**Приложение к Договору №……**

**Порядок взаимодействия Торговой точки с платежным шлюзом Банка для оплаты товаров/услуг с использованием платежных карт.**

**1.Определения:**

*Платежный шлюз* – совокупность программных и аппаратных средств, выполняющих: 1) Обработку запросов Торговых точек на проведение операций. 2) Проведение операций 3) Передачу результатов проведения операций Торговым точкам.

*Секретный ключ* – набор случайных символов, сгенерированный модулем безопасности Банка для формирования HMAC.

*HMAC –* hash-based message authenticate code. Набор символов, сформированный при обработке входящих параметров по алгоритму SHA1 с использованием секретного ключа. HMAC передается отдельным параметром P\_SIGN в запросах Торговых точек к платежному шлюзу и передаче ответов на эти запросы обратно Торговым точкам. Предназначен для обеспечения целостности запроса и обоюдной аутентификации Банка и Торговой точки.

*Авторизация –* процедура получения разрешения на проведение операции у Банка, выпустившего карту.

**2. Общие положения:**

А) Перед проведением тестирования Торговая точка сообщает IP адрес сервера, доменное имя сервера, URL CGI-скрипта, обрабатывающего уведомления на запросы проведения операций и порт для отправки уведомлений о результатах проведения операций. Данные параметры отправляются на эл. адрес lakhtin@psbank.ru

Б) Банк присваивает и сообщает значение параметров TERMINAL и MERCHANT для производственной среды.

В) Банк генерирует и сообщает 2 компоненты секретного ключа для генерации HMAC запросов в производственной среде. Чистое значение секретного ключа Торговая точка получает после выполнения операции XOR над компонентами. Для тестовой среды Торговая точка использует следующие параметры:

TERMINAL = 79036768

MERCHANT = 790367686219999

KEY = C50E41160302E0F5D6D59F1AA3925C45

№ карты = 4268033703545624

Срок действия карты: 03/14 (ММ/ГГ)

Имя Держателя карты: TEST

CVV2: 516

**С МОМЕНТА ПЕРЕДАЧИ КОМПОНЕНТОВ СЕКРЕТНОГО КЛЮЧА ДЛЯ ГЕНЕРАЦИИ HMAC В ПРОИЗВОДСТВЕННОЙ СРЕДЕ ТОРГОВОЙ ТОЧКЕ, ОНА НЕСЕТ ПОЛНУЮ ОТВЕТСВЕННОСТЬ ЗА СОХРАННОСТЬ КОНФИДЕНЦИАЛЬНОСТИ ЗНАЧЕНИЙ ЭТИХ КОМПОНЕНТОВ.**

Г) Во избежание финансовых потерь, торговая точка **обязана** генерировать HMAC для каждого запроса на проведение любой операции и проверять HMAC каждого уведомления о результате проведения этих запросов.

**3. Алгоритм проведения операций:**

А) *Оплата –* Торговая точка формирует POST – запрос и отправляет его на сервер Банка. Для тестовой среды: http://193.200.10.117:8080/cgi-bin/cgi\_link. Для производственной среды: https://3ds.payment.ru/cgi-bin/cgi\_link. Список отправляемых Торговой точкой параметров для проведения оплаты: **AMOUNT,** **CURRENCY,** **ORDER,** **DESC,** **TERMINAL,** **TRTYPE,** **MERCH\_NAME,** **MERCHANT,** **EMAIL,** **TIMESTAMP,** **NONCE,** **BACKREF,** **P\_SIGN**. Названия параметров передаются в верхнем регистре. Порядок передачи параметров не важен. Описание параметров POST – запроса и допустимых значений приведены в соответствующей таблице. Банк получает запрос, проверяет HMAC (переданный параметром P\_SIGN), сформированный Торговой точкой, проводит авторизацию и отправляет результат проведения операции в виде POST – запроса по оговоренному заранее (п. 2А) с Торговой точкой URL. Список отправляемых Банком параметров по результату проведения оплаты: **AMOUNT, CURRENCY, ORDER, DESC, TERMINAL, TRTYPE, MERCH\_NAME, MERCHANT, EMAIL, TIMESTAMP, NONCE, BACKREF, RESULT, RC, RCTEXT, AUTHCODE, RRN, INT\_REF, P\_SIGN.**

Б) *Отмена* - Торговая точка формирует POST – запрос и отправляет его на сервер Банка. Для тестовой среды: http://193.200.10.117:8080/cgi-bin/cgi\_link. Для производственной среды: https://3ds.payment.ru/cgi-bin/cgi\_link. Список отправляемых Торговой точкой параметров для проведения отмены: **ORDER, AMOUNT, CURRENCY, ORG\_AMOUNT, RRN, INT\_REF, TRTYPE, TERMINAL, BACKREF, EMAIL, TIMESTAMP, NONCE, P\_SIGN.** Названия параметров передаются в верхнем регистре. Порядок передачи параметров не важен. Описание параметров POST – запроса и допустимых значений приведены в соответствующей таблице. Банк получает запрос, проверяет HMAC (переданный параметром P\_SIGN), сформированный Торговой точкой, проводит авторизацию и отправляет результат проведения операции в виде POST – запроса по оговоренному заранее (п. 2А) с Торговой точкой URL. Список отправляемых Банком параметров по результату проведения отмены: **ORDER, AMOUNT, CURRENCY, ORG\_AMOUNT, RRN, INT\_REF, TRTYPE, TERMINAL, BACKREF, EMAIL, TIMESTAMP, NONCE, RESULT, RC, RCTEXT, P\_SIGN.**

**4. Описание параметров POST – запроса и допустимых значений.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Название параметра** | **Формат данных / длина \*** | **Значение для оплаты (запрос от Торговой точки)** | **Значение для оплаты (ответ от Банка)** | **Значение для отмены (запрос от Торговой точки)** | **Значение для отмены (ответ от Банка)** | **Описание** |
| **AMOUNT** | числовой с десятичной точкой / 1-11 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Формирует Торговая точка | Транслируется из запроса Торговой точки | Сумма операции |
| **CURRENCY** | символьный / 3 | RUB, USD, EUR | Транслируется из запроса Торговой точки | RUR, USD, EUR | Транслируется из запроса Торговой точки | Валюта операции |
| **ORDER** | числовой / 6-32 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Транслируется из запроса на оплату | Транслируется из запроса Торговой точки | Уникальный номер заказа. |
| **DESC** | символьный / 50 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Не используется | Не используется | Описание заказа |
| **TERMINAL** | числовой / 8 | Торговая точка передает значение , присвоенное банком | Транслируется из запроса Торговой точки | Торговая точка передает значение , присвоенное банком | Транслируется из запроса Торговой точки | Уникальный номер виртуального терминала торговой точки. |
| **TRTYPE** | числовой / 1-2 | 1 | 1 | 24 | 24 | Тип запрашиваемой операции |
| **MERCH\_NAME** | символьный / 50 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Не используется | Не используется | Короткое название Торговой точки |
| **MERCHANT** | числовой / 12-15 | Торговая точка передает значение , присвоенное банком | Транслируется из запроса Торговой точки | Не используется | Не используется | Уникальный номер торговой точки. |
| **EMAIL** | символьный / 3 - 80 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Формирует Торговая точка | Транслируется из запроса Торговой точки | Адрес эл. почты Торговой точки |
| **TIMESTAMP** | числовой / 14 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Формирует Торговая точка | Транслируется из запроса Торговой точки | UTC время проведения операции в формате YYYYMMDDHHMISS (Московское время -4 часа) |
| **NONCE** | символьный / 16-32 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Формирует Торговая точка | Транслируется из запроса Торговой точки | Случайное число в шестнадцатеричном формате |
| **BACKREF** | символьный / 1-250 | Формирует Торговая точка | Транслируется из запроса Торговой точки | Формирует Торговая точка | Транслируется из запроса Торговой точки | URL для возврата на сайт Торговой точки после проведения операции |
| **P\_SIGN** | символьный / 40 | Формирует Торговая точка | Формирует Банк | Формирует Торговая точка | Формирует Банк | HMAC запроса |
| **RC** | числовой /1-2 | Не используется | Формирует Банк | Не используется | Формирует Банк | Respose Code. Код ответа на попытку проведения операции. |
| **RCTEXT** | символьный / 1-250 | Не используется | Формирует Банк | Не используется | Формирует Банк | Response Code Text. Расшифровка кода ответа на попытку проведения операции |
| **AUTHCODE** | символьный/ 6-32 | Не используется | Формирует Банк | Не используется | Формирует Банк | Код авторизации. Буквенно-цифровой код, выдаваемый банком, выпустившим карту, в случае успешной попытки проведения операции |
| **RRN** | числовой / 12 | Не используется | Формирует Банк | Транслируется из ответа на оплату | Транслируется из запроса Торговой точки | Retrieval Reference Number – Уникальный идентификатор запроса на списание средств с карты (RRN оплаты и отмены всегда совпадают) |
| **INT\_REF** | символьный / 1-32 | Не используется | Формирует Банк | Транслируется из ответа на оплату | Транслируется из запроса Торговой точки | Internal Reference – Уникальный идентификатор операции на платежном шлюзе (Int\_Ref оплаты и отмены всегда совпадают) |
| **RESULT** | Числовой / 1 | Не используется | 0 – операция успешно завершена  1 – запрос идентифицирован как повторный  2 – запрос отклонен Банком  3 – запрос отклонен Платежным шлюзом | Не используется | 0 – операция успешно завершена  1 – запрос идентифицирован как повторный  2 – запрос отклонен Банком  3 – запрос отклонен Платежным шлюзом | Результат обработки запроса на операцию. |
| **ORG\_AMOUNT** | числовой с десятичной точкой / 1-11 | Не используется | Не используется | Формирует Торговая точка | Транслируется из запроса Торговой точки | Сумма оригинальной операции (сумма оплаты) |

**\* Формат данных:** А) Числовой –содержит только числа Б) Символьный – может содержать любые печатаемые символы

**5. Алгоритм формирования HMAC.**

HMAC формируется в 2 этапа: 1 – формирование строки данных для HMAC. 2 – Формирование HMAC.

HMAC должен проверяться Банком при получении запроса на проведение операции от Торговой точки и при получении ответа по результату проведения операции от Банка Торговой точкой.

1) Если параметр участвует в формировании HMAC, то после его обработки для формирования HMAC, данные будут иметь вид: (длина значения параметра)+(значение параметра). Если же параметр, участвуя в формировании HMAC, не определен (передается с неопределенным значением), то в строку для формирования HMAC передается символ «-».

**ПРИМЕР:**

*Торговая точка передает POST-запрос с целью проведения операции оплаты. Среди прочих параметров присутствуют: AMOUNT=67.22, ORDER=123987, DESC=””, TERMINAL=”12365478”. Последовательность соединения параметров: AMOUNT, ORDER, DESC, TERMINAL.*

*В приведенном примере, строка для формирования HMAC будет выглядеть:*

***567.226123987-812365478***

2) Формируется HMAC по алгоритму SHA1 от подготовленной строки (в примере - **567.226123987-812365478**) с использованием секретного ключа Торговой точки. Ключ должен быть упакован в бинарную строку.

**ПРИМЕР ФОРМИРОВАНИЯ HMAC ДЛЯ PHP:**

<?php  
$hmac = hash\_hmac('sha1','подготовленная строка',pack('H\*', 'секретный ключ'));  
?>

3) Последовательность соединения Торговой точкой параметров в тестовой и производственной среде для:

А) Формирования HMAC запроса проведения оплаты товара:

**AMOUNT,CURRENCY,ORDER,MERCH\_NAME,MERCHANT,TERMINAL,EMAIL,TRTYPE,TIMESTAMP,NONCE,BACKREF**

Б) Проверки HMAC ответа на запрос проведения оплаты товара:

**AMOUNT,CURRENCY,ORDER,MERCH\_NAME,MERCHANT,TERMINAL,EMAIL,TRTYPE,TIMESTAMP,NONCE,BACKREF**, **RESULT, RC, RCTEXT, AUTHCODE, RRN, INT\_REF**

В) Формирования HMAC запроса проведения отмены:

**ORDER, AMOUNT, CURRENCY, ORG\_AMOUNT, RRN, INT\_REF, TRTYPE, TERMINAL, BACKREF, EMAIL, TIMESTAMP, NONCE**

Г) Проверки HMAC ответа на запрос проведения отмены:

**ORDER, AMOUNT, CURRENCY, ORG\_AMOUNT, RRN, INT\_REF, TRTYPE, TERMINAL, BACKREF, EMAIL, TIMESTAMP, NONCE, RESULT, RC, RCTEXT**