
FUzNZZkFnMkhvWSJ9LCJhY3NVUkwiOiJodHRwczovL2VhY3EtZHMtbW9jay1zZXJ2aWNlLXRlc3QudGN
zYmFuay5ydS9jaGFsbGVuZ2UvZDkzZjdjNjYtM2VjZiOOZDEwLWJhNjItNDYwNDZlN2I3NTk2InO.hQLVTT5
YMAY8TjISRdYX2ITO4zH8Z8DgoB4kIAyVfkuJOX6AGIKXSVcIVSNgC-
A_SEkCZRqAyUeuOZJtpoIVyOf1mumBGEK-
uC6yVQlX5WSPidQUj4nuBvpYsfdrGPeoHWvNsrBpMMxvvW4559jtbAUYOONcW3rwDShAi4gVKgJcssMP
AM1zOOR5viO_ClUs-
CW1k9a2O1Hv6cYcEBuO2JQ8NPLampEkZ55nOmwcPPTEziXeZsq9VjROXNfBewbA4wLuQmh8aSrcOcw
FtJoOCPpdrsKiY77KPTOc8XMmZZK_FiAxzrWocfHraqC7cRJNQ5glEBakXvSfrwGg_xXA",
  "AcsReferenceNumber": "12345",
  "SdkTransID": "d5a44dfe-673b-4666-82f9-96346107e424"
}

! Если в ответе метода FinishAuthorize возвращается статус 3DS_CHECKING, мерчанту необходимо сформировать запрос (может быть два и более в рамках одного challenge) на URL ACS банка, выпустившего карту (в ответе параметр ACSUrl) и вместе с этим перенаправить клиента на эту же страницу ACSUrl для прохождения 3DS.

URL: ACSUrl (возвращается в ответе метода FinishAuthorize/AttachCard внутри параметра acsSignedContent)

Метод: POST

Формат запроса: x-www-form-urlencoded

Таблица 2.5.7. Параметры запроса creq

Наименование	Тип	Обязательность	deviceChannel	Описание
creq	String	Да	02-BRW	JSON с параметрами threeDSServerTransID, acsTransID, challengeWindowSize, messageType, messageVersion, закодированный в формат base-64
creq	String	Да	01-APP	JWE object с параметрами threeDSServerTransID, acsTransID, messageType, messageVersion, sdkTransID, sdkCounterStoA, закодированный в формат PS256

JSON/JWE creq

Наименование	Тип	Обязательность	deviceChannel	Описание
threeDSServerTransID	String	Да	01-APP 02-BRW	Идентификатор транзакции из ответа метода FinishAuthorize
acsTransID	String	Да	01-APP 02-BRW	Идентификатор транзакции, присвоенный ACS, полученный в ответе на FinishAuthorize
challengeWindow Size	String	Да	02-BRW	Размер экрана, на котором открыта страница ACS. Допустимые значения: • 01 = 250 x 400 • 02 = 390 x 400 • 03 = 500 x 600 • 04 = 600 x 400 • 05 = Full screen
messageType	String	Да	01-APP 02-BRW	Передается фиксированное значение «CReq»
messageVersion	String	Да	01-APP 02-BRW	Версия 3DS, полученная из ответа метода Check3dsVersion
sdkTransID	String	Да	01-APP	Уникальный идентификатор транзакции, назначенный 3DS SDK для идентификации одной транзакции, полученный в ответе на FinishAuthorize
sdkCounterStoA	String	Да	01-APP	Внутренний счетчик 3DS SDK внутри ACS Поддерживаемые значения: 000-255

В Creq запрещено использовать padding

Пример запроса на ACS:

```
<body onload="document.form.submit()" >
<form name="form" action="{ACSUrl}" method="post" >
  <input type="hidden" name="creq"
value="ewogICJhY3NUcmFucOlEIjogImUxNzZkNWQzLTJmMTktNDBmNS04MjMOLTQ2ZDMONjRlMGIwO
CIsCiAgImNoYWxsZW5nZVdpbmRvd1NpemUiOiAiMDMiLAogICJtZXNzYWdlVHlwZSI6ICJDUmVxIiwKICAi
bWVzc2FnZVZlcnNpb24iOiAiMi4xLjAiLAogICJOaHJlZURT
2VydmVyVHJhbnNJRCI6ICJkNzE3MWEwNiO3MTU5LTRiZGQtODkxYS1hNTYwZmU5OTM4ZDIiCnOK" >
</form>
```

</body>

Creq декодированный из base64:


```
{
 "acsTransID": "e176d5d3-2f19-40f5-8234-46d3464e0b08",
 "challengeWindowSize": "03",
 "messageType": "CReq",
 "messageVersion": "2.1.0",
 "threeDSServerTransID": "d7171a06-7159-4bdd-891a-a560fe9938d2"
}
```


Формат ответа: Cres, полученный по NotificationUrl из запроса FinishAuthorize/AttachCard для 02BRW/3DS SDK для 01-APP

Таблица 2.5.8. Параметры ответа cres

Наименование	Тип	Обязательность	deviceChannel	Описание
cres	String	Да	02-BRW	JSON с параметрами threeDSServerTransID, acsTransID, messageType, messageVersion, transStatus, закодированный в формат base-64
cres	String	Да	01-APP	JWE object с параметрами threeDSServerTransID, acsTransID, acsUiType, challengeCompletionInd, challengeInfoHeader, challengeInfoLabel, challengeInfoText, challengeInfoTextIndicator, expandInfoLabel, expandInfoText, issuerImage, messageType, messageVersion, psImage, resendInformationLabel, sdkTransID, submitAuthenticationLabel, whyInfoLabel, whyInfoText, acsCounterAtoS, закодированный в формат PS256

JSON/JWE cres

Наименование	Тип	Обязательность	deviceChannel	Описание
threeDSServerTransID	String	Да	01-APP 02-BRW	Идентификатор транзакции из ответа метода Check3dsVersion
acsTransID	String	Да	01-APP 02-BRW	Идентификатор транзакции, присвоенный ACS
acsUiType	String	Обязательное для финального cres	01-APP	Тип пользовательского интерфейса
challengeAddInfo	String	Нет	01-APP	Дополнительный текст в форме подтверждения
challengeCompletionInd	String	Да	01-APP	Индикатор завершения подтверждения Y = Challenge завершен, дальнейший обмен сообщениями не требуется N = Challenge не завершен, и требуется дополнительный обмен сообщениями
challengeInfoHea der	String	Нет	01-APP	Заголовок страницы подтверждения
challengeInfoLabel	String	Нет	01-APP	Тип информации, запрошенной от пользователя при подтверждении
challengeInfoText	String	Нет	01-APP	Текст, предоставленный пользователю при подтверждении
challengeInfoTextIndicator	String	Нет	01-APP	Индикатор наличия рамки или иконки возле текста рядом с полем ввода на форме подтверждения
expandInfoLabel	String	Нет	01-APP	Название поля дополнительной информации

expandInfoText	String	Нет	01-APP	Текст поля дополнительной информации
issuerImage	String	Нет	01-APP	URL-адрес картинки подтверждения
messageType	String	Да	01-APP 02-BRW	Передается фиксированное значение «CRes»
messageVersion	String	Да	01-APP 02-BRW	Версия 3DS
transStatus	String	Обязательное для финального cres	01-APP 02-BRW	Результат выполнения Challenge flow ‘Y’ – аутентификация выполнена успешна ‘N’ – аутентификация не пройдена, пользователь отказался или ввел неверные данные ‘U’ – не удалось выполнить аутентификацию / проверку учетной записи; техническая или иная проблема, как указано в ARes или RReq. ‘A’ – попытки обработки завершены; пользователь не аутентифицирован/не подтвержден, но было предоставлено доказательство попытки аутентификации/ подтверждения. ‘C’ – требуется вызов; требуется дополнительная аутентификация с использованием CReq/CRes. ‘R’ – аутентификация/ верификация учетной записи отклонены; Эмитент отклоняет аутентификацию /верификацию и требует не предпринимать попытки авторизации.
psImage	String	Нет	01-APP	URL-адрес картинки платежной системы

resendInformationLabel	String	Нет	01-APP	Текст кнопки повторной отправки подтверждения
sdkTransID	String	Да	01-APP	Уникальный идентификатор транзакции, назначенный 3DS SDK для идентификации одной транзакции
submitAuthenticationLabel	String	Обязательное, если ACSUIType = 01, 02, 03.	01-APP	Текст кнопки завершения аутентификации
whyInfoLabel	String	Нет	01-APP	Заголовок в UI в секции, объясняющий пользователю причину прохождения аутентификации
whyInfoText	String	Нет	01-APP	Текст в UI в секции, объясняющий пользователю причину прохождения аутентификации
acsCounterAtoS	String	Да	01-APP	Счетчик, используемый как дополнительная мера безопасности в канале 3DS SDK

При успешном результате прохождения 3-D Secure подтверждается инициированный платеж с помощью методов Submit3DSAuthorization или Submit3DSAuthorizationV2, в зависимости от версии 3DS.

2.6 Метод Submit3DSAuthorization

Метод для схемы PCI DSS

Описание: Осуществляет проверку результатов прохождения 3-D Secure и при успешном результате прохождения 3-D Secure подтверждает инициированный платеж.
При использовании одностадийной оплаты осуществляет списание денежных средств с карты покупателя.
При двухстадийной оплате осуществляет блокировку указанной суммы на карте покупателя.

Запрос

Метод: POST
Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Submit3DSAuthorization
Боевой URL: https://securepay.tinkoff.ru/v2/Submit3DSAuthorization
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Формат запроса: x-www-form-urlencoded
После получения на TermUrl мерчанта ответа ACS с результатами прохождения 3-D Secure необходимо сформировать запрос к методу Submit3DSAuthorization со следующими параметрами:

Таблица 2.6.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
MD	String	Да	Уникальный идентификатор транзакции в системе банка (возвращается в ответе от ACS)
PaRes	String	Да	Шифрованная строка, содержащая результаты 3-D Secure аутентификации (возвращается в ответе от ACS)
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком

Пример запроса:
```
<body onload="document.form.submit()" >
<form name="form" action="https://rest-api-test.tinkoff.ru/v2/Submit3DSAuthorization" method="post"
>
 <input type="hidden" name="MD" value="2561504" >
```

```
  <input type="hidden" name="PaRes"
value="eJxVUttygjAU/BWG1w4mXKXOMY5WOrVTrOOtl7cAqeJI1AAO+vVNFKrlaffkZM9mD9Crsq12ZC
JPd7yrmy2sa4zHuyTlq66+mD8bvt4jMF8LxoYzFpeCEQhZntMVO9JE3vC8Hx9j27A8LzEcN7aNCPu24VI
rihKXetiPdAKT/pQdCNSDiJzTsgA1VCqKeE15QYDGh8FoTBy73fZtQDWFjInRkFi4+Uz82JbH1zJwmjEyHc
wAXRDEu5IX4kQ8R/YOBEqxJeui2HcQOlGesKolSkCqCuhmYFIqlEuVKk3IDL8uPwI3jDaBGZ4XeLxZVeFw5
I7nX11AqgMSWjDpzPSxb/ma6XRct4Pl4y51oJkar5zLx1wx7NWI/t3BfQFkxkKuoHHfMGDVfseZugLoDwO
6+X16UfHFhUyk/32OMH3vZ5+nYBu/2d4xcMTDsnO4j19VqJcmpZjKYKT3q6QigJQMqveF6lVL908X+A
WMIbbt" >
  <input type="hidden" name="PaymentId " value="10063" >
  <input type="hidden" name="TerminalKey" value="TinkoffBankTest" >
  <input type="hidden" name="Token"
value="871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6" > </form>
</body>
```

Ответ

Формат ответа: JSON

Таблица 2.6.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Статус платежа:

- при успешном сценарии и одностадийном проведении платежа: CONFIRMED
- при успешном сценарии и двухстадийном проведении платежа: AUTHORIZED
- при неуспешном: REJECTED

Пример ответа:

```
{
"Success":true,
"ErrorCode":"0",
"TerminalKey":"TinkoffBankTest",
"Status":"CONFIRMED",
```

"PaymentId":"10063",
"OrderId":"21050",
"Amount":100000
}

2.7 Метод Submit3DSAuthorizationV2

Метод для схемы PCI DSS

Описание: Осуществляет проверку результатов прохождения 3-D Secure v2 и при успешном результате прохождения 3-D Secure v2 подтверждает инициированный платеж.

При использовании одностадийной оплаты осуществляет списание денежных средств с карты покупателя.

При двухстадийной оплате осуществляет блокировку указанной суммы на карте покупателя

Запрос

Метод: POST

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Submit3DSAuthorizationV2

Боевой URL: https://securepay.tinkoff.ru/v2/Submit3DSAuthorizationV2

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Формат запроса: x-www-form-urlencoded

После получения на NotificationUrl мерчанта ответа ACS (Cres) с результатами прохождения 3-D Secure v2 необходимо сформировать запрос к методу Submit3DSAuthorizationV2 со следующими параметрами:

Таблица 2.7.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком

Ответ

Формат ответа: JSON

Таблица 2.7.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки

Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Статус платежа:

- при успешном сценарии и одностадийном проведении платежа: CONFIRMED
- при успешном сценарии и двухстадийном проведении платежа: AUTHORIZED
- при неуспешном: REJECTED

Пример ответа:


```
{
"Success":true,
"ErrorCode":"0",
"TerminalKey":"TinkoffBankTest",
"Status":"CONFIRMED",
"PaymentId":"10063",
"OrderId":"21050",
"Amount":100000
}
```

2.8 Метод Confirm

Метод схем PCI DSS \ Без PCI DSS

Описание: Осуществляет списание заблокированных денежных средств. Используется при двухстадийном проведении платежа.

Применим только к платежам в статусе AUTHORIZED. Статус транзакции перед разблокировкой выставляется в CONFIRMING. Сумма списания может быть меньше или равна сумме авторизации.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Confirm
Боевой URL: https://securepay.tinkoff.ru/v2/Confirm
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.8.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента
Amount	Number	Нет	Сумма в копейках (если не передан, используется Amount, переданный в методе Init)

Пример запроса:


```
{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 2.8.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

```
{
"Success": true,
"ErrorCode": "0",
"TerminalKey": "1485466639730",
"Status": "CONFIRMED",
"PaymentId": “2164657”,
"OrderId": "PAYMENT117539"
}
```

2.9 Метод Charge

Метод схем PCI DSS \ Без PCI DSS

Описание: Осуществляет рекуррентный (повторный) платеж — безакцептное списание денежных средств со счета банковской карты Покупателя.

Для возможности его использования Покупатель должен совершить хотя бы один платеж в пользу Продавца, который должен быть указан как рекуррентный (см. параметр Recurrent в 2.3. Метод Init), фактически являющийся первичным. По завершении оплаты в нотификации на AUTHORIZED или CONFIRMED будет передан параметр RebillId.

В дальнейшем для совершения рекуррентного платежа Площадка должна вызвать метод Init, а затем без переадресации на PaymentURL вызвать метод Charge для оплаты по тем же самым реквизитам и передать параметр RebillId, полученный при совершении первичного платежа.

Метод Charge работает по одностадийной и двухстадийной схеме оплаты. Чтобы перейти на двухстадийную схему, нужно написать обращение на acq_help@tbank.ru с просьбой переключить схему рекуррентов.

Для использования рекуррентных платежей по одностадийной схеме (без PCI DSS) необходима следующая последовательность действий:

1. Совершить родительский платеж путем вызова Init с указанием дополнительных параметров Recurrent=Y и CustomerKey.
2. После оплаты заказа Покупателем в нотификации на статус AUTHORIZED или CONFIRMED будет передан параметр RebillId, который необходимо сохранить
3. Спустя некоторое время для совершения рекуррентного платежа необходимо вызвать метод Init со стандартным набором параметров (параметры Recurrent и CustomerKey здесь не нужны).
4. Получить в ответ на Init параметр PaymentId.
5. Вызвать метод Charge с параметром RebillId, полученным в п.2, и параметром PaymentId, полученным в п.4.
   При успешном сценарии операция перейдет в статус AUTHORIZED, а затем – в CONFIRMED.

Для использования рекуррентных платежей по двухстадийной схеме (без PCI DSS) необходима следующая последовательность действий:

1. Совершить родительский платеж путем вызова Init с указанием дополнительных параметров Recurrent=Y и CustomerKey.
2. После оплаты заказа Покупателем в нотификации на статус AUTHORIZED или CONFIRMED будет передан параметр RebillId, который необходимо сохранить.
3. Спустя некоторое время для совершения рекуррентного платежа необходимо вызвать метод Init со стандартным набором параметров (параметры Recurrent и CustomerKey здесь не нужны).
4. Получить в ответ на Init параметр PaymentId.
5. Вызвать метод Charge с параметром RebillId, полученным в п.2, и параметром PaymentId, полученным в п.4. При успешном сценарии операция перейдет в статус AUTHORIZED.
6. Вызвать метод Confirm для подтверждения платежа

Для использования рекуррентных платежей по одностадийной схеме (с PCI DSS) необходима следующая последовательность действий:

1. Совершить родительский платеж путем вызова Init с указанием дополнительных параметров Recurrent=Y и CustomerKey.

2. Вызвать метод Check3dsVersion для проверки ожидаемой версии 3DS протокола.
3. Вызвать метод FinishAuthorize для оплаты заказа. При необходимости, проверить прохождение 3DS проверки методами Submit3DSAuthorization/Submit3DSAuthorizationV2 в зависимости от версии 3DS. После оплаты заказа Покупателем в нотификации на статус AUTHORIZED или CONFIRMED будет передан параметр RebillId, который необходимо сохранить.
4. Спустя некоторое время для совершения рекуррентного платежа необходимо вызвать метод Init со стандартным набором параметров (параметры Recurrent и CustomerKey здесь не нужны).
5. Получить в ответ на Init параметр PaymentId.
6. Вызвать метод Charge с параметром RebillId, полученным в п.3, и параметром PaymentId, полученным в п.5. При успешном сценарии операция перейдет в статус AUTHORIZED.

Для использования рекуррентных платежей по двухстадийной схеме (с PCI DSS) необходима следующая последовательность действий:

1. Совершить родительский платеж путем вызова Init с указанием дополнительных параметров Recurrent=Y и CustomerKey.
2. Вызвать метод Check3dsVersion для проверки ожидаемой версии 3DS протокола.
3. Вызвать метод FinishAuthorize для оплаты заказа. При необходимости, проверить прохождение 3DS проверки методами Submit3DSAuthorization/Submit3DSAuthorizationV2 в зависимости от версии 3DS. После оплаты заказа Покупателем в нотификации на статус AUTHORIZED или CONFIRMED будет передан параметр RebillId, который необходимо сохранить.
4. Вызвать метод Confirm для подтверждения платежа. При необходимости отмены платежа вызвать метод Cancel.
5. Спустя некоторое время для совершения рекуррентного платежа необходимо вызвать метод Init со стандартным набором параметров (параметры Recurrent и CustomerKey здесь не нужны).
6. Получить в ответ на Init параметр PaymentId
7. Вызвать метод Charge с параметром RebillId, полученным в п.3, и параметром PaymentId, полученным в п.5. При успешном сценарии операция перейдет в статус AUTHORIZED. Денежные средства будут заблокированы на карте покупателя.
8. Вызвать метод Confirm для подтверждения платежа.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Charge

Боевой URL: https://securepay.tinkoff.ru/v2/Charge

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.9.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком

PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка, полученный в ответе на вызов метода Init
RebillId	String	Да	Идентификатор рекуррентного платежа (см. параметр Recurrent в методе Init)
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента
SendEmail	bool	Нет	true – если покупатель хочет получать уведомления на почту
InfoEmail	String	Нет (Обязателен при передаче SendEmail)	Адрес почты покупателя

Пример запроса:

{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"RebillId":"145919",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}

Ответ

Формат ответа: JSON

Таблица 2.9.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Amount	Number	Да	Сумма списания в копейках

ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:


```
{
"TerminalKey":"TinkoffBankTest",
"OrderId":"100668",
"Success":"true",
"Status":"CONFIRMED",
"PaymentId":"63100",
"Amount":444,
"ErrorCode":"0",
}
```

2.10. Метод Cancel

Метод для схем PCI DSS \ Без PCI DSS

Описание: Отменяет платежную сессию. В зависимости от статуса платежа переводит его в следующие состояния:

Таблица 2.10.1. Статусы платежа

Начальный статус	Статус после проведения операции
NEW	CANCELED
AUTHORIZED	PARTIAL_REVERSED – если отмена не на полную сумму
AUTHORIZED	REVERSED
CONFIRMED	PARTIAL_REFUNDED – если отмена не на полную сумму
CONFIRMED	REFUNDED – если отмена на полную сумму

Если платеж находился в статусе AUTHORIZED производится отмена холдирования средств на карте клиента. При переходе из статуса CONFIRMED – возврат денежных средств на карту клиента.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/Cancel
Боевой URL: https://securepay.tinkoff.ru/v2/Cancel
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.10.2. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента
Amount	Number	Нет*	Сумма отмены в копейках. Минимальное значение — 100.

QrMemberId	String	Нет	Код банка в классификации СБП, в который необходимо выполнить возврат См параметр MemberId в [Методе QrMembersList]
ExternalRequestId	String	Нет**	Идентификатор операции на стороне мерчанта

* в случае отмены статуса NEW поле Amount, даже если оно проставлено, игнорируется. Отмена производится на полную сумму.

** Если поле заполнено, то перед проведением возврата проверяется запрос на отмену с таким ExternalRequestId:

- если такой запрос уже есть, то в ответе вернется текущее состояние платежной операции;
- если такого запроса нет, то произойдет отмена платежа.

Если поле не передано или пустое (“”), то запрос будет обработан без проверки ранее созданных возвратов.

Пример запроса:

```
{
"TerminalKey":"TinkoffBankTest"
"PaymentId":"10063"
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 2.10.3. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
OrderId	String	Да	Номер заказа в системе Площадки
OriginalAmount	Number	Да	Сумма в копейках до операции отмены

NewAmount	Number	Да	Сумма в копейках после операции отмены
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки
ExternalRequestId	String	Нет	Идентификатор операции на стороне мерчанта

Пример ответа:


```
{
"TerminalKey": "1485466639730",
"Success": true,
"Status": "REVERSED",
"ErrorCode": "0",
"PaymentId": “2167708”,
"OrderId": "PAYMENT117558",
"OriginalAmount": 1000,
"NewAmount": 0
}
```

2.11. Метод GetState

Метод для схем PCI DSS \ Без PCI DSS

Описание: Возвращает статус платежа.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/GetState

Боевой URL: https://securepay.tinkoff.ru/v2/GetState

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.11.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента

Пример запроса:

```
{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 2.11.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки

Success	bool	Да	Успешность запроса (true/false)
Status	String	Да	Статус транзакции
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Amount	Number	Да	Сумма операции в копейках
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"TerminalKey":"TinkoffBankTest",
"OrderId":"21057",
"Success":true,
"Status":"NEW",
"PaymentId":"10063",
"ErrorCode":"0",
"Amount": 1000
}

Таблица 2.11.3. Возможные статусы транзакции

Статус	Промежуточный?	Значение
NEW	Нет	Платеж зарегистрирован в шлюзе, но его обработка в процессинге не начата
CANCELED	Нет	Платеж отменен Площадкой
PREAUTHORIZING	Да	Проверка платежных данных Покупателя
FORM_SHOWED	Нет	Покупатель переправлен на страницу оплаты
AUTHORIZING	Да	Покупатель начал аутентификацию
3DS_CHECKING	Нет	Покупатель начал аутентификацию по протоколу 3-D Secure. Сессии, находящиеся в статусе 3DS_CHECKING более 36 часов, будут автоматически закрываться.

3DS_CHECKED	Да	Покупатель завершил аутентификацию по протоколу 3D Secure
AUTH_FAIL	Да	Не пройдена проверка по протоколу 3-D Secure
PAY_CHECKING	Да	Платеж обрабатывается
AUTHORIZED	Нет	Средства заблокированы, но не списаны
REVERSING	Да	Начало отмены блокировки средств
REVERSED	Нет	Денежные средства разблокированы
CONFIRMING	Да	Начало списания денежных средств
CONFIRM_CHECKING	Да	Платеж обрабатывается. В течение 60 минут операции присвоится конечный статус согласно схеме
CONFIRMED	Нет	Денежные средства списаны
REFUNDING	Да	Начало возврата денежных средств
ASYNC_REFUNDING	Да	Обработка возврата денежных средств по QR
PARTIAL_REFUNDED	Нет	Произведен частичный возврат денежных средств
REFUNDED	Нет	Произведен возврат денежных средств
REJECTED	Нет	Платеж отклонен банком
DEADLINE_EXPIRED	Нет	Платежная сессия закрыта в связи с превышением срока отсутствия активности по текущему статусу

2.12. Метод CheckOrder

Метод для схем PCI DSS \ Без PCI DSS

Описание: Возвращает статус заказа.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/CheckOrder

Боевой URL: https://securepay.tinkoff.ru/v2/CheckOrder

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 2.12.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	Number	Да	Номер заказа в системе Площадки
Token	String	Да	Подпись запроса

Пример запроса:


```
{
"TerminalKey":"TinkoffBankTest",
"OrderId":"21057",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```


Ответ

Формат ответа: JSON

Таблица 2.12.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки

Details	String	Нет	Подробное описание ошибки
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Payments	Object	Да	Детали

Таблица 2.12.3. Структура объекта Payments

Наименование	Тип	Обязательность	Описание
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Amount	Number	Нет	Сумма операции в копейках
Status	String	Да	Статус транзакции
RRN	String	Нет	RRN операции
Success	String	Да	Успешность запроса (true/false)
ErrorCode	Number	Да	Код ошибки, «0» - если успешно
Message	String	Да	Краткое описание ошибки

Пример ответа:

```
{
   "Success": true,
   "ErrorCode": "0",
   "Message": "OK",
   "OrderId": "21057",
   "TerminalKey": "TinkoffBankTest",
   "Payments": [
      {
         "Status": "REJECTED",
         "PaymentId": “10063”,
         "Rrn": 1234567,
         "Amount": 555,
         "Success": false,
         "ErrorCode": "1051",
         "Message": "Недостаточно средств на карте"
      },
      {
         "Status": "AUTH_FAIL",
         "PaymentId": “1005563”,
```

```
      "Rrn": 1234567,
      "Amount": 555,
      "Success": false,
      "ErrorCode": "76",
      "Message": "Операция по иностранной карте недоступна."
    },
    {
      "Status": "NEW",
      "PaymentId": "100553363",
      "Rrn": 1234567,
      "Amount": 555,
      "Success": true,
      "ErrorCode": "0",
      "Message": "ok"
    }
]}
```

2.13. Оплата через T-Pay Web на сайте мерчанта

Методы для схемы PCI DSS

Оплата доступна на мобильных устройствах и десктопах, проводится последовательным вызовом методов:

- /TinkoffPay/terminals/{terminalKey}/status
- /init
- /TinkoffPay/transactions/{paymentId}/versions/{version}/link либо /TinkoffPay/{paymentId}/QR

2.13.1. Метод TinkoffPay/terminals/{terminalKey}/status

Метод для схемы PCI DSS

Описание: определение возможности проведения платежа T-Pay на терминале и устройстве.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/TinkoffPay/terminals/{terminalKey}/status

Боевой URL: https://securepay.tinkoff.ru/v2/TinkoffPay/terminals/{terminalKey}/status

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: GET

Таблица 2.14.1.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком

Ответ

Таблица 2.14.1.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки
Params	Object	Да	Параметры ответа

Таблица 2.14.2.3. Структура объекта Params

Наименование	Тип	Обязательность	Описание
Allowed	bool	Да	Наличие возможности проведения оплаты T-Pay по API, SDK
Version	String	Нет*	Версия T-Pay, доступная на терминале: 1.0 (e-invoice) 2.0 (T-Pay)

***** Обязательное при Allowed = true

Если версия в ответе метода 1.0, то оплата может быть проведена только с мобильного устройства.

Пример ответа:

```
{
  "Success":true,
  "ErrorCode":"0",
  "Params":{
    "Allowed":true,
    "Version":"1.0"
  }
}
```

2.13.2. Метод TinkoffPay/transactions/{paymentId}/versions/{version}/link

Метод для схемы PCI DSS

Описание: получение Link для безусловного редиректа на мобильных устройствах

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/TinkoffPay/transactions/{paymentId}/versions/{version}/link

Боевой URL: https://securepay.tinkoff.ru/v2/TinkoffPay/transactions/{paymentId}/versions/{version}/link

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: GET

Таблица 2.14.2.1 Параметры запроса

Наименование	Тип	Обязательность	Описание
paymentId	Number	Да	Идентификатор платежа
version	String	Да	Версия T-Pay: 1.0 (e-invoice) 2.0 (T-Pay)

Ответ

Таблица 2.14.2.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки
Params*	Object	Да	Параметры ответа

Таблица 2.14.2.3. Структура объекта Params

Наименование	Тип	Обязательность	Описание
RedirectUrl	String	Да	Link для перехода в приложение MB на мобильных устройствах
WebQR	String	Нет	URL для получения QR

Пример ответа:

```
{
   "Success": true,
   "ErrorCode": "0",
   "Params": {
     "RedirectUrl": "https://www.tinkoff.ru/tpay/2000000000000037338",
     "WebQR": "https://securepay.tinkoff.ru/v2/TinkoffPay/2332790853/QR"
    }
}
```

Устаревший ответ для версии 1.0(e-invoice):

```
{
   "Success": true,
   "ErrorCode": "0",
   "Params": {
     "RedirectUrl": "tinkoffbank://Main/EInvoicing?billId=5000015507&providerId=e-invoicing"
    }
}
```

2.13.3. Метод GET /v2/TinkoffPay/{paymentId}/QR

Метод для схемы PCI DSS

Описание: получение QR для десктопов

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/TinkoffPay/{paymentId}/QR

Боевой URL: https://securepay.tinkoff.ru/v2/TinkoffPay/{paymentId}/QR

* Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: GET

Таблица 2.14.3.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
paymentId	Number	Да	Идентификатор платежа

Ответ

Формат ответа: imageSVG

Таблица 2.14.3.2. Параметры ответа

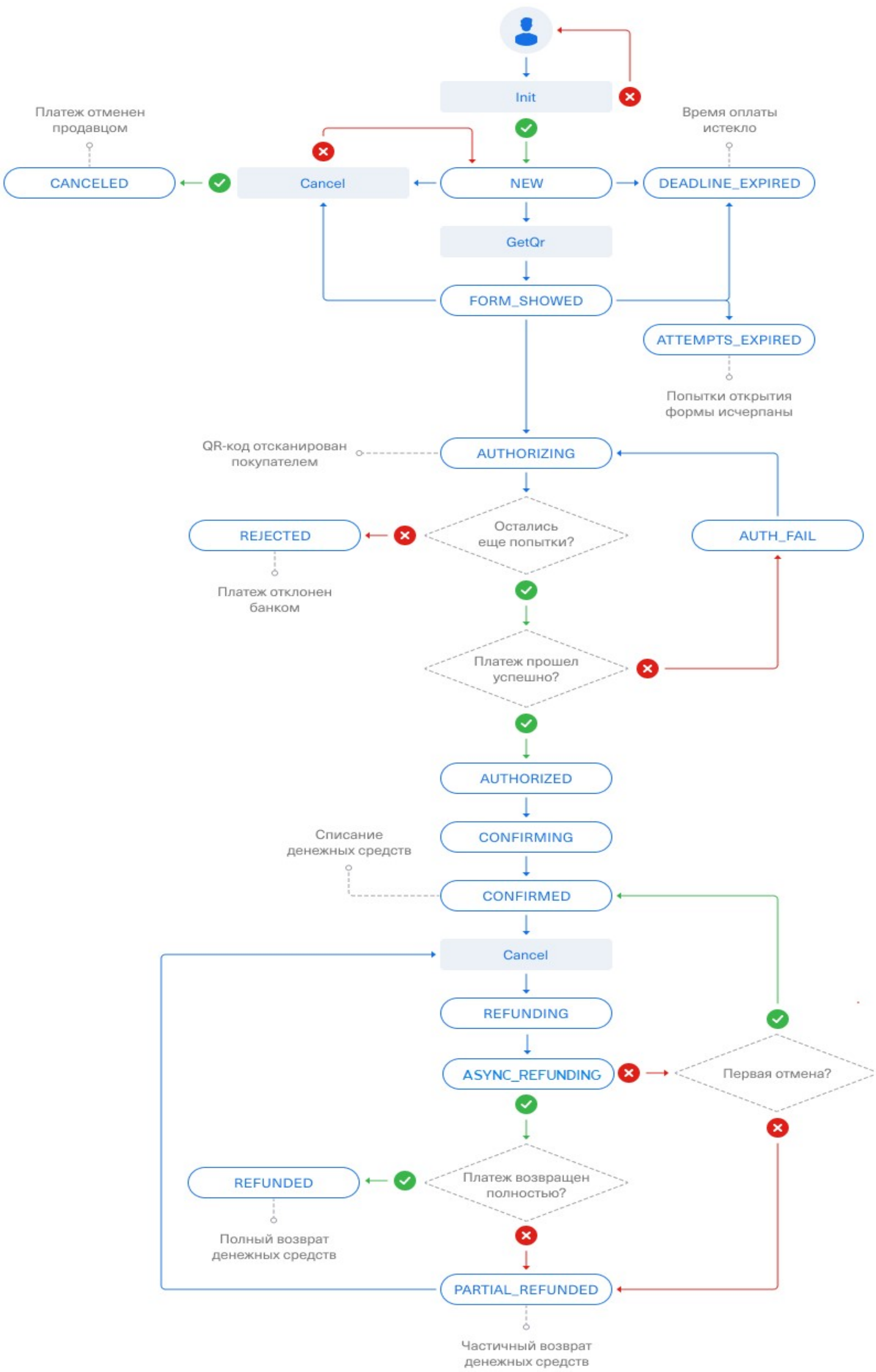
Наименование	Тип	Обязательность	Описание
QR	imageSVG	Нет	WebQR для T-Pay

3. Методы оплаты по QR

Метод для схемы PCI DSS

URL отправки запросов https://securepay.tinkoff.ru/v2/

3.1. Схема проведения платежа при оплате по QR



3.2. Метод GetQr

Метод для схемы PCI DSS

Описание: Регистрирует QR и возвращает информацию о нем. Должен быть вызван после вызова метода Init.

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/GetQr

Метод: POST

Таблица 3.2.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
DataType	String	Нет	Тип возвращаемых данных PAYLOAD – В ответе возвращается только Payload (по-умолчанию) IMAGE – В ответе возвращается SVG изображение QR
Token	String	Да	Подпись запроса

Пример запроса:

```
{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 3.2.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
Data	String	Да	В зависимости от параметра DataType в запросе это: Payload - информация, которая должна быть закодирована в QR или SVG изображение QR в котором уже закодирован Payload
PaymentId	Number	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

```
{
"TerminalKey":"TinkoffBankTest",
"OrderId":"21057",
"Success":true,
"Data":"https://qr.nspk.ru/AS1000670LSS7DN18SJQDNP4B05KLJL2?type=01&bank=100000000
001&sum=10000&cur=RUB&crc=C "PaymentId":10063,
"ErrorCode":"0"
}
```

3.3. Метод QrMembersList

Метод для схемы PCI DSS

Описание: Список участников куда может быть осуществлен возврат платежа, совершенного по QR.

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/QrMembersList

Метод: POST

Таблица 3.4.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
Token	String	Да	Подпись запроса

Пример запроса:

```
{
 "TerminalKey":"TinkoffBankTest",
 "PaymentId":"10063",
 "Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 3.4.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
Members	Array of objects	Нет	Массив списка участников. Возвращается только если возврат возможен
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки

Таблица 3.4.3. Параметры объекта Member

Наименование	Тип	Обязательность	Описание
MemberId	String	Да	Идентификатор участника
MemberName	String	Да	Наименование участника
IsPayee	Boolean	Да	true - если данный участник был получателем указанного платежа, false - в противном случае

Пример ответа:


```
{
  "Members": [
    {
      "MemberId": "1000000”,
      "MemberName": "АО\"Газпромбанк\"",
      "IsPayee": true
    },
    {
      "MemberId": "1000000",
      "MemberName": "ПАО \"Сбербанк\"",
      "IsPayee": false
    }
  ],
  "Success": true,
  "ErrorCode": "0",
  "Message": "OK"
}
```

3.4. Метод AddAccountQr

Метод для схемы PCI DSS

Описание: Инициирует привязку счета покупателя к магазину и возвращает информацию о нём

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/AddAccountQr

Метод: POST

Таблица 3.5.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала
Description	String	Да	Подробное описание деталей заказа
DataType	String	Нет	Тип возвращаемых данных PAYLOAD – В ответе возвращается только Payload (по-умолчанию) IMAGE – В ответе возвращается SVG изображение QR
DATA	Object	Нет	JSON объект, содержащий дополнительные параметры в виде “ключ”:” значение”. Данные параметры будут переданы на страницу оплаты (в случае ее кастомизации). Максимальная длина для каждого передаваемого параметра: ключ – 20 знаков; значение – 100 знаков Максимальное количество пар «ключ:значение» не может превышать 20
RedirectDueDate	Datetime	Нет	Срок жизни ссылки или динамического QR-кода СБП (если выбран данный способ оплаты)*. Если текущая дата превышает дату, переданную в данном параметре, ссылка для оплаты или возможность платежа по QR-коду становятся недоступными и платёж выполнить нельзя. Максимальное значение: 90 дней от текущей даты. Минимальное значение: 1 минута от текущей даты. Формат даты: YYYY-MM-DDTHH24:MI:SS+GMT Пример даты: 2016-08-31T12:28:00+03:00

Token	String	Да	Подпись запроса

* В случае, если параметр RedirectDueDate не был передан, проверяется настроечный параметр платежного терминала REDIRECT_TIMEOUT, который может содержать значение срока жизни ссылки в часах. Если его значение больше нуля, то оно будет установлено в качестве срока жизни ссылки или динамического QR-кода. Иначе, устанавливается значение «по умолчанию» - 1440 мин. (1 сутки).

Пример запроса:

```
{
  "TerminalKey":"TinkoffBankTest",
  "RedirectDueDate":"2016-08-31T12:28:00+03:00",
  “DataType”: “payload”,
  "Description": "Подписка в пользу АО\"Кофеек\", регулярность раз в месяц, сумма 100 рублей",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

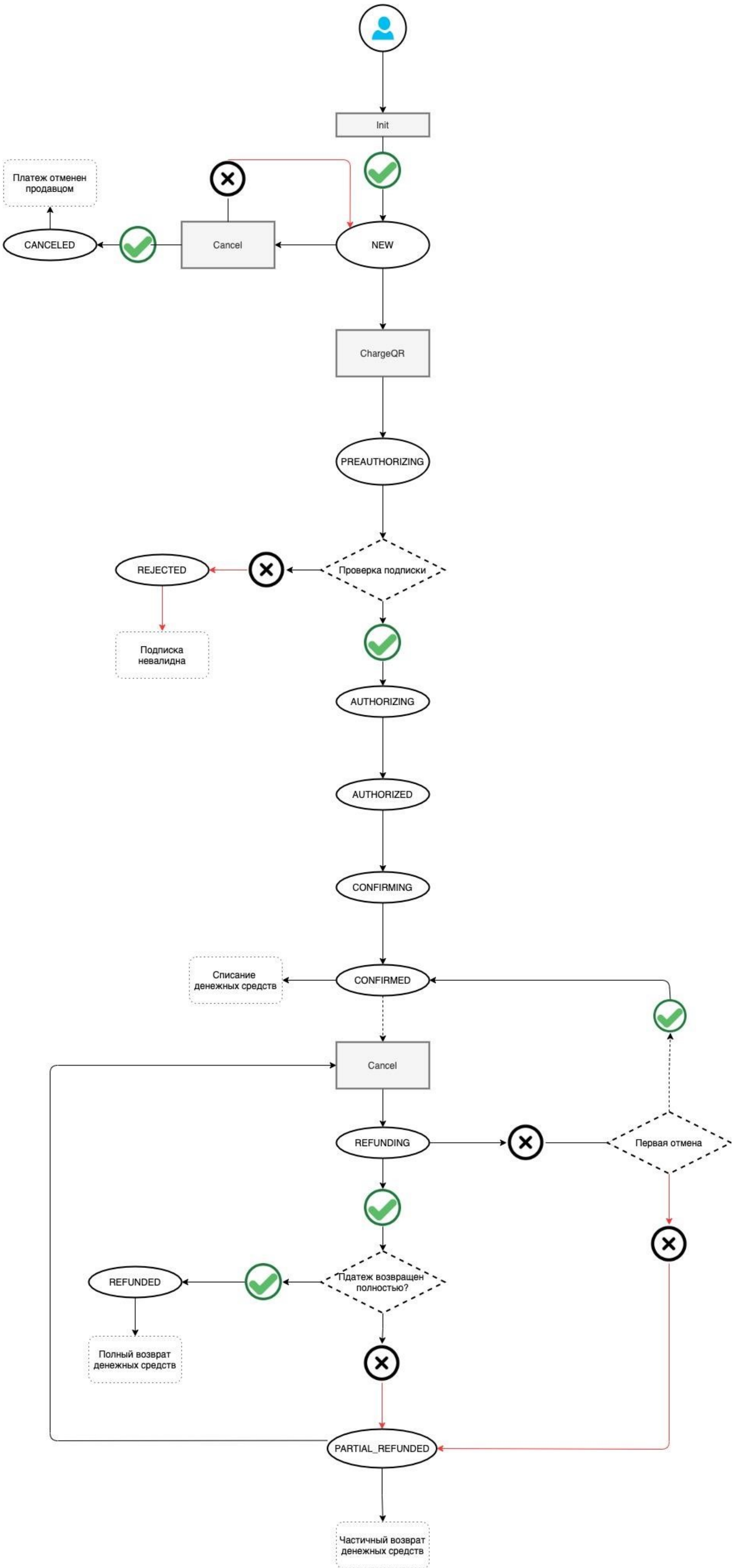
Формат ответа: JSON

Таблица 3.5.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала
Data	String	Да	В зависимости от параметра DataType в запросе это: Payload - информация, которая должна быть закодирована в QR, или SVG изображение QR, в котором уже закодирован Payload
RequestKey	String	Да	Идентификатор запроса на привязку счета
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно, Код ошибки, «3013» - "Рекуррентные платежи недоступны", Код ошибки, «3001» - "Оплата через QrPay недоступна"
Message	String	Нет	Краткое описание ошибки

Пример ответа:


```
{
   "TerminalKey":"TinkoffBankTest",
   "RequestKey":"AB1000670LSS7DN18SJQDNP4B05KLJL2",
   "Data":"https://qr.nspk.ru/AS1000670LSS7DN18SJQDNP4B05KLJL2?type=01&bank=10000000
   0001&sum=10000&cur=RUB&crc=C08B", "Success": true,
   "Message":"OK",
   "ErrorCode":"0"
}
```



Init
Платеж отменен продавцом
CANCELED
Cancel
NEW
ChargeQR
PREAUTHORIZING
REJECTED
Проверка подписки
Подписка невалидна
AUTHORIZING
AUTHORIZED
CONFIRMING
Списание денежных средств
CONFIRMED
Cancel
REFUNDING
Первая отмена
REFUNDED
Платеж возвращен полностью?
Полный возврат денежных средств
PARTIAL_REFUNDED
Частичный возврат денежных средств

3.5. Метод ChargeQr

Метод для схем PCI DSS \ Без PCI DSS

Проведение платежа по привязанному счету QR

Должен быть вызван после вызова метода Init, в котором передан параметр Reccurent =Y.

Описание: осуществляет рекуррентный платеж — списание денежных средств Покупателя по ранее привязанному счету.

Для совершения рекуррентного платежа Площадка должна вызвать метод Init, а затем вызвать метод ChargeQr для оплаты по тем же самым реквизитам и передать параметр AccountToken, полученный после привязки счета по QR

ChargeQr выполняет внутренние проверки и возвращает промежуточный результат.
Негативный - отказ на стороне Банка-эквайера, для уточнения причины см. Коды ошибок.
Позитивный - платеж передан в обработку НСПК и Банка-эмитента.
Конечным результатом обработки будет изменение статуса на CONFIRMED или CANCELED, который можно получить методом GetState или в автоматически отправляемой нотификации.

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/ChargeQr

Метод: POST

Таблица 3.6.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
AccountToken	String	Да	Идентификатор привязки счета, назначаемый Банком Плательщика
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес клиента
SendEmail	bool	Нет	true – если покупатель хочет получать уведомления на почту
InfoEmail	String	Нет (Обязателен при передаче SendEmail)	Адрес почты покупателя

Пример запроса:

```
{
"TerminalKey":"TinkoffBankTest",
"PaymentId":"10063",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
 “AccountToken”: “70LSS7DN18SJQRS10006DNPKLJL24B05”
}
```

Ответ

Формат ответа: JSON

Таблица 3.6.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Да	Номер заказа в системе Площадки
Success	bool	Да	Успешность прохождения запроса (true/false)
Status	String	Да	Статус транзакции
Amount	Number	Да	Сумма списания в копейках
Currency	Number	Да	Код валюты ISO 421.
PaymentId	String	Да	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Да	Код ошибки, «0» - если успешно, Код ошибки, «3013» - "Рекуррентные платежи недоступны", Код ошибки, «3015» - “Неверный статус AccountToken”
Message	String	Нет	Краткое описание ошибки

Пример ответа:

```
{
 "TerminalKey":"TinkoffBankTest",
 "OrderId":"21057",
 "Success":true,
"Status": “`OK“,
 "Amount": 100,
"Currency": “643“,
 "PaymentId":"10063",
 "ErrorCode":"0" }
```

3.6. Метод GetAddAccountQrState

Метод для схем PCI DSS \ Без PCI DSS

Описание: возвращает статус привязки счета Покупателя по магазину

Таблица 3.7.1. Статусы привязки счета

Наименование	Описание
NEW	Получен запрос на привязку счёту
PROCESSING	В обработке
ACTIVE	Привязка счета успешна
INACITVE	Привязка счета неуспешна/деактивирована

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/GetAddAccountQrState

Метод: POST

Таблица 3.7.2. Параметры запроса

Наименование	Тип	Обязательность	Описание
RequestKey	String	Да	Идентификатор запроса на привязку счета
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
Token	String	Да	Подпись запроса

Пример запроса:

```
{
  "TerminalKey":"TinkoffBankTest",
  "Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6",
  "RequestKey":"AB1000670LSS7DN18SJQDNP4B05KLJL2",
}
```

Ответ

Формат ответа: JSON

Таблица 3.7.3. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
RequestKey	String	Да	Идентификатор запроса на привязку счета
Status	String	Да	Статус привязки
BankMemberId	String	Нет	Идентификатор Банка Плательщика, который будет совершать оплату по привязанному счету - заполнен, если статус ACTIVE, INACTIVE
BankMemberName	String	Нет	Наименование Банка, заполнен если BankMemberId передан
Success	bool	Да	Успешность прохождения запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» - если успешно, Код ошибки, «3012» - “ Привязка счета не найдена”
Message	String	Нет	Краткое описание ошибки

Пример ответа:


```
{
  "TerminalKey":"TinkoffBankTest",
  "RequestKey": "AB1000670LSS7DN18SJQDNP4B05KLJL2",
  "Status": "NEW",
  "Success":true,
  "Message":"OK",
  "ErrorCode":"0"
}
```

3.7. Метод GetAccountQrList

Метод для схем PCI DSS \ Без PCI DSS

Описание: Возвращает список привязанных счетов покупателей по магазину

Запрос

Боевой URL: https://securepay.tinkoff.ru/v2/GetAccountQrList

Метод: POST

Таблица 3.8.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала
Token	String	Да	Подпись запроса

Пример запроса:

```
{
"TerminalKey": "1623341225522",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: Массив JSON

Таблица 3.8.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
RequestKey	String	Да	Идентификатор запроса на привязку счета
Status	String	Да	Статус привязки
AccountToken	String	Нет	Идентификатор привязки счета, назначаемый Банком Плательщика
BankMemberId	String	Нет	Идентификатор Банка Плательщика, который будет совершать оплату по привязанному счету - заполнен, если статус ACTIVE, INACTIVE
BankMemberName	String	Нет	Наименование Банка, заполнен, если BankMemberId передан
Success	bool	Да	Успешность прохождения запроса (true/false)

ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки

Пример ответа:


```
{
  "AccountTokens": [
    {
      "RequestKey": "AB1000670LSS7DN18SJQDNP4B05KLJL2",
      "Status": "ACTIVE",
      "AccountToken": "70LSS7DN18SJQRS10006DNPKLJL24B05",
      "BankMemberId": "100000000004",
      "BankMemberName": "Промсвязьбанк"
    },
    {
      "RequestKey": "AB1000670LSS7DN18SJQDNP4B05KLJL3",
      "Status": "ACTIVE",
      "AccountToken": "70LSS7DN18SJQRS10006DNPKLJL24B33",
      "BankMemberId": "100000000004",
      "BankMemberName": "Промсвязьбанк"
    }
  ],
  "TerminalKey": "TinkoffBankTest",
  "Success": true,
  "ErrorCode": "0",
  "Message": "OK"
}
```

4. Нотификации Площадки об операциях

Нотификации – это уведомления магазину о статусе выполнения платежа. На основании этих уведомлений магазин должен предоставлять услугу/товар покупателю.

4.1. Нотификации по электронной почте

Т-Банк Бизнес может присылать письма с уведомлениями об успешных платежах. Настроить нотификации на электронную почту можно по обращению в службу технической поддержки acq_help@tbank.ru. Уведомления на почту можно комбинировать с уведомлениями, отправляемыми по http(s).

4.2. Нотификации по http(s)

Описание: Т-Банк Бизнес может уведомлять магазин об успешных/ошибочных платежах и изменении статуса платежа. Для этого в настройках терминала необходимо указать URL, на который будут отправляться POST-запросы со статусами.

При вызове методов Authorize, FinishAuthorize, Confirm, Cancel на адрес Notification URL высылается уведомление POST-запросом с информацией об операции. При использовании одностадийного проведения платежа при обращении к методу FinishAuthorize нотификация отправляется на сайт Площадки на адрес Notification URL синхронно и ожидает ответа в течение 10 секунд. После получения ответа или неполучения его за заданное время сервис переадресует Покупателя на Success URL или Fail URL в зависимости от результата платежа.

В случае успешной обработки нотификации Площадка должна вернуть ответ с телом сообщения: OK (без тегов и заглавными английскими буквами).

Если тело сообщения отлично от OK, любая нотификация считается неуспешной, и сервис будет повторно отправлять нотификацию раз в час в течение 24 часов. Если нотификация за это время так и не доставлена, она складывается в дамп.

Вышесказанное так же действительно и при вызове метода Charge за исключением того, что данный метод не осуществляет переадресации Покупателя.

Если в NotificationURL используются порты, допустимо использование порта 443 (HTTPS).

Актуальный список внешних сетей*, используемых Т-Банком, для отправки нотификаций:

91.194.226.0/23

91.218.132.0/22

212.233.80.0/22

*Для корректной работы нотификаций необходимо добавить данные сети в исключения сетевых фильтров или других видов защиты в случае их использования.

URL: Notification URL

Метод: POST

Таблица 4.2.1. Параметры нотификации

Наименование	Тип	Описание
TerminalKey	String	Идентификатор терминала, выдается Площадке Банком
OrderId	String	Номер заказа в системе Площадки
Success	Boolean	Успешность прохождения запроса (true/false)
Status	String	Статус транзакции
PaymentId	String	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Код ошибки, «0» - если успешно
Amount	Number	Текущая сумма транзакции в копейках
CardId	Number	Если разрешена автоматическая привязка карт Покупателей к терминалу, и при вызове метода Init был передан параметр CustomerKey - в этот параметр будет передан идентификатор привязанной карты
Pan	String	Замаскированный номер карты/Замаскированный номер телефона
ExpDate	String	Срок действия карты
RebillId	String	Если при вызове метода Init платеж был помечен как рекуррентный - после подтверждения оплаты в этот параметр будет передан идентификатор рекуррентного платежа
Token	String	Подпись запроса. Формируется по такому же принципу, как и в случае запросов в банк
DATA	String	Дополнительные параметры платежа, переданные при создании заказа
SpAccumulationId	String	Идентификатор сделки (DealId). Вне зависимости от способа создания сделки ее идентификатор всегда возвращается в параметре SpAccumulationId вне блока DATA

* Параметры, передаваемые в нотификации, могут изменяться.
Рекомендуется проверять данные, полученные в нотификации:

1. Сеть, с которой будут приходить уведомления: 91.218.132.1, 91.218.133.1 и из списка, указанного выше.
2. Проверить Token.
3. Проверить сумму платежа.

4. Проверить идентификатор терминала.
5. Проверить номер заказа в системе Площадки.

Таблица 4.2.2. Статусы платежей, по которым приходят http(s)-нотификации

Status	Описание
AUTHORIZED	Деньги захолдированы на карте клиента. Ожидается подтверждение операции*
CONFIRMED	Операция подтверждена
REVERSED	Операция отменена
REFUNDED	Произведён возврат
PARTIAL_REFUNDED	Произведён частичный возврат
REJECTED	Списание денежных средств закончилась ошибкой
3DS_CHECKING	Автоматическое закрытие сессии, которая превысила срок пребывания в статусе 3DS_CHECKING (более 36 часов)**

***** Операция может быть подтверждена:

- Через Личный Кабинет;
- Запросом Confirm;
- Автоматически, если у магазина настроена одностадийная схема оплаты.

По неподтвержденным операциям возмещение не производится. Узнать статус платежа можно с помощью вызова метода GetState.

****** Для получения нотификаций по 3DS_CHECKING клиент должен реализовать на своей стороне возможность получения нотификаций со статусом DEADLINE_EXPIRED, а также написать на почту acq_help@tbank.ru с просьбой включить отправку нотификаций об автозакрытии сессий в статусе 3DS_CHECKING.

Пример http(s)-нотификации:

```
{
"TerminalKey":"1510572937960",
"OrderId":"test2",
"Success":true,
"Status":"CONFIRMED",
"PaymentId":"2006896",
"ErrorCode":"0",
"Amount":102120,
"CardId":867911,
```

"Pan":"430000**0777",
"ExpDate":"1122",
"Token":"d0815e288f121255d5d6b77831fb486cc5e9f91914a3f
58a99b6118b54676d84"
}

Ответ на HTTP(s)-нотификацию

В случае успешной обработки нотификации Площадке необходимо вернуть ответ HTTP CODE = 200 и с телом сообщения: OK (без тегов и заглавными английскими буквами).

PHP. Пример ответа на http(s)-нотификацию

```
<?php echo «OK»; ?>
```

Java. Пример ответа на http(s)-нотификацию

```
@POST
@Path("/ok")
public Response NotifyResponse() { return Response.status(200).entity("OK").build(); }
```

Если ответ «OK» не получен, нотификация считается неуспешной, и сервис будет повторно отправлять данную нотификацию раз в час в течение 24 часов.
Если нотификация за это время не доставлена, она будет сложена в архив.
При получении нотификации и перед её обработкой настоятельно рекомендуем проверить подпись.

Проверка токенов

Для формирования подписи запроса для нотификации необходимо:

1. Собрать массив всех передаваемых параметров в виде пар Ключ-Значение (кроме параметра Token). Например:
   [["TerminalKey","1321054611234DEMO"],["OrderId","201709"],["Success","true"],["Status","AUTHORIZED"],["PaymentId","8742591"],["ErrorCode","0"],["Amount","9855"],["CardId","322264"],["Pan","430000******0777"],["ExpDate","1122"],["RebillId ","101709"]]
2. Добавить в массив пару (Password, значение). Password – пароль для терминала, указан в Личном кабинете https://business.tbank.ru/:
   [["TerminalKey","1321054611234DEMO"],["OrderId","201709"],["Success","true"],["Status","AUTHORIZED"],["PaymentId","8742591"],["ErrorCode","0"],["Amount","9855"],["CardId","322264"],["Pan","430000******0777"],["ExpDate","1122"],["RebillId ","101709"],["Password", "Dfsfh56dgKl"]]
3. Отсортировать массив по Ключам по алфавиту:
   [["Amount","9855"],["CardId","322264"],["ErrorCode","0"],["ExpDate","1122"],["OrderId","201709"],["Pan","430000******0777"],["Password","Dfsfh56dgKl"],["PaymentId","8742591"],["RebillId","101709"],["Status","AUTHORIZED"],["Success","true"],[" TerminalKey","1321054611234DEMO"]]
4. Конкатенировать значения всех пар:
   98553222640112220170943000******0777Dfsfh56dgKl8742591101709AUTHORIZEDtrue1321054611234DEMO
5. Вычислить SHA-256 от полученного в п.4. значения:
   b906d28e76c6428e37b25fcf86c0adc52c63d503013fdd632e300593d165766b

Пример генерации токена:

```
private static final String PASSWORD_KEY = "Password"; private static final String PASSWORD_VALUE =
"12345678";
private String generateToken(final Map<String, String> parameters) throws
UnsupportedEncodingException,
NoSuchAlgorithmException { final Map<String, String> sortedParameters = new TreeMap<String,
String>(parameters); if (sortedParameters.containsKey(TOKEN)) { sortedParameters.remove(TOKEN);
}
sortedParameters.put(PASSWORD_KEY, PASSWORD_VALUE); final String paramString =
Joiner.on("").skipNulls().join(sortedParameters.values()); return calculateSha256(paramString);
}
```

Сравнение токенов

```
private boolean checkToken(final Map<String,String> params, final String expectedToken) { final String
actualToken = params.get(TOKEN); return !(expectedToken == null ||
!expectedToken.equals(actualToken));
}
```

4.3. Нотификация о привязке карты

Нотификации о привязке – это уведомления магазину о статусе выполнения метода привязки карты AttachCard.

После успешного выполнения метода AttachCard на адрес Notification URL высылается уведомление POST-запросом с информацией о привязке карты. Нотификация отправляется на сайт Площадки на адрес Notification URL синхронно и ожидает ответа в течение 10 секунд. После получения ответа или неполучения его за заданное время сервис переадресует Покупателя на Success AddCard URL или Fail AddCard URL в зависимости от результата привязки карты.

В случае успешной обработки нотификации Площадка должна вернуть ответ с телом сообщения: OK (без тегов и заглавными английскими буквами).

Если тело сообщения отлично от OK, любая нотификация считается неуспешной, и сервис будет повторно отправлять нотификацию раз в час в течение 24 часов. Если нотификация за это время так и не доставлена, она складывается в дамп.

URL: Notification URL

Метод: POST

Таблица 4.3.1. Параметры нотификации

Наименование	Тип	Описание
TerminalKey	String	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Идентификатор покупателя в системе Площадки
RequestKey	String	Идентификатор запроса на привязку карты
Success	bool	Успешность запроса
Status	String	Статус привязки
PaymentId	String	Уникальный идентификатор транзакции в системе банка
ErrorCode	String	Код ошибки, «0» - если успешно
CardId	Number	Идентификатор привязанной карты
Pan	String	Маскированный номер карты
ExpDate	String	Срок действия карты
NotificationType	String	Тип нотификации, всегда константа «LINKCARD»

RebillId	String	Идентификатор рекуррентного платежа
Token	String	Подпись запроса. Формируется по такому же принципу, как и в случае запросов в банк

Таблица 4.3.2. Статусы привязок, по которым приходят http(s)-нотификации

Status	Описание
COMPLETED	Карта успешно привязана
REJECTED	Привязка карты неуспешна

Пример http(s)-нотификации:


```
{
"TerminalKey":"1510572937960",
"CustomerKey":"G_customer5",
"RequestKey":"9ca9b229-dc31-4712-8e53-b3f9540869e5",
"Success": true,
"Status":"COMPLETED",
"PaymentId":”700000045896”,
"ErrorCode":"0",
"CardId":70000000857,
"Pan":"430000******0777",
"ExpDate":"1122",
"NotificationType":"LINKCARD",
"RebillId":"700000004090",
"Token":"f2fdd7fec8225872590e1558b7ea258c75df8f300d808006c41ab540dd7514d9"
}
```


Ответ на HTTP(s)-нотификацию

В случае успешной обработки нотификации Площадке необходимо вернуть ответ HTTP CODE = 200 и с телом сообщения: OK (без тегов и заглавными английскими буквами).

PHP. Пример ответа на http(s)-нотификацию

```
<?php echo «OK»; ?>
```

Java. Пример ответа на http(s)-нотификацию

```
@POST
@Path("/ok")
public Response NotifyResponse() { return Response.status(200).entity("OK").build(); }
```

Если ответ «OK» не получен, нотификация считается неуспешной, и сервис будет повторно отправлять данную нотификацию раз в час в течение 24 часов.

Если нотификация за это время не доставлена, она будет сложена в архив.

При получении нотификации и перед её обработкой настоятельно рекомендуем проверить подпись.

4.4 Нотификация о статусе привязки счета

Описание: После привязки счета по QR, магазину отправляется статус привязки и токен. Нотификация будет приходить по статусам ACTIVE и INACTIVE.

Таблица 4.6.1. Статусы привязки счета

Наименование	Описание
ACTIVE	привязка счета успешна
INACTIVE	привязка счета неуспешна/деактивирована

Запрос

URL: Notification URL
Метод: POST

Таблица 4.6.2. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
RequestKey	String	Да	Идентификатор запроса на привязку счета
Status	String	Да	Статус привязки
AccountToken	String	Нет	Идентификатор привязки счета - Token, назначаемый Банком
BankMemberId	String	Нет	Идентификатор Банка Плательщика, который будет совершать оплату по привязанному счету - заполнен, если статус ACTIVE
BankMemberName	String	Нет	Наименование Банка, заполнен если BankMemberId передан
NotificationType	String	Да	Тип нотификации, всегда константа «LINKACCOUNT»
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» если успешно

Message	String	Нет	Краткое описание ошибки
Token	String	Да	Подпись запроса. Формируется по такому же принципу, как и в случае запросов в банк

Пример http(s)-нотификации:

```
{
    "TerminalKey": "TinkoffBankTest",
    "RequestKey ": "AB1000670LSS7DN18SJQDNP4B05KLJL2",
    "Token": "871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6 ",
    "Status": "ACTIVE",
    "AccountToken": " 70LSS7DN18SJQRS10006DNPKLJL24B05",
    "BankMemberId": "100000000004",
    "BankMemberName": "Промсвязьбанк",
    "NotificationType": "LINKACCOUNT",
    "Success": true,
    "Message": "OK",
    "ErrorCode": "0"
},
```

Ответ на HTTP(s)-нотификацию

В случае успешной обработки нотификации Площадке необходимо вернуть ответ HTTP CODE = 200 и с телом сообщения: OK (без тегов и заглавными английскими буквами).

PHP. Пример ответа на http(s)-нотификацию

```
<?php echo «OK»; ?>
```

Java. Пример ответа на http(s)-нотификацию

```
{
@POST
@Path("/ok")
public Response NotifyResponse() {
return Response.status(200).entity("OK").build();
}
```

Если ответ «OK» не получен, нотификация считается неуспешной, и сервис будет повторно отправлять данную нотификацию раз в час в течение 24 часов.

Если нотификация за это время не доставлена, она будет сложена в архив.

5. Методы работы с привязанными картами и клиентами

Необходимо обратить внимание, что для корректной работы методов банком должна быть разрешена привязка карт и клиентов к терминалу Площадки.
В результате привязки карты к параметру CustomerKey будет привязана CardId.

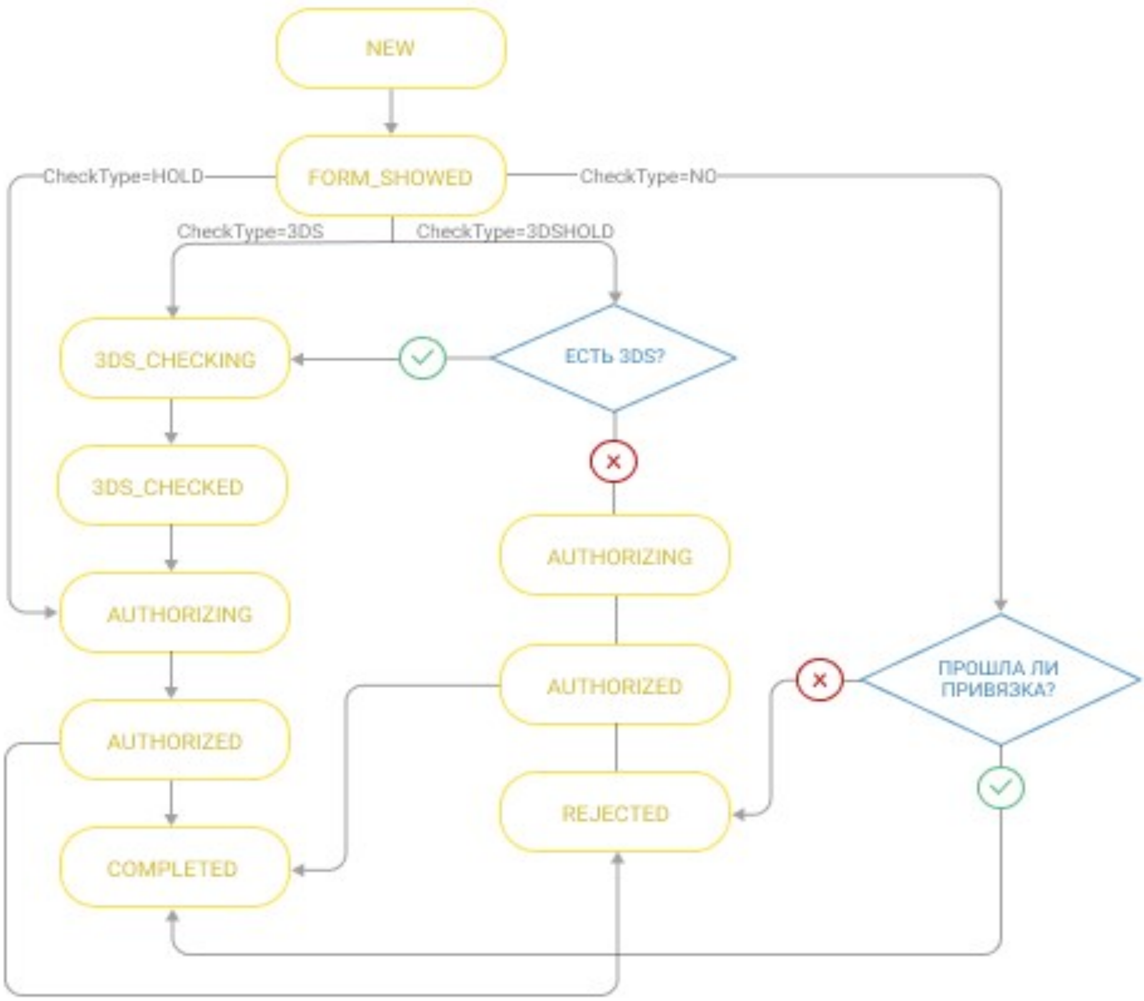


Рисунок 1. Статусная схема привязки карт

Описание статусов:

- NEW — новая сессия;
- FORM_SHOWED — показ формы привязки карты;
- 3DS_CHECKING — отправка пользователя на проверку 3DS
- 3DS_CHECKED — пользователь успешно прошел проверку 3DS;
- AUTHORIZING — отправка платежа на 0 руб.;
- AUTHORIZED — платеж на 0 руб. прошел успешно;
- COMPLETED — привязка успешно завершена;
- REJECTED — привязка отклонена.

5.1. Метод AddCustomer

Описание: Регистрирует покупателя в терминале Площадки.

Возможна автоматическая привязка покупателя и карты, по которой был совершен платеж, при передаче параметра CustomerKey в методе Init. Это можно использовать для сохранения и последующего отображения Покупателю замаскированного номера карты, по которой будет совершен рекуррентный платеж.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/AddCustomer
Боевой URL: https://securepay.tinkoff.ru/v2/AddCustomer
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.1.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес запроса
Email	String	Нет	Email клиента
Phone	String	Нет	Телефон клиента

Пример запроса:

```
{
"TerminalKey": "TinkoffBankTest",
"CustomerKey":"Customer1",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 5.1.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» – если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"TerminalKey": "TinkoffBankTest",
"CustomerKey": "Customer1",
"Success": true,
"ErrorCode": "0"
}

5.2. Метод GetCustomer

Описание: Возвращает данные покупателя, зарегистрированного в терминале Площадки.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/GetCustomer

Боевой URL: https://securepay.tinkoff.ru/v2/GetCustomer

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.2.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
IP	String	Нет	IP-адрес запроса
Token	String	Да	Подпись запроса

Пример запроса:

```
{
"TerminalKey": "TinkoffBankTest",
"CustomerKey: "Customer1",
"Token": "871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 5.2.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Success	bool	Да	Успешность запроса (true/false)

ErrorCode	String	Да	Код ошибки, «0» - успешно
Email	String	Нет	Email клиента
Phone	String	Нет	Телефон клиента (+71234567890)
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"TerminalKey": "TinkoffBankTest",
"CustomerKey": "Customer1",
"Success": true,
"ErrorCode": "0"
}

5.3. Метод RemoveCustomer

Описание: Удаляет сохраненные данные покупателя.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/RemoveCustomer

Боевой URL: https://securepay.tinkoff.ru/v2/RemoveCustomer
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.3.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Token	String	Да	Подпись запроса
IP	String	Нет	IP-адрес запроса

Пример запроса:
```
{
"TerminalKey": "TinkoffBankTest",
"CustomerKey": "Customer1",
"Token": "871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 5.3.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Success	bool	Да	Успешность запроса (true/false)

ErrorCode	String	Да	Код ошибки, «0» - если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"TerminalKey": "TinkoffBankTest",
"CustomerKey": "Customer1",
"Success": true,
"ErrorCode": "0"
}

5.4. Метод AddCard

Описание: Инициирует привязку карты к покупателю.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/AddCard

Боевой URL: https://securepay.tinkoff.ru/v2/AddCard

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.4.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Token	String	Да	Подпись запроса
CheckType	String	Нет	Есть CheckType не передается, автоматически проставляется значение NO. Возможные значения: – NO – сохранить карту без проверок. RebillID для рекуррентных платежей не возвращается; – HOLD – при сохранении сделать списание на 0 руб. RebillID возвращается для терминалов без поддержки 3DS. – 3DS – при сохранении карты выполнить проверку 3DS и выполнить списание на 0 р. В этом случае RebillID будет только для 3DS карт. Карты, не поддерживающие 3DS, привязаны не будут. – 3DSHOLD – при привязке карты выполняем проверку, поддерживает карта 3DS или нет. Для всех карт выполняется списание на 0р.
IP	String	Нет	IP-адрес запроса
ResidentState	Boolean	Нет	Признак резидентности добавляемой карты. Возможные значения: true - Карта РФ, false - Карта не РФ, null - Не специфицируется (универсальная карта)

Пример запроса:

{

"TerminalKey": "testRegressBank",
"CustomerKey": "testCustomer1234",
"CheckType": "HOLD",
"Token": "30797e66108934dfa3d841b856fdad227c6b9c46d6a39296e02dc800d86d181e",
"ResidentState": true
}

Ответ

Формат ответа: JSON

Таблица 5.4.2. Параметры ответа

Имя	Тип	Обязательность	Описание
PaymentId	Number	Да	Уникальный идентификатор транзакции в системе банка
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
RequestKey	String	Да	Идентификатор запроса на привязку карты
PaymentURL	String	Да	UUID, используется для работы без PCI DSS
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» если успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"PaymentId": 800000113483,
"Success": true,
"ErrorCode": "0",
"TerminalKey": "1485466639730",
"CustomerKey": "906540",
"PaymentURL": "82a31a62-6067-4ad8-b379-04bf13e37642d",
"RequestKey": "ed989549-d3be-4758-95c7-22647e03f9ec"
}

5.5. Метод AttachCard

Метод для схемы PCI DSS

Описание: Завершает привязку карты к покупателю.
В случае успешной привязки переадресует клиента на Success Add Card URL в противном случае на Fail Add Card URL.
Для прохождения 3DS второй версии перед вызовом метода должен быть вызван /v2/check3dsVersion и выполнен 3DS Method, который является обязательным при прохождении 3DS по протоколу версии 2.0.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/AttachCard
Боевой URL: https://securepay.tinkoff.ru/v2/AttachCard
*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.5.1. Параметры запроса

Имя	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
RequestKey	String	Да	Идентификатор запроса на привязку карты
CardData	String	Да	Зашифрованные данные карты в формате: "PAN=%pan%;ExpDate=%month%%year%;CVV=%secure_code%"
DATA*	Object	Нет	Ключ = значение дополнительных параметров через “|”, например, Email = a@test.ru|Phone = +71234567890. Если ключи или значения содержат в себе спец символы, то получившееся значение должно быть закодировано функцией urlencode. Максимальная длина для каждого передаваемого параметра: – Ключ – 20 знаков, – Значение – 100 знаков. Максимальное количество пар «ключ-значение» не может превышать 20
Token	String	Да	Подпись запроса

Пример запроса:

{
"TerminalKey":"testRegress",
"CardData":"U5jDbwqOVx+2vDApxe/rfACMt+rfWXzPdJ8ZXxNFVIiZaLZrOW72bGe9cKZdIDnekWOnqm88
YxRD↵jyfa5RuOkY5cQV
alU+juS1u1zpamSDtaGFeb8sRZfhj72yGw+io+qHGSBeorcfgoKStyKGuBPWfG↵dOPLHuyBE6QgZyIAM1Xf
dmNlVOUAxOnkTGDsskL
pIt3AWhw2e8KOarOvwbgCTDjznDB1/DLgOWO1↵Aj/bXyLJoG1BkOrPBm9JURs+f+uyFaeOhkRicNKNgXo
N5pJTSQxOEauOi6ylsVJ
B3WK5MNYXtj6x↵GlxcmTk/LD9kvHcjTeojcAlDzRZ87GdWeY8wgg==",
"RequestKey":"13021e10-a3ed-4f14-bcd1-823b5ac37390",
"Token":"7241ac8307f349afb7bb9dda760717721bbb45950b97
c67289f23d8c69cc7b96", }

***** ВАЖНО! Для 3DS второй версии в DATA необходимо передавать параметры, описанные в таблице DATA для 3DS v2 (см. выше на стр. 24). В HttpHeaders запроса обязательны заголовки: “User-Agent” и “Accept”.

Ответ

Формат ответа: JSON

Таблица 5.5.2. Параметры ответа

Имя	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
RequestKey	String	Да	Идентификатор запроса на привязку карты
CardId	String	Да	Идентификатор карты в системе банка
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Да	Код ошибки, «0» если успешно
Status	String	Нет	Статус привязки карты
RebillId	String	Нет	Идентификатор рекуррентного платежа
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:


```
{
  "Success": true,
  "ErrorCode": "0",
  "TerminalKey": "testRegress",
  "CustomerKey": "testRegress5",
  "RequestKey": "8de92934-26c9-474c-a4ce-424f2021d24d",
  "CardId": "5555",
  "RebillId": "130799909"
}
```


ВАЖНО! Если в ответе метода AttachCard возвращается статус 3DS_CHECKING, мерчанту необходимо сформировать запрос на URL ACS банка, выпустившего карту (в ответе параметр ACSUrl). Подробное описание метода описано выше на стр. 43.

5.6. Метод GetAddCardState

Описание: Возвращает статус привязки карты.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/GetAddCardState

Боевой URL: https://securepay.tinkoff.ru/v2/GetAddCardState

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.6.1. Параметры запроса

Имя	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
RequestKey	String	Да	Идентификатор запроса на привязку карты
Token	String	Да	Подпись запроса

Пример запроса:

```
{
 "TerminalKey": "testRegress",
 "RequestKey": "13021e10-a3ed-4f14-bcd1-823b5ac37390",
 "Token": "7241ac8307f349afb7bb9dda760717721bbb45950b97c67289f23d8c69cc1111"
}
```

Ответ

Таблица 5.6.2. Параметры ответа

Имя	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
RequestKey	String	Да	Идентификатор запроса на привязку карты
Status	String	Да	Статус привязки карты
Success	bool	Да	Успешность запроса (true/false)
ErrorCode	String	Нет	Код ошибки, «0» - если успешно
CustomerKey	String	Нет	Идентификатор покупателя в системе Площадки
CardId	String	Нет	Идентификатор карты в системе банка

RebillId	String	Нет	Идентификатор рекуррентного платежа
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:

{
"TerminalKey": "1213551193128",
"RequestKey": "c28a965b-7968-4d14-b05c-682b5221b8da",
"Status": "COMPLETED",
"Success": true,
"ErrorCode": "0",
"CustomerKey": "Test-112",
"CardId": "881000",
"RebillId": "130799276"
}

5.7. Метод GetCardList

Описание: Возвращает список привязанных карт покупателя. В том числе показывает удаленные карты.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/GetCardList

Боевой URL: https://securepay.tinkoff.ru/v2/GetCardList

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.7.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
IP	String	Нет	IP-адрес запроса
Token	String	Да	Подпись запроса

Пример запроса:

```
{
 "TerminalKey":"TinkoffBankTest",
 "CustomerKey":"Customer1",

"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b8
5e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: Массив JSON

Таблица 5.7.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
CardId	String	Да	Идентификатор карты в системе банка
Pan	String	Да	Номер карты 411111******1111
Status	String	Да	Статус карты: A – активная, I – не активная, D - удаленная

RebillId	String	Нет	Идентификатор рекуррентного платежа (см. параметр Recurrent в методе Init)
CardType	Enum	Да	Тип карты: – карта списания (0); – карта пополнения (1); – карта пополнения и списания (2)
ExpDate	String	Нет	Срок действия карты

Пример ответа:

[
{
"CardId": "881900",
"Pan": "518223******0036",
"Status": "D",
"RebillId": "",
"CardType": 0,
"ExpDate": "1122"
},
{
"CardId": "882263",
"Pan": "448744******4487",
"Status": "A",
"RebillId": "",
"CardType": 0,
"ExpDate": "0619"
}
]

5.8. Метод RemoveCard

Описание: Удаляет привязанную карту покупателя.

Запрос

Тестовый URL*: https://rest-api-test.tinkoff.ru/v2/RemoveCard

Боевой URL: https://securepay.tinkoff.ru/v2/RemoveCard

*Для возможности отправки запросов на тестовую среду напишите на почту acq_help@tbank.ru с просьбой добавить ваши IP в WL. Запрос необходимо отправлять с боевого терминала

Метод: POST

Таблица 5.8.1. Параметры запроса

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Идентификатор терминала, выдается Площадке Банком
CardId	String	Да	Идентификатор карты в системе банка
CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
IP	String	Нет	IP-адрес запроса
Token	String	Да	Подпись запроса

Пример запроса:

```
{
"TerminalKey":"TinkoffBankTest",
"CardId":"4750",
"CustomerKey":"Customer1",
"Token":"871199b37f207f0c4f721a37cdcc71dfcea880b4a4b85e3cf852c5dc1e99a8d6"
}
```

Ответ

Формат ответа: JSON

Таблица 5.8.2. Параметры ответа

Наименование	Тип	Обязательность	Описание
TerminalKey	String	Да	Платежный ключ, выдается Площадке при заведении терминала
CardId	String	Да	Идентификатор карты в системе банка

CustomerKey	String	Да	Идентификатор покупателя в системе Площадки
Status	String	Да	Статус карты: D – удалена
Success	bool	Да	Успешность запроса (true/false)
CardType	Enum	Да	Тип карты: – карта списания (0); – карта пополнения (1); – карта пополнения и списания (2).
ErrorCode	String	Да	Код ошибки, «0» - успешно
Message	String	Нет	Краткое описание ошибки
Details	String	Нет	Подробное описание ошибки

Пример ответа:


```
{
"Success": true,
"ErrorCode": "0",
"TerminalKey": "1509463751731DEMO",
"CustomerKey": "740892",
"CardId": "879157",
"Status": "D",
"CardType": 0
}
```

6. Коды ошибок, передаваемые на FailURL

Подробный список ошибок с описанием представлен в отдельном документе по следующей ссылке.

7. Список тестовых карт

Описание: Вы можете использовать любой срок действия для тестовой карты. Можно произвести несколько тестовых привязок с разными сроками действия и потом с помощью метода GetCardList посмотреть, какие карты привязаны. Тестовые карты используются при проведении операций на тестовой среде.

Таблица 7.1 Список тестовых карт для оплаты через протокол 3ds2.0

Поведение карты	TranStatus*	Описание	PAN
Ошибка оплаты Ошибка при списании	Нет	-	2201382000000021 expDate: 12/25 cvv: 123
Ошибка оплаты Недостаточно средств	Нет	Ошибка по карте возникает только при передаче значения Amount = 2233 в методе Init	2201382000000831 expDate: 12/25 cvv: 123
Успешная оплата 3ds 2.0 Frictionless Flow	Нет	AUTHENTICATION_SUCCESSFUL Успешное прохождение аутентификации без ввода пароля	2201382000000013 expDate: 12/25 cvv: 123
Успешная оплата 3ds 2.0 Challenge flow	C	CHALLENGE_REQURIED Требуется полное прохождение 3DS с редиректом на acsURL. Открытие формы для ввода одноразового пароля (OTP)	2201382000000047 expDate: 12/25 cvv: 123 Метод аутентификации на ACS: Static Passcode. Ввести верный пароль 1qwezxc
Ошибка оплаты 3ds2.0 Restricted	R	ACCOUNT_VERIFICATION_REJECTED Эмитент отклонил аутентификацию	2201382000000005 expDate: 12/25 cvv: 123
Ошибка оплаты Frictionless Flow Not Authenticated	N	NOT_AUTHENTICATED Карта не поддерживает 3DS	2201382000000021 expDate: 12/25 cvv: 123
Успешная оплата Card not Enrolled (Attempt)	A	ATTEMPTS_PROCESSING_PERFORMED Эмитент недоступен или не поддерживает 3DS v2.1. Платежная система разрешает провести Pay, но эмитент мог отклонить авторизацию	2201382000000039 expDate: 12/25 cvv: 123

Таблица 7.2 Список тестовых карт для оплаты через протокол 3ds1.0

Поведение карты	TranStatus*	Описание	PAN
Успешная оплата	Нет	-	5586200071492158 expDate: 12/25 cvv: 123
Ошибка оплаты Недостаточно средств при сумме авторизации >1000 рублей	Нет	-	5586200071499591 expDate: 12/25 cvv: 123

Таблица 7.3 Список тестовых карт для оплаты без 3ds

Поведение карты	TranStatus*	Описание	PAN
Успешная оплата	Нет	-	2200770239097761 expDate: 12/25 cvv: 123
Ошибка оплаты Недостаточно средств	Нет	-	4249170392197566 expDate: 12/25 cvv: 123
Ошибка оплаты Ошибка при списании	Нет	-	5586200071492075 expDate: 12/25 cvv: 123

***** Описание параметра TransStatus находится в описании параметров ответа cres (JSON/JWE cres объект)

8. Правила расчета возмещений по операционному реестру

При наличии РКО от Т-Банка выплаты производятся в календарные дни. При отсутствии – в дни работы расчетно-кассового центра по графику Центробанка.
Возмещение считается за один календарный день.

Таблица 8.1 Типы операций и их влияние на подсчет реестра

Тип операции	Пояснение	Плюс/минус
Debit	Операция оплаты	Плюс
Credit	Операция возврата	Минус
Fee	Комиссия по операции оплаты (в том числе неуспешной)	Минус
CancelRefund	Отмена возврата	Плюс
Chargeback	Опротестование операции эмитентом	Минус
2Chargeback	Арбитражное опротестование эмитентом	Минус
Chargeback_Reversal	Отмена опротестования операции эмитентом	Плюс
2Chargeback_Reversal	Отмена арбитражного опротестования операции эмитентом	Плюс
CR_Chargeback	Возврат операции Refund от эмитента (карта или договор закрыты)	Плюс
Representment	Обратное опротестование Chargeback Т-Банком	Плюс
Representment_Reversal	Отмена обратного опротестования 2Chargeback Т-Банком	Минус
AUTH_FAIL	Неуспешная авторизация. Сама операция в расчете не участвует. Участвует только комиссия за них.	-
CreditClientCorrection	FeeColl (Ручное урегулирование операции с банкомэмитентом по договоренности или при списании с Т-Банка по клирингу)	Минус
DebitClientCorrection	FeeColl (Ручное урегулирование операции с банкомэмитентом по договоренности или при списании с Т-Банка по клирингу)	Плюс
CreditCorrection	Списание с ТСП претензии клиента Т-Банка	Минус
DebitCorrection	Зачисление ТСП претензии клиента Т-Банка	Плюс