

**Инструкция для коммерсантов по
подключению к тестовой системе
интернет-эквайринга
АО «Банк ЦентрКредит»
API**

Таблица изменений

| ВЕРСИЯ | ДАТА | ОПИСАНИЕ ИЗМЕНЕНИЯ | ИЗМЕНЕНО |
|--------|------------|---|--------------------------|
| 0.1 | 01.01.2018 | Начальная версия | Банк ЦентрКредит |
| 0.2 | 10.04.2019 | Добавлено описание документа | Самбетбаев Айдос |
| 0.3 | 08.05.2019 | Добавлено описание документа | Самбетбаев Айдос |
| 0.4 | 07.06.2019 | Добавлено проверка соединения | Самбетбаев Айдос |
| 0.5 | 12.06.2019 | Добавлено памятки по переходу в промышленный режим | Самбетбаев Айдос |
| 0.6 | 10.07.2019 | Добавлено описание токена без авторизации | Самбетбаев Айдос |
| 0.7 | 18.07.2019 | Добавлено Информация по кодам ответа | Самбетбаев Айдос |
| 0.8 | 15.09.2019 | Добавления описания в рамках совершения рекуррентных платежей (подписки) | Гусляков Виктор Маркович |
| 0.9 | 31.01.2020 | Добавлено режим работы API | Алтайұлы Асылбек |
| 1.0 | 26.02.2020 | Расширен пункт 3. Макирование операций | Алтайұлы Асылбек |
| 1.1 | 06.03.2020 | Добавление операции P2P по токену | Алтайұлы Асылбек |
| 1.2 | 29.05.2020 | Разделение режимов работы WEB VIEW и API. Расширение пункта «Макирование операции» и подпункта «Возможные ошибки при проведении оплаты» | Алтайұлы Асылбек |
| 1.3 | 13.07.2020 | Доработан раздел Запрос на создание токена (TRTYPE=81) | Алтайұлы Асылбек |
| 1.4 | 16.07.2020 | Доработан раздел НОТИФИКАЦИИ | Алтайұлы Асылбек |
| 1.5 | 04.08.2020 | Расширен пункт «Покупка (Retail, TRTYPE=1)», обновлен пункт «P2P переводы (TRTYPE=8)» и добавлен пункт «Пример макирования запроса на P2P перевод (TRTYPE=8)» | Алтайұлы Асылбек |
| 1.6 | 13.08.2020 | Обновлены пункты: P2P переводы, P2P перевод с карты на токен, P2P перевод с токена на карту | Бейсембаева Назым |
| 1.7 | 03.09.2020 | Добавлены следующие пункты и подпункты: - Безопасная сделка (Отложенное списание, TRTYPE=12 & TRTYPE=21); -- Предварительная авторизация (TRTYPE=12); -- Завершение вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21); -- Пример макирования запроса предварительной авторизации (TRTYPE=12); -- Пример макирования запроса завершения вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21). Обновлен оформление инструкции. | Алтайұлы Асылбек |
| 1.8 | 16.09.2020 | Добавлены пункт: - 3DSecure API; - Поле M_INFO (Дополнительная информация по протоколу EMVCo 3DS v2). | Алтайұлы Асылбек |
| 1.9 | 12.11.2020 | Описан схема взаимодействия 3DSecure API | Алтайұлы Асылбек |
| 2.0 | 31.03.2021 | Дополнен подпункт 7 пункта Card without 3DSecure по параметру RND_AMOUNT | Алтайұлы Асылбек |
| 2.1 | 18.06.2021 | Актуализирована информацию про рекуррентных платежей | Алтайұлы Асылбек |

Оглавление

| | |
|--|----|
| ПАРАМЕТРЫ ДЛЯ ПОДКЛЮЧЕНИЯ | 6 |
| URL подключения | 6 |
| Тестовый ключ (для макирования) | 7 |
| Тестовые карты | 7 |
| ПЕРЕХОД В ПРОМЫШЛЕННЫЙ РЕЖИМ | 7 |
| ОПИСАНИЕ ОСНОВНЫХ ОПЕРАЦИЙ | 8 |
| Покупка (Retail, TRTYPE=1) | 9 |
| P2P переводы (TRTYPE=8) | 12 |
| P2P перевод с карты на токен | 12 |
| P2P перевод с токена на карту | 14 |
| Безопасная сделка (Отложенное списание, TRTYPE=12 & TRTYPE=21) | 16 |
| Предварительная авторизация (TRTYPE=12) | 16 |
| Завершение вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21)..... | 18 |
| Отмена покупки (Reversal, TRTYPE=22) | 20 |
| Запрос на создание токена (TRTYPE=81) | 21 |
| Удаление токена (TRTYPE=82) | 22 |
| Совершение рекуррентных платежей (TRTYPE=1 & TRTYPE=171)..... | 23 |
| Инициирование цепочки рекуррентных транзакций | 23 |
| Транзакции, инициированные ТСП, без участия клиента (Merchant Initiated Transaction) / MIT..... | 24 |
| Проверка соединения (TRTYPE=800) | 26 |
| МАКИРОВАНИЕ ОПЕРАЦИИ | 27 |
| Реализация MAC-подписи на Java | 28 |
| Реализация MAC-подписи на PHP..... | 28 |
| Реализация MAC-подписи на Python | 28 |
| Реализация MAC-подписи на JavaScript..... | 28 |
| Пример макирования запроса покупки (Retail, TRTYPE=1) | 30 |
| Пример макирования запроса на P2P перевод (TRTYPE=8) | 31 |
| Пример макирования запроса предварительной авторизации (TRTYPE=12)..... | 32 |
| Пример макирования запроса завершения вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21)..... | 33 |
| Пример макирования запроса отмены покупки (Reversal, TRTYPE=22) | 34 |
| Пример макирования запроса на создание токена (TRTYPE=81) | 35 |
| Пример макирования запроса на удаление токена (TRTYPE=82)..... | 36 |

| | |
|--|----|
| Пример макирования запроса на вторичную операцию периодического платежа (TRTYPE=171) | 37 |
| НОТИФИКАЦИИ | 38 |
| Поле M_INFO (Дополнительная информация по протоколу EMVCo 3DS v2) | 39 |
| 3DSecure v1 API | 46 |
| Card with 3DSecure | 46 |
| Card without 3DSecure | 48 |
| ТЕСТИРОВАНИЕ В СРЕДЕ SOAP UI | 51 |
| Настройка инструмента SOAP UI для проведения тестовых операций | 52 |
| ИНФОРМАЦИЯ ПО КОДАМ ОТВЕТА | 53 |
| FAQ | 54 |
| Если в бою MAC-подпись обязательна, зачем проводить тесты на 81140826? | 54 |
| Возможные ошибки при проведении оплаты | 54 |
| Код ответа банка: 05 – Transaction declined | 54 |
| Код ответа банка: 05 – Не оплачивать | 54 |
| Код ответа банка: 13 – Invalid account | 54 |
| Код ответа банка: 42 – No universal account | 54 |
| Код ответа банка: 51 – Недостаточно средств | 54 |
| Код ответа банка: 54 – Expired card | 54 |
| Код ответа банка: 57 – Транзакция запрещена | 54 |
| Код ответа банка: 61 – Превышен лимит на сумму | 54 |
| Код ответа банка: 65 – Exceeds frequency limit | 55 |
| Код ответа банка: 65 – Превышен лимит операций | 55 |
| Код ответа банка: 91 – Issuer unavailable | 55 |
| Error message: Authentication failed | 55 |
| Error message: Ошибка аутентификации | 55 |
| Error message: Duplicate transaction | 55 |
| Error message: Ошибка в номере карты | 55 |
| Error message: Ошибка в формате запроса | 55 |
| Error message: Отказано в доступе | 55 |
| Error message: Транзакция просрочена | 55 |
| Возможные ошибки при заполнении полей | 56 |
| ORDER=456321598733 (указан пример) | 56 |
| TIMESTAMP=201903141125 (указан пример) | 56 |
| NONCE=1344d7e1752b99 (указан пример) | 56 |

ПАРАМЕТРЫ ДЛЯ ПОДКЛЮЧЕНИЯ

URL подключения

URL адрес тестового eCommerce хоста, на который необходимо отправлять запросы:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link
```

Хост всегда доступен, отдельных доступов запрашивать не нужно.

Перед тем как перейти на промышленный режим:

- Надо определиться с видом нотификации и отправить необходимые данные в банк соответственно с выбором вида нотификации (по возможности во время тестирования). Это сэкономит время при переходе на промышленный режим после ваших успешных тестовых транзакций. Для настройки нотификации нужно предоставить информацию, как вы будете получать результаты транзакции (дополнительная информация находится в разделе НОТИФИКАЦИИ):
 - ✓ если нотификация на URL поддерживает SSL, то необходимо предоставить следующие данные:
 - по HTTPS:
 - сертификаты (CA_File, Cert, Key);
 - URL адрес;
 - PORT;
 - POST/GET;
 - логин и пароль (Basic Authentication);
 - поддерживает ли протокол TLS 1.2;
 - расположен ли ваш сайт на виртуальном хосте.
 - ✓ если нотификация на URL и этот URL защищен на уровне Basic Authentication, то необходимо предоставить следующие данные:
 - по HTTP/HTTPS:
 - URL адрес;
 - PORT;
 - POST/GET;
 - логин и пароль (Basic Authentication);
 - поддерживает ли протокол TLS 1.2;
 - расположен ли ваш сайт на виртуальном хосте.
 - ✓ если на E-Mail, то необходимо предоставить следующие данные:
 - электронный адрес получателя merchant@domain.com;
 - формат заголовка, тела письма для уведомления (желательно с примером).
 - Провести операцию через тестовую площадку *без макирования* и *с макированием* на успешное или неуспешное выполнение операции. Также предоставить данные об операциях, для проверки корректности всех моментов.
 - Запросы типов операции отправляется методом POST.

ID тестовых терминалов (указывается в параметре TERMINAL входящего запроса) для API без макирования терминал 81140826, с макированием терминал 81140825.

Тестовый ключ (для макирования)

Компоненты MAC ключа (криптографический ключ):

Key Component 1

Hex Value of Component: 690B5589573ACB3608DB7395A319B175

Key Check Value: CE503A

Key Component 2

Hex Value of Component: 02BBF98BB3411445D15498E2DC22E3E1

Key Check Value: C5225F

Из двух компонент необходимо собрать ключ с помощью операции XOR между компонентами. В интернете есть несколько сайтов, которые позволяют это сделать, например, этот: <https://toolslick.com/math/bitwise/xor-calculator>.

Собранный тестовый ключ:

6BB0AC02E47BDF73D98FEB777F3B5294

KCV: A4771B

Тестовые карты

| PAN | EXP DATE | CVV2 | RBS number | Country |
|------------------|----------|------|-----------------------------|---------|
| 5104450033134199 | 04/21 | 270 | ALM/18/P/190458-DC/271192 | KZT |
| 4899887654084306 | 07/21 | 423 | ALM/19/P/124837-C/19/205276 | KZT |
| 4012001037141112 | 12/27 | 212 | | USD |
| 4667208436889823 | 11/21 | 977 | ALM/17/P/132468-DC/194128 | KZT |
| 5204180487356910 | 11/20 | 852 | ALM/17/P/132468-DC/194128 | KZT |
| 5204180487694740 | 11/20 | 704 | ALM/17/P/132468-DC/194128 | KZT |

ПЕРЕХОД В ПРОМЫШЛЕННЫЙ РЕЖИМ

Для перехода в промышленный режим необходимо выполнить следующие действия:

1. Получить компоненты промышленного ключа;
2. Изменяем тестовый URL на промышленную:

```
https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link
```

3. Настраиваем промышленный номер терминала, который был присвоен коммерсанту;
4. Согласовать поля и их порядок, для макирования транзакций;
5. Провести операцию через площадку на успешное или неуспешное выполнение операции. Также предоставить данные об операциях, для проверки корректности всех моментов.

ОПИСАНИЕ ОСНОВНЫХ ОПЕРАЦИЙ

Типы операций (TRTYPE):

| | |
|-----|--|
| 1 | Запрос на выполнение финансовой части торговой операции |
| 8 | P2P платеж. |
| 12 | Предварительная авторизация |
| 21 | Завершение вторичной торговой операции со ссылкой на первичную транзакцию |
| 22 | Запрос отмены вторичной операции со ссылкой на первичную транзакцию. |
| 81 | Запрос на создание токена (регистрация карты). |
| 82 | Запрос на удаление токена (удаление зарегистрированной карты). |
| 171 | Вторичная операция периодического платежа. Обязательные поля RECUR_REF (RRN из первичной (оригинальной) транзакции) и INT_REF (ссылка на внутренний номер транзакции из первичной (оригинальной) транзакции). Номер карты PAN и срок действия карты не участвуют в проведении данной транзакции. |
| 800 | Проверка соединения |

Внимание! Платежи с использованием платежных карточек на территории Республики Казахстан осуществляются в национальной валюте Республики Казахстан – **тенге (398)**, за исключением случаев, предусмотренных статьей 6 Закона Республики Казахстан от 2 июля 2018 года "О валютном регулировании и валютном контроле".

Покупка (Retail, TRTYPE=1)

После отправки запроса клиенту на стороне мерчанта откроется сайт мерчанта или приложение мерчанта для ввода карточных данных держателя карты и другая информация. После ввода карточных данных и нажатия кнопки Одобрения клиенту будет отображено окно с результатами операции.

На стороне банка данные обрабатываются и результат операции будет предоставлен мерчанту в виде JSON.

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------------|---------------------------|--|
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, тенге-398) |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| DESC | 58 | Строка | 1-50 | Описание заказа |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| MERCH_GMT | 56 | Знак и число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММСС) |
| TRTYPE | 22 | Цифровое | 1 | Тип транзакции (Для операции покупки используется значение - 1) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| BACKREF | 41 | URL | 1-250 | URL сайта торговца для обратного перехода клиента на сайт торговца (значение должно содержать http://www или https://www в зависимости от протокола) |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |
| LANG | 31 | Строка | 2 | Язык транзакции. Значение данного поля будет использовано в качестве расширения файла сообщения. |
| CARD | 23 | Цифровое | 19 | Номер карты (PAN). Поле не является обязательным для транзакций с вводом PIN-кода. |
| EXP | 24 | Строка | 02 | Месяц окончания срока действия карты (двузначное число). Может быть представлено как список значений (01-12) для выбора необходимого значения: <code><option value="01">01 January</option></code> <code><option value="02">02 February</option></code> <code><option value="03">03 March</option></code> <code><option value="04">04 April</option></code> <code><option value="05">05 May</option></code> <code><option value="06">06 June</option></code> <code><option value="07">07 July</option></code> <code><option value="08">08 August</option></code> <code><option value="09">09 September</option></code> <code><option value="10">10 October</option></code> <code><option value="11">11 November</option></code> <code><option value="12">12 December</option></code> |
| EXP_YEAR | 32 | Цифровое | 02 | Год истечения срока действия карты (двузначное число). |
| CVC2 | 30 | Цифровое | 03 | Код проверки карты. CVV2/CVC2 карты |
| CVC2_RC | 50 | Цифровое | 01 | Код наличия CVC2. Должен быть представлен в виде списка следующих значений для выбора необходимого значения: <code><option selected value="1">CVC2 is present</option></code> (присутствует) <code><option value="0">CVC2 is not provided</option></code> (не предоставлен) <code><option value="2">CVC2 is illegible</option></code> (неразборчив) <code><option value="9">No CVC2 on card</option></code> (не указан на карте) |

Значения полей ORDER, TIMESTAMP, NONCE и P_SIGN необходимо актуализировать под каждый запрос.

Запросы необходимо отправлять методом POST. Пример запроса операции покупки:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?AMOUNT=10&CURRENCY=398&ORDER=654654200&DESC=12345&TRTYPE=1&TERMINAL=81140826&LANG=kz&CARD=5104450033134199&EXP=04&EXP_YEAR=21&CVC2=270&CVC2_RC=1&MERCHANT=TestShop&MERCH_GMT=6&TIMESTAMP=20200713064910&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA&BACKREF=https://www.testdomain.kz
```

Ответ:

```
{"AMOUNT": "10", "ORG AMOUNT": "", "CURRENCY": "398", "ORDER": "654654200", "DESC": "12345", "MERCH_NAME": "", "MERCHANT": "TestShop", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "1", "TIMESTAMP": "20200713064910", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "https://www.testdomain.kz", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT DIAG CODE": "NONE", "AUTHCODE": "157365", "RRN": "019585064562", "INT REF": "E2A4FD2DB2C1C529", "CARD": "5104XXXXXXXX4199", "TOKEN ID": "", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

Параметры, которые необходимо отправлять в запросе операции покупки с помощью токена:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------------|---------------------------|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, тенге-398) |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| DESC | 58 | Строка | 1-50 | Описание заказа |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| MERCH_GMT | 56 | Знак и число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММСС) |
| TRTYPE | 22 | Цифровое | 1 | Тип транзакции (Для операции покупки используется значение - 1) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| BACKREF | 41 | URL | 1-250 | URL сайта торговца для обратного перехода клиента на сайт торговца (значение должно содержать http://www или https://www в зависимости от протокола) |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |
| LANG | 31 | Строка | 2 | Язык транзакции. Значение данного поля будет использовано в качестве расширения файла сообщения. |
| MERCH_TOKEN_ID | 227 | Строка | 32 | Токен мерчанта |

Значения полей ORDER, TIMESTAMP, NONCE и P_SIGN необходимо актуализировать под каждый запрос.

Запросы необходимо отправлять методом POST. Пример запроса операции покупки с помощью токена (Создание токена описан в разделе *Запрос на создание токена (TRTYPE=81)*):

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?MERCH_TOKEN_ID=3930B105F9304BE448E161340E437D16&AMOUNT=10&CURRENCY=398&ORDER=1589347449458&DESC=PAYMENT1589347449227&MERCHANT=TestShop&TRTYPE=1&TERMINAL=81140826&MERCH_GMT=6&TIMESTAMP=20200713090709&NONCE=AC81B1FA25634EA595FF5FB8AE668610&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA&LANG=en&BACKREF=https://www.testdomain.kz
```

Ответ:

```
{"AMOUNT": "10", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "1589347449458", "DESC": "PAYME  
NT1589347449227", "MERCH_NAME": "", "MERCHANT": "TestShop", "TERMINAL": "81140826", "EMAIL":  
"", "TRTYPE": "1", "TIMESTAMP": "20200713090709", "NONCE": "AC81B1FA25634EA595FF5FB8AE66861  
0", "BACKREF": "https://www.testdomain.kz", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "  
EXT_DIAG_CODE": "NONE", "AUTHCODE": "157369", "RRN": "019585064574", "INT_REF": "80AE7B51A48  
99BC6", "CARD": "5104XXXXXXXX4199", "TOKEN_ID": "3930B105F9304BE448E161340E437D16", "P_SIG  
N": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

P2P переводы (TRTYPE=8)

В рамках разделения АСТ и ОСТ транзакции в тестовой среде, был реализован функционал перевода с карты на токен и с токена на карту.

Токен для тестирования на терминале без макирования (81140826):

4D1908A4B9FF4FDCDA4D9674B60E6145 – это токен карты **4667208436889823** 11/21

Токен для тестирования на терминале с макированием (81140825):

F02B7A2226BC4C08E00F5B578699986B – это токен карты **4667208436889823** 11/21

Создана страница тестовых P2P переводов с карты на токен и с токена на карту, по следующим адресам:

[e-Gateway P2P transaction from Card to Token](#)

[e-Gateway P2P transaction from Token to Card](#)

P2P перевод с карты на токен

Чтобы выполнить P2P перевод с карты на токен необходимо перейти по ссылке [e-Gateway P2P transaction from Card to Token](#). Переходим на страницу:

e-Gateway P2P transaction from Card to Token

| | |
|--|---|
| Enter your card number: | <input type="text"/> |
| Enter expiration date of your card: | 12 December ▼ 2020 ▼ |
| Enter your card CVC2 value: | <input type="text"/> (last three digits on the signature panel) |
| Enter token: | <input type="text" value="4D1908A4B9FF4FDCDA4D9674B60E6145"/> |
| Order amount: | <input type="text" value="10"/> |
| Order currency: | KZT ▼ |
| Email: | <input type="text"/> |
| Order number: | <input type="text" value="992859"/> |
| Merchant terminal: | 81140826 ▼ (Hidden field) |
| Description: | <input type="text" value="P2PFromCardToToken"/> |
| TRTYPE: | <input type="text" value="8"/> |
| Language: | <input type="text" value="kz"/> |
| Merchant: | <input type="text" value="P2PBCKZ"/> |
| MERCH_GMT: | <input type="text" value="6"/> |
| <input type="button" value="Approve"/> | |

Заполняете поля:

1. Enter your card number – Номер карты
2. Enter expiration date of your card – Срок действия карты
3. Enter your card CVC2 value – CVC код
4. Enter token:
Токен для тестирования на терминале без макирования (81140826):
4D1908A4B9FF4FDCDA4D9674B60E6145 – это токен карты **4667208436889823** 11/21
Токен для тестирования на терминале с макированием (81140825):
F02B7A2226BC4C08E00F5B578699986B – это токен карты **4667208436889823** 11/21
5. Order amount – Сумма
6. Order currency – Валюта
7. Email - Указывается адрес электронной почты получателя
8. Order number - Уникальный идентификатор перевода

9. Merchant terminal - Уникальный ID терминала

(Так как это тестовая страница и используется терминал без макирования заполнение этих данных достаточно. При тестировании с терминалом, который поддерживает макирование нужно дополнить строку запроса параметрами указанные ниже в таблице).

После заполнения нажимаете на **Approve**.

В запросе отправляется:

Данные карты отправителя в параметрах CARD, EXP, EXP_YEAR и CVC2;

Данные о получателе платежа (TOKEN) указывается в параметре MERCH_PAYTO_TOKEN_ID.

У параметра ORDER значение должно быть уникальным. В параметре EMAIL указывается адрес электронной почты получателя.

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|----------------------|----------|----------------|---------------------------|--|
| CARD | 23 | Цифровое | 19 | Номер карты (PAN). Поле не является обязательным для транзакций с вводом PIN-кода. |
| EXP | 24 | Строка | 02 | Месяц окончания срока действия карты (двузначное число). Может быть представлено как список значений (01-12) для выбора необходимого значения: <option value="01">01 January</option> <option value="02">02 February</option> <option value="03">03 March</option> <option value="04">04 April</option> <option value="05">05 May</option> <option value="06">06 June</option> <option value="07">07 July</option> <option value="08">08 August</option> <option value="09">09 September</option> <option value="10">10 October</option> <option value="11">11 November</option> <option value="12">12 December</option> |
| EXP_YEAR | 32 | Цифровое | 02 | Год истечения срока действия карты (двузначное число). |
| CVC2 | 30 | Цифровое | 03 | Код проверки карты. CVV2/CVC2 карты |
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, KZT->398, RUB->643, USD->840, EUR->978) |
| MERCH_PAYTO_TOKEN_ID | 231 | Строка | 32 | Токен торговца для P2P-транзакции. |
| EMAIL | 37 | E-mail | 80 | Адрес электронной почты получателя |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| DESC | 58 | Строка | 1-50 | Описание заказа торговца. В случае 3D-Secure транзакции данный параметр обязателен. |
| TRTYPE | 22 | Цифровое | 1 | Тип транзакции (для операции p2p перевода используется значение – 8) |
| LANG | 31 | Строка | 2 | Язык транзакции. Значение данного поля будет использовано в качестве расширения файла сообщения (kz, ru, en). |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса операции P2P на токен:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link?CARD=5104450033134199&EXP=04&EXP_YEAR=21&CVC2=270&AMOUNT=21&CURRENCY=398&MERCHANT_PAYTO_TOKEN_ID=4D1908A4B9FF4FDCDA4D9674B60E6145&EMAIL=emailofmerchant%40gmail.com&ORDER=811779&TERMINAL=81140826&DESC=BCCP2P&TRTYPE=8&LANG=kz&MERCHANT=testShop&MERCHANT_GMT=6&TIMESTAMP=20200804132400&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA
```

Ответ:

```
{"AMOUNT": "21", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "811779", "DESC": "BCCP2P", "MERCHANT_NAME": "", "MERCHANT": "testShop", "TERMINAL": "81140826", "EMAIL": "emailofmerchant@gmail.com", "TRTYPE": "8", "TIMESTAMP": "20200804132400", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "DS_ERROR", "AUTHCODE": "157499", "RRN": "021785066669", "INT_REF": "5BF2B2FC05EB2470", "CARD": "5104XXXXXXX4199", "TOKEN_ID": "", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

P2P перевод с токена на карту

Для осуществления P2P перевод с токена на карту необходимо перейти по ссылке [e-Gateway P2P transaction from Token to Card](#). Переходим на страницу:

e-Gateway P2P transaction from Token to Card

Enter token: 4D1908A4B9FF4FDCDA4D9674B60E6145

Enter card number: 5104450033134199

Order amount: 10

Order currency: KZT

Email:

Order number: 195038

Merchant terminal: 81140826 (Hidden field)

Description: P2PFromTokenToCard

TRTYPE: 8

Language: kz

Merchant: P2PBCKZ

MERCH_GMT: 6

Approve

Заполняете поля:

1. Enter token:
Токен для тестирования на терминале без макирования (81140826):
4D1908A4B9FF4FDCDA4D9674B60E6145 – это токен карты **4667208436889823** 11/21
Токен для тестирования на терминале с макированием (81140825):
F02B7A2226BC4C08E00F5B578699986B – это токен карты **4667208436889823** 11/21
2. Enter card number – Номер карты получателя платежа
3. Order amount – Сумма
4. Order currency – Валюта
5. Email – Указывается адрес электронной почты получателя
6. Order number - Уникальный идентификатор перевода
7. Merchant terminal - Уникальный ID терминала

(Так как это тестовая страница и используется терминал без макирования заполнение этих данных достаточно. При тестировании с терминалом, который поддерживает макирование нужно дополнить строку запроса параметрами указанные ниже в таблице).

После заполнения нажимаете на **Approve**.

В запросе отправляется MERCH_TOKEN_ID мерчанта. Номер карты получателя платежа указывается в параметре PAYMENT_TO. У параметра ORDER значение должно быть уникальным. В параметре EMAIL указывается адрес электронной почты получателя.

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|---------------|---------------------------|---|
| MERCH_TOKEN_ID | 227 | Строка | 32 | ТОКЕН |
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, KZT->398, RUB->643, USD->840, EUR->978) |
| PAYMENT_TO | 62 | Строка | 2-36 | Дополнительная информация о получателе платежа (Номер карты получателя) |
| EMAIL | 37 | E-mail | 80 | Адрес электронной почты получателя |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| DESC | 58 | Строка | 1-50 | Описание заказа торговца. В случае 3D-Secure транзакции данный параметр обязателен. |
| TRTYPE | 22 | Цифровое | 1 | Тип транзакции (для операции р2р перевода используется значение – 8) |
| LANG | 31 | Строка | 2 | Язык транзакции. Значение данного поля будет использовано в качестве расширения файла сообщения (kz, ru, en). |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧММ) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса операции P2P на карту:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link?MERCH_TOKEN_ID=4D1908A4B9FF4FDCDA4D9674B60E6145&AMOUNT=16&CURRENCY=398&PAYMENT_TO=5104450033134199&EMAIL=emailofclient%40gmail.com&ORDER=346802&TERMINAL=81140826&DESC=BCCP2P&TRTYPE=8&LANG=kz&MERCHANT=testShop&MERCH_GMT=6&TIMESTAMP=20200804132700&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDD A48FA
```

Ответ:

```
{"AMOUNT": "16", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "346802", "DESC": "BCCP2P", "MERCHANT_NAME": "", "MERCHANT": "testShop", "TERMINAL": "81140826", "EMAIL": "emailofclient@gmail.com", "TRTYPE": "8", "TIMESTAMP": "20200804132700", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "DS_ERROR", "AUTHCODE": "141177", "RRN": "021785066672", "INT_REF": "E2D2FE62DCF17A31", "CARD": "4667XXXXXXX9823", "TOKEN_ID": "4D1908A4B9FF4FDCDA4D9674B60E6145", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

Безопасная сделка (Отложенное списание, TRTYPE=12 & TRTYPE=21)

При оплате в интернет-магазине списание с карты/зачисление возмещения на счет мерчанта производится после дополнительного подтверждения о получении товара (с возможным изменением суммы платежа). Например, клиент на интернет портале, на базе eComm, производит приобретение товара, после приобретения товара происходит блокирование средств на карточном счете клиента. Факт списания происходит на момент получения товара.

Производится выполнение предварительной авторизации (TRTYPE=12), вслед за которой производится завершение торговой операции (TRTYPE=21), соответствующая авторизации (сумма финансовой операции может отличаться, как в большую, так и в меньшую сторону +50% и -50% от суммы предварительной авторизации).

Предварительная авторизация (TRTYPE=12)

Пример осуществления предварительной авторизации отражен по ссылке [e-Gateway Предварительная авторизация API](#). Переходим на страницу:

e-Gateway

Предварительная авторизация API

Enter your card number:

Enter expiration date of your card: 12 December ▾ 2020 ▾

Enter your card CVC2 value: (last three digits on the signature panel)

Enter your card CVC2_RC value: CVC2 указан ▾

Почтовый индекс клиента:

Почтовый адрес клиента:

Order amount:

Order currency: KZT ▾

Order number:

Описание:

Имя торговца:

URL сайта торговца:

Merchant:

Merchant terminal: 81140826 ▾

Email:

2-символьный код страны магазина торговца:

MERCH_GMT:

TIMESTAMP:

Список торговых марок, карты которых принимает торговец:

TRTYPE:

URL торговца для отправки результата авторизации:

NONCE:

P_SIGN:

(Так как это тестовая страница и используется терминал без макирования, такие параметры как TIMESTAMP, NONCE и P_SIGN не актуализированы. При тестировании с терминалом, который поддерживает макирование нужно актуализировать при каждом запросе эти параметры, включая ORDER).

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------------|---------------------------|--|
| CARD | 23 | Цифровое | 19 | Номер карты (PAN). Поле не является обязательным для транзакций с вводом PIN-кода. |
| EXP | 24 | Строка | 02 | Месяц окончания срока действия карты (двузначное число). Может быть представлено как список значений (01-12) для выбора необходимого значения: <option value="01">01 January</option> <option value="02">02 February</option> <option value="03">03 March</option> <option value="04">04 April</option> <option value="05">05 May</option> <option value="06">06 June</option> <option value="07">07 July</option> <option value="08">08 August</option> <option value="09">09 September</option> <option value="10">10 October</option> <option value="11">11 November</option> <option value="12">12 December</option> |
| EXP_YEAR | 32 | Цифровое | 02 | Год истечения срока действия карты (двузначное число). |
| CVC2 | 30 | Цифровое | 03 | Код проверки карты. CVV2/CVC2 карты |
| CVC2_RC | 50 | Цифровое | 01 | Код наличия CVC2. Должен быть представлен в виде списка следующих значений для выбора необходимого значения: <option selected value="1">CVC2 is present</option> (присутствует) <option value="0">CVC2 is not provided</option> (не предоставлен) <option value="2">CVC2 is illegible</option> (неразборчив) <option value="9">No CVC2 on card</option> (не указан на карте) |
| ZIP | 35 | Цифровое | 6 | Почтовый индекс клиента. |
| AVS | 36 | Строка | 80 | Почтовый адрес клиента. |
| AMOUNT | 25 | Цифровое | 12 | Общая сумма заказа |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| DESC | 58 | Строка | 1-50 | Описание заказа торговца. В случае 3D-Secure транзакции данный параметр обязателен. |
| MERCH_NAME | 53 | Строка | 1-50 | Имя торговца |
| MERCH_URL | 55 | Строка | 1-250 | URL сайта торговца |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| EMAIL | 37 | E-mail | 80 | Адрес электронной почты держателя карты для отправки счета |
| COUNTRY | 54 | Строка | 2 | 2-символьный код страны магазина торговца |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| BRANDS | 57 | Строка | 1-80 | Список торговых марок, карты которых принимает торговец (например, VISA, ЕМСС). |
| TRTYPE | 22 | Цифровое | 2 | Тип транзакции (Для операции предварительной авторизации используется значение - 12) |
| BACKREF | 41 | URL | 1-250 | URL сайта торговца для обратного перехода клиента на сайт торговца (значение должно содержать http://www или https://www в зависимости от протокола) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса операции предварительной авторизации:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?CARD=5104450033134199&EXP=04&EXP_YEAR=21&CVC2=270&CVC2_RC=1&ZIP=050040&AVS=address&AMOUNT=10&CURRENCY=398&ORDER=1234567965&DESC=testrequest&MERCH_NAME=ShopName&MERCH_URL=https://testdomain.kz&MERCHANT=shop&TERMINAL=81140826&EMAIL=testuser@gmail.com&COUNTRY=KZ&MERCH_GMT=6&TIMESTAMP=20200827043507&BRANDS=VISA,MasterCard&TRTYPE=12&BACKREF=https://www.testdomain.kz&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA
```

Ответ:

```
{ "AMOUNT": "10", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "1234567965", "DESC": "testrequest", "MERCH_NAME": "ShopName", "MERCHANT": "shop", "TERMINAL": "81140826", "EMAIL": "testuser@gmail.com", "TRTYPE": "12", "TIMESTAMP": "20200827043507", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "https://www.testdomain.kz", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "NONE", "AUTHCODE": "157604", "RRN": "024085068769", "INT_REF": "CBE572F7113499D7", "CARD": "5104XXXXXXXX4199", "TOKEN_ID": "", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA" }
```

Завершение вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21)

В параметре RRN и INT_REF указывается значения из ответа предварительной авторизации.

Пример осуществления предварительной авторизации отражен по ссылке [e-Gateway Завершение вторичной торговой операции со ссылкой на первичную транзакцию API](#). Переходим на страницу:

e-Gateway

Завершение вторичной торговой операции со ссылкой на первичную транзакцию API

| | |
|---|---|
| Order number: | <input type="text" value="141163"/> |
| Order amount: | <input type="text" value="16"/> |
| Order currency: | <input type="text" value="KZT"/> |
| Уникальный ссылочный номер транзакции из авторизационного ответа: | <input type="text"/> |
| Внутренний ссылочный номер из авторизационного ответа: | <input type="text"/> |
| TRTYPE: | <input type="text" value="21"/> |
| Merchant terminal: | <input type="text" value="81140826"/> |
| URL торговца для отправки итогового сообщения: | <input type="text" value="https://test3ds.bcc.kz:5445/endPreAuthAPI.html"/> |
| TIMESTAMP: | <input type="text"/> |
| NONCE: | <input type="text" value="F2E2DD7E603A7AAF5E1BC35DEE1F6C94"/> |
| P_SIGN: | <input type="text" value="8F9E1FC3A33C435749BE999A258D1257C32E6C7B"/> |
| <input type="button" value="Approve"/> | |

(Так как это тестовая страница и используется терминал без макирования, такие параметры как TIMESTAMP, NONCE и P_SIGN не актуализированы. При тестировании с терминалом, который поддерживает макирование нужно актуализировать при каждом запросе эти параметры, включая ORDER).

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------|---------------------------|---|
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| AMOUNT | 25 | Цифровое | 12 | Общая сумма заказа |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции |

| | | | | |
|-----------|----|----------------|-------|---|
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции из авторизационного ответа |
| INT_REF | 51 | Цифровое | 1-12 | Внутренний ссылочный номер из авторизационного ответа |
| TRTYPE | 22 | Цифровое | 2 | Тип транзакции (Для завершения вторичной торговой операции со ссылкой на первичную транзакцию используется значение - 21) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| BACKREF | 41 | URL | 1-250 | URL сайта торговца для обратного перехода клиента на сайт торговца (значение должно содержать http://www или https://www в зависимости от протокола) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧМ) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса завершения вторичной торговой операции со ссылкой на первичную транзакцию:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?ORDER=12345678956&AMOUNT=10&CURRENCY=398&RRN=024085068769&INT_REF=CBE572F7113499D7&TRTYPE=21&TERMINAL=81140826&BACKREF=https://www.testdomain.kz&TIMESTAMP=20200827043807&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA
```

Ответ:

```
{"AMOUNT": "10", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "12345678956", "DESC": "", "MERCHANT_NAME": "", "MERCHANT": "", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "21", "TIMESTAMP": "20200827043807", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "https://www.testdomain.kz", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "NONE", "AUTHCODE": "157603", "RRN": "024085068769", "INT_REF": "509DEE9BCC706588", "CARD": "", "TOKEN_ID": "", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

Отмена покупки (Reversal, TRTYPE=22)

Параметры, которые необходимо отправлять в запросе:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|---------------|---------------------------|--|
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| ORG_AMOUNT | 52 | Цифровое | 12 | Сумма исходной транзакции |
| AMOUNT | 25 | Цифровое | 12 | Отменяемая сумма |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции |
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции, приходит в уведомлении после совершения операции (Нужно указывать RRN той операции, которую требуется отменить) |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка, приходит в уведомлении после совершения операции (Нужно указывать INT_REF той операции, которую требуется отменить) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧМ) |
| TRTYPE | 22 | Цифровое | 2 | Тип транзакции (Для операции отмены покупки используется значение - 22) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса операции отмены покупки:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?ORDER=1590127770766&ORG_AMOUNT=10&AMOUNT=10&CURRENCY=398&RRN=019585064574&INT_REF=80AE7B51A4899BC6&TERMINAL=81140826&TIMESTAMP=20200713100930&TRTYPE=22&NONCE=A4601A0EF7084E6B85CC58199F37807F&P_SIGN=A17CD0B620AF61A66934EA6C74FC078A5965D594
```

Ответ:

```
{"AMOUNT": "10", "ORG_AMOUNT": "10", "CURRENCY": "398", "ORDER": "1590127770766", "DESC": "", "MERCH_NAME": "", "MERCHANT": "", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "22", "TIMESTAMP": "20200713100930", "NONCE": "A4601A0EF7084E6B85CC58199F37807F", "BACKREF": "", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "NONE", "AUTHCODE": "157369", "RRN": "019585064574", "INT_REF": "80AE7B51A4899BC6", "CARD": "", "TOKEN_ID": "", "P_SIGN": "A17CD0B620AF61A66934EA6C74FC078A5965D594"}
```

Запрос на создание токена (TRTYPE=81)

Для удобства постоянных клиентов, зарегистрированных в интернет-магазине, чтобы не вводить каждый раз при совершении покупки карточные реквизиты, есть возможность создания токена карты для дальнейшего проведения операций с использованием токена.

Создать запрос на токенизацию карты можно после любой успешно проведенной транзакции. То есть первую транзакцию клиент проводит с вводом карточных данных на странице банка, а все последующие операции уже проходят без перехода на данную страницу.

Для создания токена необходимо отправить запрос, содержащий следующие поля:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|---------------|---------------------------|--|
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции, приходит в уведомлении после совершения операции (Нужно указывать RRN операции по которой мы хотим создать токен для карты) |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка, приходит в уведомлении после совершения операции (Нужно указывать INT_REF операции по которой мы хотим создать токен для карты) |
| TRTYPE | 22 | Цифровое | | Тип транзакции (Для операции создания токена используется значение - 81) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧММ) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?ORDER=121021&RRN=019585064562&INT_REF=E2A4FD2DB2C1C529&TRTYPE=81&TERMINAL=81140826&MERCH_GMT=6&TIMESTAMP=20200713085800&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=5CEFB11D72E403994DF149E47CB56910DDDA48FA&LANG=kz
```

Ответ:

```
{"AMOUNT": "0", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "121021", "DESC": "", "MERCH_NAME": "", "MERCHANT": "", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "81", "TIMESTAMP": "20200713085800", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "", "AUTHCODE": "", "RRN": "019585064562", "INT_REF": "E2A4FD2DB2C1C529", "CARD": "5104XXXXXXXX4199", "TOKEN_ID": "3930B105F9304BE448E161340E437D16", "P_SIGN": "5CEFB11D72E403994DF149E47CB56910DDDA48FA"}
```

В результате будет сгенерирован токен - **3930B105F9304BE448E161340E437D16**.

Значение токена мерчант может получить при помощи нотификации. Инструкция нотификации указаны в пункте НОТИФИКАЦИИ.

В дальнейшем операции покупки можно выполнять по токену.

Удаление токена (TRTYPE=82)

Описание полей:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|---------------|---------------------------|--|
| MERCH_TOKEN_ID | 227 | Строка | 32 | ID токена который необходимо удалить |
| MERCH_GMT | 56 | Знак и число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧММСС) |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, KZT->398, RUB->643, USD->840, EUR->978) |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| TRTYPE | 22 | Цифровое | 2 | Тип транзакции (Для операции удаления токена используется значение - 82) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |

Запросы необходимо отправлять методом POST. Пример запроса:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?MERCH_TOKEN_ID=3930B105F9304BE448E161340E437D16&CURRENCY=398&ORDER=1589352821936&TRTYPE=82&TERMINAL=81140826&MERCH_GMT=6&TIMESTAMP=20200713094600&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=D78AA26A1030962939CF7090305C8EAA4CE0B71E
```

Ответ:

```
{"AMOUNT": "0", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "1589352821936", "DESC": "", "MERCHANT_NAME": "", "MERCHANT": "", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "82", "TIMESTAMP": "20200713094600", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "", "RESULT": "0", "RC": "0", "RCTEXT": "Approved", "EXT_DIAG_CODE": "", "AUTHCODE": "", "RRN": "", "INT_REF": "", "CARD": "", "TOKEN_ID": "3930B105F9304BE448E161340E437D16", "P_SIGN": "D78AA26A1030962939CF7090305C8EAA4CE0B71E"}
```

Совершение рекуррентных платежей (TRTYPE=1 & TRTYPE=171)

Рекуррентные платежи, также известные как платежи по подписке или «автоплатежи» — возможность выполнять регулярные списания денег с банковской карты покупателя без повторного ввода реквизитов карты и без участия плательщика для инициации очередного платежа.

Рекуррентные платежи всегда начинаются с первого (установочного) платежа, для выполнения которого плательщик должен ввести реквизиты своей карты. Для последующих регулярных платежей обязательно нужно ознакомить держателя карты с графиком и получить его согласие на безакцептное списание.

Инициирование цепочки рекуррентных транзакций

Параметры, которые необходимо для совершения первого платежа:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------------|---------------------------|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, тенге-398) |
| ORDER | 27 | Цифровое | 6-32 | Уникальный идентификатор заказа интернет торговца |
| DESC | 58 | Строка | 1-50 | Описание заказа |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |
| MERCH_GMT | 56 | Знак и число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММСС) |
| TRTYPE | 22 | Цифровое | 1 | Тип транзакции (Для операции покупки используется значение - 1) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |
| BACKREF | 41 | URL | 1-250 | URL сайта торговца для обратного перехода клиента на сайт торговца (значение должно содержать http://www или https://www в зависимости от протокола) |
| P_SIGN | 44 | Строка | 1-256 | Код аутентификации сообщений (MAC подпись запроса с использованием собранного ключа) |
| MERCH_TRAN_STATE | 130 | Строка | 1 | Индикатор инициирования <i>Cardholder Initiated Transaction</i> / <i>CIT</i> авторизации. Формат: (1 AN). В случае если операцию выполняет клиент (первая операция, необходимо использовать значение параметра S MERCH_TRAN_STATE='S' |
| MERCH_RN_ID | 129 | Строка | 16 | уникальный идентификатор, который формируется торговцем и используется при последующих рекуррентных авторизациях. Формат: (16 AN) |
| RECUR_FREQ | 179 | Цифровое | 1-4 | Частота периодических платежей: минимальное количество дней между авторизациями. Обычно это значение задается равным 28. Формат: Цифровое(1-4). |
| RECUR_EXP | 180 | ГГГГММДД | 8 | Дата окончания периодических платежей. После этой даты ни одна авторизация не будет обслужена. Формат: ГГГГММДД. Значение RECUR_EXP не должна быть позже истечения срока действия карты. |
| CARD | 23 | Цифровое | 19 | Номер карты (PAN). Поле не является обязательным для транзакций с вводом PIN-кода. |
| EXP | 24 | Строка | 02 | Месяц окончания срока действия карты (двузначное число). Может быть представлено как список значений (01-12) для выбора необходимого значения: <option value="01">01 January</option> <option value="02">02 February</option> <option value="03">03 March</option> <option value="04">04 April</option> <option value="05">05 May</option> <option value="06">06 June</option> <option value="07">07 July</option> |

| | | | | |
|----------|----|----------|----|--|
| | | | | <option value="08">08 August</option> <option value="09">09 September</option> <option value="10">10 October</option> <option value="11">11 November</option> <option value="12">12 December</option> |
| EXP_YEAR | 32 | Цифровое | 02 | Год истечения срока действия карты (двузначное число). |
| CVC2 | 30 | Цифровое | 03 | Код проверки карты. CVV2/CVC2 карты |
| CVC2_RC | 50 | Цифровое | 01 | Код наличия CVC2. Должен быть представлен в виде списка следующих значений для выбора необходимого значения: <option selected value="1">CVC2 is present</option> (присутствует) <option value="0">CVC2 is not provided</option> (не предоставлен) <option value="2">CVC2 is illegible</option> (неразборчив) <option value="9">No CVC2 on card</option> (не указан на карте) |

Запросы необходимо отправлять методом POST. Пример запроса операции покупки с подпиской:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?AMOUNT=1&CURRENCY=398&ORDER=1591579372815&MERCHANT=ZFSHOPAUTO&TERMINAL=81140826&MERCH_GMT=6&TIMESTAMP=20200624044951&TRTYPE=1&NONCE=55DB735425AF42B1AB07E87F4C4FB874&DESC=AUTOPayFirst&BACKREF=http%3A%2F%2Fwww.example.com&MERCH_TRAN_STATE=S&MERCH_RN_ID=8B7AFFD8F31A45E1&RECUR_FREQ=28&RECUR_EXP=20200925&CARD=5104450033134199&EXP=04&EXP_YEAR=21&CVC2=270&CVC2_RC=1&P_SIGN=C8CD6B2988A3F590AD92F7C440E25FB3
```

Ответ:

```
{ "AMOUNT": "1", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "1591579372815", "DESC": "AUTOPayFirst", "MERCH_NAME": "", "MERCHANT": "ZFSHOPAUTO", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "1", "TIMESTAMP": "20200624044951", "NONCE": "55DB735425AF42B1AB07E87F4C4FB874", "BACKREF": "http://www.example.com", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "NONE", "AUTHCODE": "157249", "RRN": "017685058523", "INT_REF": "EBA95E9505CE4F03", "CARD": "5104XXXXXXXX4199", "TOKEN_ID": "", "P_SIGN": "C8CD6B2988A3F590AD92F7C440E25FB3" }
```

Внимание!

В ответном сообщении торговец получает идентификаторы **RECUR_REF** (RRN) и **INT_REF**. Данные значения торговец должен сохранить у себя в цепочке рекуррентных сообщений вместе с **MERCH_RN_ID** и использовать при последующих операциях.

Транзакции, инициированные ТСП, без участия клиента (Merchant Initiated Transaction) / MIT

Параметры, которые необходимо для совершения повторяющего платежа:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------|---------------------------|--|
| TRTYPE | 22 | Цифровое | 3 | Тип транзакции (Вторичная операция периодического платежа используемое значение - 171) |
| MERCH_TRAN_STATE | 130 | Строка | 1 | Индикатор инициирования <i>Merchant Initiated Transaction</i> / MIT авторизации. Формат: (1 AN). В случае если операцию выполняет клиент (вторичная операция, необходимо использовать значение параметра M MERCH_TRAN_STATE='M') |
| MERCH_RN_ID | 129 | Строка | 16 | уникальный идентификатор, который формируется торговцем и используется при последующих рекуррентных авторизациях. Формат: (16 AN) |
| RECUR_REF | 181 | Цифровое | 12 | Ссылка на авторизацию при периодических платежах. (код оригинальной авторизации RRN) |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка. Поле является обязательным для вторичных транзакций со ссылкой на первичную транзакцию. Должно соответствовать полю INT_REF исходного ответа. |

| | | | | |
|----------|----|----------|----|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма транзакции |
| CURRENCY | 26 | Строка | 3 | Валюта транзакции (Необходимо передавать код валюты, тенге-398) |

Запросы необходимо отправлять методом POST. Пример запроса:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link/?TERMINAL=81140826&TRTYPE=171&MERCH_RN_ID=8B7AFFD8F31A45E1&RECUR_REF=017685058523&INT_REF=EBA95E9505CE4F03&LANG=kz&AMOUNT=1&CURRENCY=398&MERCH_TRAN_STATE=M&ORDER=12345679850&TIMESTAMP=20200624051800&NONCE=E891AD5AE1C9DD32493B5C2897EDA12E&P_SIGN=C8CD6B2988A3F590AD92F7C440E25FB3
```

Ответ:

```
{"AMOUNT": "1", "ORG_AMOUNT": "", "CURRENCY": "398", "ORDER": "12345679850", "DESC": "", "MERCH_NAME": "", "MERCHANT": "", "TERMINAL": "81140826", "EMAIL": "", "TRTYPE": "171", "TIMESTAMP": "20200624051800", "NONCE": "E891AD5AE1C9DD32493B5C2897EDA12E", "BACKREF": "", "RESULT": "0", "RC": "00", "RCTEXT": "Approved", "EXT_DIAG_CODE": "NONE", "AUTHCODE": "157250", "RRN": "017685058524", "INT_REF": "50C29B7A29C2B5E2", "CARD": "", "TOKEN_ID": "", "P_SIGN": "C8CD6B2988A3F590AD92F7C440E25FB3"}
```

Проверка соединения (TRTYPE=800)

Для проверки соединения необходимо отправить запрос, содержащий следующие поля:

| Название параметра | Код поле | Тип | Длина допустимых значений | Описание |
|--------------------|----------|----------|---------------------------|---|
| TRTYPE | 22 | Цифровое | 3 | Тип транзакции (Для операции используется значение - 800) |
| TERMINAL | 21 | Строка | 8 | Уникальный ID терминала (предоставляется банком) |

Запросы необходимо отправлять методом POST. Пример запроса:

```
https://test3ds.bcc.kz:5445/cgi-bin/cgi_link?TERMINAL=81140826&TRTYPE=800&LANG=kz
```

Ответ:

```
{"AMOUNT":"0","ORG_AMOUNT":"","CURRENCY":"840","ORDER":"","DESC":"","MERCH_NAME":"","MERCHANT":"","TERMINAL":"81140826","EMAIL":"","TRTYPE":"800","TIMESTAMP":"20200804155827","NONCE":"","BACKREF":"","RESULT":"0","RC":"0","RCTEXT":"Approved","EXT_DIAG_CODE":"","AUTHCODE":"","RRN":"","INT_REF":"","CARD":"","TOKEN_ID":"","P_SIGN":""}
```

МАКИРОВАНИЕ ОПЕРАЦИИ

Макирование – это средство обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных. MAC обычно применяется для обеспечения целостности и защиты от фальсификации передаваемой информации.

API с целью использования проверки тестовой операций с MAC подписью заведен терминал 88888881.

В зависимости от типа операции указанные **поля идут в строгой последовательности, без лишних дополнительных полей**. Например, строка источника MAC TRTYPE=1 (Retail) содержит поля "25,26,27,29,21,56,47,22,61". По необходимым типам транзакции более подробные примеры описаны ниже. Чтобы аутентифицировать запросы, поступающие на шлюз электронной коммерции, торговая система мерчанта должна иметь возможность вычислять и проверять коды аутентификации запросов. Запросы, которые отправляются в шлюз электронной коммерции, должны быть подписаны MAC ключом. MAC вычисляется по указанным в примерах полям (за исключением поля P_SIGN). Торговая система мерчанта должна собирать строку источника для макирования из указанных в таблицах значений полей. Перед значением каждого поля проставляется префикс длины поля. Если поле по какой-то причине отсутствует, то вместо него необходимо указывать символ тире «-». После сборки строки источника MAC торговая система мерчанта должна применять криптографический алгоритм для генерации MAC кода аутентификации сообщения. Торговая система мерчанта должна реализовать выбранный алгоритм либо в виде аппаратного или программного обеспечения, либо полностью отвечать за безопасное хранение и использование соответствующих криптографических ключей. Эффективная длина ключа должна быть не менее 112 бит для симметричных криптографических алгоритмов и 1024 бит для алгоритма RSA. Алгоритм MAC по умолчанию - HMAC_SHA1. Стандартные опции включают Triple DES ABA / ABC CBC MAC, AES 128 CBC MAC и RSA / SHA1. Полученное значение строки источника шифруется собранным MAC ключом и указывается в поле P_SIGN входящего сообщения. Проверить правильно ли формируется значение поля P_SIGN, вы можете использовать сайт: <https://www.liavaag.org/English/SHA-Generator/HMAC/> Здесь в поле Input будет ваша строка источника для макирования. Input Type: TEXT. Key: ключ собранный с двух компонентов. Key type: HEX. SHA variant: SHA-1. Output type: HEX. В поле Result будет показан значение поля P_SIGN. Пример показан на скрине:

Input

516.64339818Order355871446156812merchantname888888881161420200224073921113

Input Type

TEXT

Key

6BBoACo2E47BDF73D98FEB77F3B5294

Key type

HEX

SHA variant

SHA-1

Output type

HEX

Result

6a252740a6677ae140docob7937d22428df6dc7f

Реализация MAC-подписи на Java

Обратите внимание, что при формировании MAC подписи, необходимо предварительно перевести данные в HEX формат.

```
public static String getHac(String dataUno, String keyUno) {
    try {
        Mac mac = Mac.getInstance("HmacSHA1");
        byte[] keyBytes = Hex.decodeHex(keyUno.toCharArray());
        SecretKeySpec secretKey = new SecretKeySpec(keyBytes,
mac.getAlgorithm());
        mac.init(secretKey);
        byte[] text = dataUno.getBytes("UTF-8");
        byte[] encodedText = mac.doFinal(text);
        byte[] hexBytes = new Hex().encode(encodedText);
        return new String(hexBytes, "UTF-8");
    } catch (Exception e) {
        throw new RuntimeException(e);
    }
}
```

Реализация MAC-подписи на PHP

Обратите внимание, что при формировании MAC подписи, необходимо предварительно перевести данные в HEX формат.

```
$key = "6BB0AC02E47BDF73D98FEB777F3B5294";
$data =
"516.64339813355871446156812merchantname8811408251614202002240739211132F2B2DD7E603A7A
AF5E1BC35DEE1F6C9A";
$decodedKey = pack("H*", $key);
echo hash_hmac("sha1", $data, $decodedKey);
```

Реализация MAC-подписи на Python

Обратите внимание, что при формировании MAC подписи, необходимо предварительно перевести данные в HEX формат.

```
import hmac
import hashlib
key = "6BB0AC02E47BDF73D98FEB777F3B5294"
data =
"516.64339813355871446156812merchantname8811408251614202002240739211132F2B2DD7E603A7A
AF5E1BC35DEE1F6C9A"
decodedKey = key.decode("hex")
hmac = hmac.new(decodedKey, data.encode('UTF-8'), hashlib.sha1)
pSign = hmac.digest().encode('hex')
print "pSign = ", pSign
```

Реализация MAC-подписи на JavaScript

Обратите внимание, что при формировании MAC подписи, необходимо предварительно перевести данные в HEX формат.

```
const jsSHA = require('jssha');
```

```
const key = "6BB0AC02E47BDF73D98FEB777F3B5294";
const data =
`516.64339813355871446156812merchantname8811408251614202002240739211132F2B2DD7E603A7A
AF5E1BC35DEE1F6C9A`
var shaObj = new jsSHA("SHA-1", "TEXT");
shaObj.setHMACKey(key, "HEX");
shaObj.update(data);
const pSign = shaObj.getHMAC("HEX").toUpperCase();
```

Пример макирования запроса покупки (Retail, TRTYPE=1)

Поля операции Retail (Покупка) для которых проверяется MAC:

| Имя поля | Код поля | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| MERCH_GMT | 56 | Знак и Число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММСС) |
| TRTYPE | 22 | Цифровое | 1 | Значение: 1 |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: AMOUNT, CURRENCY, ORDER, MERCHANT, TERMINAL, MERCH_GMT, TIMESTAMP, TRTYPE, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поля | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| ORDER | 27 | 13 | 3558714461568 |
| MERCHANT | 29 | 12 | merchantname |
| TERMINAL | 21 | 8 | 81140825 |
| MERCH_GMT | 56 | 1 | 6 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 1 | 1 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

516.64339813355871446156812merchantname8811408251614202002240739211132F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «4EF4941B7EF1047FB11AF46D666775F9A746324A».

Пример макирования запроса на P2P перевод (TRTYPE=8)

Поля операции удаления токена для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| MERCHANT | 29 | Строка | 15 | Идентификатор торговца (название интернет-магазина) |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| TRTYPE | 22 | Цифровое | 2 | Значение: 8 |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: AMOUNT, CURRENCY, MERCHANT, TERMINAL, MERCH_GMT, TIMESTAMP, TRTYPE, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| MERCHANT | 29 | 12 | merchantname |
| TERMINAL | 21 | 8 | 81140825 |
| MERCH_GMT | 56 | 1 | 6 |
| TIMESTAMP | 47 | 14 | 20200804073921 |
| TRTYPE | 22 | 1 | 8 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

516.64339812merchantname8811408251614202008040739211832F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «BE6D0571E1FEDCC9725E90065A47539223272F79».

Пример макирования запроса предварительной авторизации (TRTYPE=12)

Поля операции предварительной авторизации для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|---|
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| MERCH_GMT | 56 | Цифровое | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| TRTYPE | 22 | Цифровое | 2 | Значение: 12 |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: AMOUNT, CURRENCY, ORDER, TERMINAL, MERCH_GMT, TIMESTAMP, TRTYPE, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| ORDER | 27 | 13 | 3558714461568 |
| TERMINAL | 21 | 8 | 81140825 |
| MERCH_GMT | 56 | 1 | 6 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 2 | 12 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

516.64339813355871446156888114082516142020022407392121232F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «73BBC1C9D8CB5EE5B67CD309E12A9FF6B510FAD4».

Пример макирования запроса завершения вторичной торговой операции со ссылкой на первичную транзакцию (TRTYPE=21)

Поля завершения вторичной торговой операции со ссылкой на первичную транзакцию для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|---------------|---------------------------|---|
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка |
| TRTYPE | 22 | Цифровое | 2 | Значение: 21 |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧММ) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: ORDER, AMOUNT, CURRENCY, RRN, INT_REF, TRTYPE, TERMINAL, TIMESTAMP, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| ORDER | 27 | 13 | 3558714461568 |
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| RRN | 28 | 12 | 821185120045 |
| INT_REF | 51 | 16 | 9C2176F638FDC05C |
| TRTYPE | 22 | 2 | 21 |
| TERMINAL | 21 | 8 | 81140825 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

133558714461568516.64339812821185120045169C2176F638FDC05C221881140825142020022407392132F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «F7D53AC57CA225F1DE4A4765534F0A175A956D41».

Пример макирования запроса отмены покупки (Reversal, TRTYPE=22)

Поля операции Reversal (Отмена покупки) для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|------------|----------|---------------|---------------------------|---|
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| ORG_AMOUNT | 52 | Цифровое | 12 | Сумма исходной транзакции |
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| TIMESTAMP | 47 | ГГГГММДДЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧММ) |
| TRTYPE | 22 | Цифровое | 2 | Значение: 22 |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: ORDER, ORG_AMOUNT, AMOUNT, CURRENCY, RRN, INT_REF, TERMINAL, TIMESTAMP, TRTYPE, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|------------|----------|-------|----------------------------------|
| ORDER | 27 | 13 | 3558714461568 |
| ORG_AMOUNT | 52 | 5 | 16.64 |
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| RRN | 28 | 12 | 821185120045 |
| INT_REF | 51 | 16 | 9C2176F638FDC05C |
| TERMINAL | 21 | 8 | 81140825 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 2 | 22 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

133558714461568516.64516.64339812821185120045169C2176F638FDC05C881140825142020022407392122232F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BВ0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «F89862A6В9020332EE35C0129AAC5E796153BF7C».

Пример макирования запроса на создание токена (TRTYPE=81)

Поля операции создания токена для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|---|
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| RRN | 28 | Цифровое | 12 | Уникальный ссылочный номер транзакции |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка |
| MERCH_GMT | 56 | Знак и Число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| TRTYPE | 22 | Цифровое | 2 | Значение: 81 |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: ORDER, RRN, INT_REF, MERCH_GMT, TIMESTAMP, TRTYPE, TERMINAL, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| ORDER | 27 | 13 | 3558714461568 |
| RRN | 28 | 12 | 821185120045 |
| INT_REF | 51 | 16 | 9C2176F638FDC05C |
| MERCH_GMT | 56 | 1 | 6 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 2 | 81 |
| TERMINAL | 21 | 8 | 81140825 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

13355871446156812821185120045169C2176F638FDC05C16142020022407392128188114082532F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «0C9B90464E72ECD199908444A18C88A83243F059».

Пример макирования запроса на удаление токена (TRTYPE=82)

Поля операции удаления токена для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|----------------|----------|----------------|---------------------------|---|
| MERCH_TOKEN_ID | 227 | Строка | 32 | ID токена который необходимо удалить |
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| MERCH_GMT | 56 | Знак и Число | 1-5 | Сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6ч.) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| TRTYPE | 22 | Цифровое | 2 | Значение: 82 |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: MERCH_TOKEN_ID, ORDER, MERCH_GMT, TIMESTAMP, TRTYPE, TERMINAL, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|----------------|----------|-------|----------------------------------|
| MERCH_TOKEN_ID | 227 | 32 | 0CBV126352804BD46EE0E0019EBCDC94 |
| ORDER | 27 | 13 | 3558714461568 |
| MERCH_GMT | 56 | 1 | 6 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 2 | 82 |
| TERMINAL | 21 | 8 | 81140825 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

320CBV126352804BD46EE0E0019EBCDC9413355871446156816142020022407392128288114082532F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BV0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «BA18582A353ABF41D933C41D8F7FA124DC46B507».

Пример макирования запроса на вторичную операцию периодического платежа (TRTYPE=171)

Поля вторичной операции периодического платежа для которых проверяется MAC:

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|---|
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |
| AMOUNT | 25 | Цифровое | 12 | Сумма входящей транзакции |
| CURRENCY | 26 | Строка | 3 | Код валюты входящей транзакции |
| INT_REF | 51 | Цифровое | 1-12 | Внутренняя ссылка |
| TERMINAL | 21 | Строка | 8 | Идентификатор терминала (присваивается банком) |
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |
| TRTYPE | 22 | Цифровое | 3 | Значение: 171 |
| RECUR_REF | 181 | Цифровое | 12 | Ссылка на авторизацию при периодических платежах. (код оригинальной авторизации RRN) |
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате |

Строка источника MAC будет содержать следующие значения полей: ORDER, AMOUNT, CURRENCY, INT_REF, TERMINAL, TIMESTAMP, TRTYPE, RECUR_REF, NONCE.

Предположим, что транзакция с полями описана ниже:

| Поле | Код поле | Длина | Значение |
|-----------|----------|-------|----------------------------------|
| ORDER | 27 | 13 | 3558714461568 |
| AMOUNT | 25 | 5 | 16.64 |
| CURRENCY | 26 | 3 | 398 |
| INT_REF | 51 | 16 | 9C2176F638FDC05C |
| TERMINAL | 21 | 8 | 81140825 |
| TIMESTAMP | 47 | 14 | 20200224073921 |
| TRTYPE | 22 | 3 | 171 |
| RECUR_REF | 181 | 12 | 925885667408 |
| NONCE | 61 | 32 | F2B2DD7E603A7AAF5E1BC35DEE1F6C9A |

Строка источника для макирования для этого примера будет следующая:

133558714461568516.643398169C2176F638FDC05C881140825142020022407392131711292588566740832F2B2DD7E603A7AAF5E1BC35DEE1F6C9A

Для нашего примера строки источника MAC и алгоритма HMAC_SHA1 с шестнадцатеричным секретным ключом «6BB0AC02E47BDF73D98FEB777F3B5294» поле P_SIGN должно быть равно: «8F9E1FC3A33C435749BE999A258D1257C32E6C7B».

НОТИФИКАЦИИ

Нотификации - это уведомления, отправляемые мерчанту после каждой проведенной операции. Нотификации отправляются по желанию на URL адрес или на Email, который мерчант сообщает в банк. Так же, чтобы мерчант был уверен в том, что на URL обращается именно банк эквайер, необходимо настроить аутентификацию с использованием логина и пароля (Basic Authentication), которые так же должны быть переданы в банк. Нотификация отправляется в виде набора полей, содержащих реквизиты проведенной операции.

При использовании нотификации в рамках рекуррентных платежей дополнительно необходимо обратиться в банк для проведения настроек по формату уведомления.

В случае если нотификация на URL поддерживает SSL, то необходимо предоставить следующие данные:

- ✓ по HTTPS:
 - сертификаты (CA_File, Cert, Key);
 - URL адрес;
 - PORT;
 - POST/GET;
 - логин и пароль (Basic Authentication);
 - поддерживает ли протокол TLS 1.2;
 - расположен ли ваш сайт на виртуальном хосте.

В случае если нотификация на URL и этот URL защищен на уровне Basic Authentication, то необходимо предоставить следующие данные:

- ✓ по HTTP/HTTPS:
 - URL адрес;
 - PORT;
 - POST/GET;
 - логин и пароль (Basic Authentication);
 - поддерживает ли протокол TLS 1.2;
 - расположен ли ваш сайт на виртуальном хосте.

В случае если на E-Mail, то необходимо предоставить следующие данные:

- электронный адрес получателя merchant@domain.com;
- формат заголовка, тела письма для уведомления (желательно с примером).

Пример стандартного набора полей, передаваемых в нотификациях (**При необходимости дополнительных полей обратитесь в банк для проведения настроек по формату уведомления**):

[Function] => TransResponse

[Result] => 0

[RC] => 00

[Amount] => 421.00

[Currency] => KZT

[Order] => 400092

[RRN] => 833085459546

[IntRef] => CA595558B8021787

[AuthCode] => 155151

где,

[RC] – Response Code, результат выполнения транзакции (00-успешно, 05-не успешно, 51-недостаточно средств),

[Amount] – сумма транзакции,

[Currency] – валюта транзакции,

[Order] – ID заказа,

[RRN] – Уникальный ссылочный номер транзакции,

[IntRef] – Внутренняя ссылка,

[AuthCode] – Код авторизации

Поле M_INFO (Дополнительная информация по протоколу EMVCo 3DS v2)

РЕКОМЕНДАЦИЯ!

Поле M_INFO является опциональным (не обязательным), рекомендация к его использованию появляется если торговец может хотеть передать дополнительную информацию ради потенциально более аккуратного риск менеджмента на стороне эмитента.

Система продавца может предоставлять конкретные данные транзакции для расширенной обработки 3DS v2. Отправка этих данных не является обязательной, интерфейс Merchant Payment Interface (MPI) должен проверить версию протокола 3DS и соответствующим образом применить эти данные.

| Название параметра | Тип | Длина допустимых значений | Описание |
|--------------------|--------|---------------------------|--|
| M_INFO | Строка | 35000 | Необязательный набор данных, связанных с 3DS v2, отправленных продавцом. Должен быть строкой в кодировке Base64 «параметр»: «данные значения» в формате JSON. Полный набор доступных данных можно найти на веб-сайте EMVCo, в документе «3-D Secure – Protocol and Core Functions Specification», в описании сообщения AReq. Все параметры в этом наборе необязательны. |

Ниже приведен пример данных, подготовленных для поля M_INFO. Далее эти данные необходимо преобразовать в Base64, чтобы получить на выходе поле M_INFO. Сбор данных можно реализовать путём выполнения js-скрипта (tdsinfo.js) в POST запросе от торговца.

```
{
  "browserJavaEnabled": false,
  "browserCookieEnabled": true,
  "browserUserAgent": "Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101
Firefox/64.0",
  "platform": "Linux x86_64",
  "browserColorDepth": 24,
  "browserLanguage": "ru",
  "browserTZ": "Europe/Moscow",
  "browserTZoffset": -3,
  "browserScreenWidth": 1207,
  "browserScreenHeight": 293,
  "browser": "Firefox",
  "browserVersion": "64.0",
  "os": "Linux",
  "appCodeName": "Mozilla",
  "appName": "Netscape",
  "product": "Gecko",
  "acctType": "03",
  "acctID": "personal account",
  "billAddrCity": "Bill City Name",
  "billAddrCountry": "840",
  "billAddrLine1": "Bill Address Line 1",
  "billAddrLine2": "Bill Address Line 2",
  "billAddrLine3": "Bill Address Line 3",
  "billAddrPostCode": "Bill Post Code",
  "billAddrState": "CO",
  "shipAddrCity": "Ship City Name",
  "shipAddrCountry": "840",
  "shipAddrLine1": "Ship Address Line 1",
  "shipAddrLine2": "Ship Address Line 2",
  "shipAddrLine3": "Ship Address Line 3",
  "shipAddrPostCode": "Ship Post Code",
  "shipAddrState": "CO",
```

```

"transType": "01",
"threeDSRequestorChallengeInd": "sample value",
"threeDSRequestorAuthenticationInd": "sample value"
"merchantRiskIndicator": {
  "shipIndicator": "02",
  "deliveryTimeframe": "01",
  "deliveryEmailAddress": "deliver@email.com",
  "reorderItemsInd": "01",
  "preOrderPurchaseInd": "02",
  "preOrderDate": "20170519",
  "giftCardAmount": "337",
  "giftCardCurr": "840",
  "giftCardCount": "02"
},
"acctInfo": {
  "chAccAgeInd": "03",
  "chAccDate": "20140328",
  "chAccChangeInd": "04",
  "chAccChange": "20160712",
  "chAccPwChangeInd": "02",
  "chAccPwChange": "20170328",
  "shipAddressUsageInd": "04",
  "shipAddressUsage": "20160714",
  "txnActivityDay": "1",
  "txnActivityYear": "21",
  "provisionAttemptsDay": "0",
  "nbPurchaseAccount": "11",
  "suspiciousAccActivity": "01",
  "shipNameIndicator": "02",
  "paymentAccInd": "04",
  "paymentAccAge": "20160917"
}
}

```

На HTML странице мерчанта можно вызывать JS скрипт таким образом:

```

<script src="js/tdsinfo.js"></script>

...

<script language="JavaScript">
function init() {
  document.getElementById("m_info").value = tdsInfo;
}

...

//Внутри формы указывается поле M_INFO
<input TYPE="HIDDEN" NAME="M_INFO" id="m_info"></input>

```

Ниже приведен список параметров, которые можно отправить на обработку 3DS v2. Отправка этих данных не является обязательной, MPI проверяет версию протокола 3DS и соответствующим образом применяет эти данные.

На каждом типе операций (TRTYPE) в строке запроса рекомендуется включить параметр M_INFO. Вместе с инструкцией есть шаблон JavaScript файла **tdsinfo.js**. Внутри настраиваются значения следующих полей:

| (Элемент данных) Имя поля | JSON Тип | Длина / Формат / Значение | Описание |
|------------------------------|-------------|---------------------------|----------|
|------------------------------|-------------|---------------------------|----------|

| | | | |
|--|---------------|---|---|
| | данные | | |
| (Browser Java Enabled) (Браузер Java включен) browserJavaEnabled | Boolean | Допустимые значения: • true • false | Логическое значение, которое представляет возможность браузера держателя карты выполнять Java. Значение возвращается из свойства navigator.javaEnabled. |
| (Browser User-Agent) (Пользователь-агент браузера) browserUserAgent | String | Длина: переменная, максимум 2048 символов. Принятое значение: Примечание: если общая длина User-Agent, отправленного браузером, превышает 2048 символов, сервер 3DS отсекает лишнюю часть. | Точное содержимое HTTP-заголовка пользовательского агента. |
| (Browser Screen Color Depth) (Глубина цвета экрана браузера) browserColorDepth | String | Длина: 1-2 символа. Допустимые значения: • 1 = 1 бит • 4 = 4 бита • 8 = 8 бит • 15 = 15 бит • 16 = 16 бит • 24 = 24 бита • 32 = 32 бита • 48 = 48 бит | Значение, представляющее битовую глубину цветовой палитры для отображения изображений в битах за пиксель. Получено из браузера держателя карты с помощью свойства screen.colorDepth. |
| (Browser Language) (Язык браузера) browserLanguage | String | Длина: переменная, 1–8 символов. | Значение, представляющее язык браузера, как определено в IETF BCP47. Возвращено из свойства navigator.language. |
| (Browser Time Zone) (Часовой пояс браузера) browserTZ | String | Длина: 1–5 символов. Принятое значение: Значение возвращается из метода getTimezoneOffset (). | Разница во времени между временем UTC и местным временем браузера держателя карты, в минутах. |
| (Browser Screen Width) (Ширина экрана браузера) browserScreenWidth | String | Длина: переменная, 1–6 символов. | Общая ширина экрана держателя карты в пикселях. Значение возвращается из свойства screen.width. |
| (Browser Screen Height) (Высота экрана браузера) browserScreenHeight | String | Длина: переменная, 1–6 символов. | Общая высота экрана Держателя карты в пикселях. Значение возвращается из свойства screen.height. |
| (Account Type) (Тип счета) acctType | String | Длина: 2 символа Допустимые значения: • 01 = Не применимо. • 02 = Кредит. • 03 = Дебет. • 04–79 = Зарезервировано для будущего использования EMVCo (значения недействительны до тех пор, пока не будут определены EMVCo). • 80–99 = DS или Специфика платежной системы. | Указывает тип учетной записи. Например, для карточного продукта с несколькими счетами. |
| (Cardholder Account Identifier) (Идентификатор счета держателя карты) acctID | String | Длина: переменная, максимум 64 символа. | Дополнительная информация об учетной записи, которую может предоставить запрашиваемая сторона 3DS. |
| (Cardholder Billing Address City) (Город платежного адреса держателя карты) billAddrCity | String | Длина: переменная, максимум 50 символов. | Город платежного адреса Держателя карты, связанный с картой, использованной для этой покупки. |
| (Cardholder Billing Address Country) (Страна платежного адреса держателя карты) billAddrCountry | String | Длина: 3 символа Принятое значение: Должен быть трехзначным цифровым кодом страны ISO 3166-1, кроме исключений, перечисленных в таблице A.5. | Страна платежного адреса Держателя карты, связанного с картой, использованной для этой покупки. |
| (Cardholder Billing Address Line 1) (Строка 1 адреса выставления счета держателя карты) | String | Длина: переменная, максимум 50 символов. | Первая строка почтового адреса или эквивалентная местная часть платежного адреса Держателя карты, |

| | | | |
|--|--------|--|--|
| billAddrLine1 | | | связанная с картой, использованной для этой покупки. |
| (Cardholder Billing Address Line 2) (Строка 2 адреса выставления счета держателя карты) billAddrLine2 | String | Длина: переменная, максимум 50 символов. | Вторая строка почтового адреса или эквивалентная местная часть платежного адреса Держателя карты, связанная с картой, использованной для этой покупки. |
| (Cardholder Billing Address Line 3) (Строка 3 адреса выставления счета держателя карты) billAddrLine3 | String | Длина: переменная, максимум 50 символов. | Третья строка почтового адреса или эквивалентная местная часть платежного адреса Держателя карты, связанная с картой, использованной для этой покупки. |
| (Cardholder Billing Address Postal Code) (Почтовый индекс платежного адреса держателя карты) billAddrPostCode | String | Длина: переменная, максимум 16 символов. | Почтовый индекс или другой почтовый индекс платежного адреса Держателя карты, связанный с картой, использованной для этой покупки. |
| (Cardholder Billing Address State) (Состояние платежного адреса держателя карты) billAddrState | String | Длина: переменная, максимум 3 символа Принятое значение: Должен быть код подразделения страны, определенный в ISO 3166-2. | Штат или провинция платежного адреса Держателя карты, связанного с картой, использованной для этой покупки. |
| (Cardholder Shipping Address City) (Город доставки адреса держателя карты) shipAddrCity | String | Длина: переменная, максимум 50 символов. | Городская часть адреса доставки, запрошенная Держателем карты. |
| (Cardholder Shipping Address Country) (Страна доставки адреса держателя карты) shipAddrCountry | String | Длина: 3 символа Принятое значение: Трехзначный код страны ISO 3166-1, отличный от перечисленных в таблице A.5. | Страна адреса доставки, запрошенного Держателем карты. |
| (Cardholder Shipping Address Line 1) (Адрес доставки держателя карты, строка 1) shipAddrLine1 | String | Длина: переменная, максимум 50 символов. | Первая строка почтового адреса или эквивалентная местная часть адреса доставки, запрошенная Держателем карты. |
| (Cardholder Shipping Address Line 2) (Адрес доставки держателя карты, строка 2) shipAddrLine2 | String | Длина: переменная, максимум 50 символов. | Вторая строка почтового адреса или эквивалентная местная часть адреса доставки, запрошенная Держателем карты. |
| (Cardholder Shipping Address Line 3) (Адрес доставки держателя карты, строка 3) shipAddrLine3 | String | Длина: переменная, максимум 50 символов. | Третья строка почтового адреса или эквивалентная местная часть адреса доставки, запрошенная Держателем карты. |
| (Cardholder Shipping Address Postal Code) (Почтовый индекс адреса доставки держателя карты) shipAddrPostCode | String | Длина: переменная, максимум 16 символов. | Почтовый индекс или другой почтовый индекс адреса доставки, запрошенный Держателем карты. |
| (Cardholder Shipping Address State) (Государственный адрес доставки держателя карты) shipAddrState | String | Длина: переменная: максимум 3 символа Принятое значение: Это должен быть код подразделения страны, определенный в ISO 3166-2. | Штат или провинция адреса доставки, связанного с картой, используемой для этой покупки. |
| (Transaction Type) (Тип операции) transType | String | Длина: 2 символа Допустимые значения: • 01 = Покупка товаров / услуг • 03 = Проверить акцент • 10 = Пополнение счета • 11 = Квазиденежная операция • 28 = Предоплаченная активация и загрузка Примечание. Значения взяты из стандарта 8583 ISO. | Определяет тип аутентифицируемой транзакции. |
| (3DS Requestor Challenge Indicator) (Индикатор запроса запрашивающего 3DS) threeDSRequestorChallengeInd | String | Длина: 2 символа Допустимые значения: • 01 = Нет предпочтений • 02 = Запрос не запрашивается | Указывает, запрошен ли запрос для этой транзакции. Например: |

| | | | |
|--|--------|---|--|
| | | <ul style="list-style-type: none"> • 03 = Запрос запрошен: предпочтение запрашивающей стороны 3DS • 04 = Запрос запрошен: Мандат • 05–79 = Зарезервировано для будущего использования EMVCo (значения недействительны до тех пор, пока не будут определены EMVCo) • 80-99 = Зарезервировано для использования DS <p>Примечание. Если элемент не указан, ожидается, что ACS будет интерпретировать как 01 = Нет предпочтения.</p> | <p>Для 01-PA у запрашивающей стороны 3DS могут возникнуть опасения по поводу транзакции и запросить вызов.</p> <p>Для 02-NPA может потребоваться проблема при добавлении новой карты в кошелек.</p> <p>Для местных / региональных требований или других переменных.</p> |
| <p>(3DS Requestor Authentication Indicator) (Индикатор аутентификации запрашивающей стороны 3DS)</p> <p>threeDSRequestorAuthenticationInd</p> | String | <p>Длина: 2 символа</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • 01 = Платежная операция • 02 = повторяющаяся транзакция • 03 = Рассрочка платежа • 04 = Добавить карту • 05 = Сохранить карту • 06 = проверка держателя карты как часть идентификатора токена EMV. • 07–79 = Зарезервировано для будущего использования EMVCo (значения недействительны до тех пор, пока не будут определены EMVCo) • 80-99 = Зарезервировано для использования DS | <p>Указывает тип запроса аутентификации. Этот элемент данных предоставляет ACS дополнительную информацию для определения наилучшего подхода к обработке запроса аутентификации.</p> |
| <p>(Merchant Risk Indicator) (Индикатор торгового риска)</p> <p>merchantRiskIndicator</p> | Object | <p>Длина: переменная</p> <p>Примечание. Данные будут отформатированы в объект JSON перед помещением в поле «Индикатор риска продавца устройства» сообщения.</p> | <p>Оценка Продавцом уровня риска мошенничества для конкретной аутентификации как для держателя карты, так и для выполняемой аутентификации.</p> |
| <p>(Shipping Indicator) (Индикатор доставки)</p> <p>shipIndicator</p> | String | <p>Длина: 2 символа</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • 01 = Доставка на платежный адрес держателя карты • 02 = Доставка на другой подтвержденный адрес, указанный в файле продавца • 03 = Доставка на адрес, отличный от платежного адреса держателя карты. • 04 = «Доставка в магазин» / получение в местном магазине (адрес магазина должен быть указан в полях адреса доставки) • 05 = Цифровые товары (включая онлайн-сервисы, электронные подарочные карты и коды погашения) • 06 = билеты на поездки и мероприятия, не отправляются • 07 = Другое (например, игры, не поставляемые цифровые услуги, подписка на мультимедиа и т. д.) | <p>Указывает способ доставки, выбранный для транзакции. Продавцы должны выбрать код индикатора доставки, который наиболее точно описывает конкретную транзакцию держателя карты, а не его общий бизнес. Если один или несколько товаров включены в продажу, используйте код индикатора доставки для физических товаров, или, если все цифровые товары, используйте код индикатора доставки, который описывает самый дорогой товар.</p> |
| <p>(Delivery Timeframe) (Срок поставки)</p> <p>deliveryTimeframe</p> | String | <p>Длина: 2 символа</p> <p>Допустимые значения:</p> <ul style="list-style-type: none"> • 01 = Электронная доставка • 02 = Доставка в тот же день • 03 = Ночная доставка • 04 = Доставка в течение двух или более дней | <p>Указывает сроки доставки товара.</p> |
| <p>(Delivery Email Address) (Адрес электронной почты для доставки)</p> <p>deliveryEmailAddress</p> | String | <p>Длина: максимум 254 символа.</p> | <p>Для электронной доставки - адрес электронной почты, на который был доставлен товар.</p> |

| | | | |
|--|--------|---|--|
| (Reorder Items Indicator) (Индикатор повторного заказа) reorderItemsInd | String | Длина: 2 символа Допустимые значения: • 01 = Заказываемся впервые • 02 = Переупорядочен | Указывает, повторно заказывает ли владелец карты ранее купленные товары. |
| (Pre-Order Purchase Indicator) (Индикатор предзаказа покупки) preOrderPurchaseInd | String | Длина: 2 символа Допустимые значения: • 01 = Товар доступен • 02 = Доступность в будущем | Указывает, размещает ли Держатель карты заказ на товары с будущей доступностью или датой выпуска. |
| (Pre-Order Date) (Дата предзаказа) preOrderDate | String | Длина: 8 символов Формат принят: Формат даты = ГГГММДД | Для предварительно заказанной покупки - ожидаемая дата, когда товар будет доступен. |
| (Gift Card Amount) (Сумма подарочной карты) giftCardAmount | String | Длина: максимум 15 символов | При покупке предоплаченной или подарочной карты общая сумма покупки предоплаченной или подарочной карт(ы) в основных единицах (например, 123.45 доллара США равно 123). |
| (Gift Card Currency) (Валюта подарочной карты) giftCardCurr | String | Длина: 3 символа | Для покупок по предоплаченной или подарочной карте - код валюты карты, определенный в ISO 4217, кроме тех, которые перечислены в таблице A.5. |
| (Gift Card Count) (Количество подарочной карты) giftCardCount | String | Длина: 2 символа | При покупке предоплаченной или подарочной карты общее количество приобретенных отдельных предоплаченных или подарочных карт / кодов. |
| (Cardholder Account Information) (Информация об учетной записи держателя карты) acctInfo | Object | Длина: переменная | Дополнительная информация об учетной записи Держателя карты, предоставленная запрашивающей стороной 3DS. |
| (Cardholder Account Age Indicator) (Индикатор возраста счета держателя карты) chAccAgeInd | String | Длина: 2 символа Допустимые значения: • 01 = Нет учетной записи (выезд гостя) • 02 = Создано во время этой транзакции • 03 = Менее 30 дней • 04 = 30-60 дней • 05 = Более 60 дней | Срок, в течение которого владелец карты имел учетную запись в 3DS Requestor. |
| (Cardholder Account Date) (Дата счета держателя карты) chAccDate | String | Длина: 8 символов Формат принят: Формат даты = ГГГММДД | Дата, когда владелец карты открыл счет в 3DS Requestor. |
| (Cardholder Account Change Indicator) (Индикатор изменения счета держателя карты) chAccChangeInd | String | Длина: 2 символа Допустимые значения: • 01 = Изменено во время этой транзакции • 02 = Менее 30 дней • 03 = 30-60 дней • 04 = Более 60 дней | Время, прошедшее с момента последнего изменения информации об учетной записи держателя карты в запросе 3DS, включая адрес для выставления счета или доставки, новую платежную учетную запись или добавление новых пользователей. |
| (Cardholder Account Change) (Изменение учетной записи держателя карты) chAccChange | String | Длина: 8 символов Формат принят: Формат даты = ГГГММДД | Дата последнего изменения учетной записи держателя карты с запрашивающей стороной 3DS, включая адрес выставления счета или доставки, новую платежную учетную запись или добавление новых пользователей. |
| (Cardholder Account Password Change Indicator) (Индикатор изменения пароля учетной записи держателя карты) chAccPwChangeInd | String | Длина: 2 символа Допустимые значения: • 01 = Без изменений • 02 = Изменено во время этой транзакции • 03 = Менее 30 дней • 04 = 30-60 дней • 05 = Более 60 дней | Указывает время, прошедшее с момента смены пароля или сброса учетной записи держателя карты с запрашиваемой стороной 3DS Requestor. |
| (Cardholder Account Password Change) (Изменение пароля учетной записи держателя карты) chAccPwChange | String | Длина: 8 символов Формат принят: Формат даты = ГГГММДД | Дата изменения пароля или сброса учетной записи держателя карты с запрашивающей стороной 3DS Requestor. |

| | | | |
|--|--------|---|--|
| (Shipping Address Usage Indicator) (Индикатор использования адреса доставки) shipAddressUsageInd | String | Длина: 2 символа Допустимые значения: • 01 = Эта транзакция • 02 = Менее 30 дней • 03 = 30-60 дней • 04 = Более 60 дней | Указывает, когда адрес доставки, используемый для этой транзакции, был впервые использован с запрашивающей стороной 3DS. |
| (Shipping Address Usage) (Использование адреса доставки) shipAddressUsage | String | Длина: 8 символов Формат принят: Формат даты = ГГГГММДД | Дата, когда адрес доставки, использованный для этой транзакции, был впервые использован с запрашивающей стороной 3DS. |
| (Number of Transactions Day) (Количество транзакций в день) txnActivityDay | String | Длина: максимум 3 символа | Количество транзакций (успешных и отмененных) для этого счета держателя карты с запрашивающей стороной 3DS по всем платежным счетам за предыдущие 24 часа. |
| (Number of Transactions Year) (Количество транзакций, год) txnActivityYear | String | Длина: максимум 3 символа | Количество транзакций (успешных и отмененных) для этого счета держателя карты с запрашивающим 3DS по всем платежным счетам за предыдущий год. |
| (Number of Provisioning Attempts Day) (Количество попыток инициализации, день) provisionAttemptsDay | String | Длина: максимум 3 символа | Количество попыток добавления карты за последние 24 часа. |
| (Cardholder Account Purchase Count) (Количество покупок на счете держателя карты) nbPurchaseAccount | String | Длина: максимум 4 символа | Количество покупок с использованием этого счета держателя карты за последние шесть месяцев. |
| (Suspicious Account Activity) (Подозрительная активность аккаунта) suspiciousAccActivity | String | Длина: 2 символа Допустимые значения: • 01 = Подозрительной активности не наблюдалось • 02 = Наблюдалась подозрительная активность | Указывает, испытывал ли запрашивающий 3DS подозрительную активность (включая предыдущее мошенничество) в учетной записи держателя карты. |
| (Shipping Name Indicator) (Индикатор отгрузочного наименования) shipNameIndicator | String | Длина: 2 символа Допустимые значения: • 01 = Имя учетной записи идентично названию доставки • 02 = Имя учетной записи отличается от названия доставки | Указывает, совпадает ли Имя держателя карты в учетной записи с названием доставки, используемым для этой транзакции. |
| (Payment Account Age Indicator) (Индикатор возраста платежного счета) paymentAccInd | String | Длина: 2 символа Допустимые значения: • 01 = Нет учетной записи (выезд гостя) • 02 = Во время этой транзакции • 03 = Менее 30 дней • 04 = 30-60 дней • 05 = Более 60 дней | Указывает продолжительность регистрации платежного аккаунта в аккаунте держателя карты с помощью запрашивающей стороны 3DS. |
| (Payment Account Age) (Возраст платежного счета) paymentAccAge | String | Длина: 8 символов Формат принят: Формат даты = ГГГГММДД | Дата, когда платежный счет был зачислен на счет держателя карты с помощью запрашивающей стороны 3DS. |

Таблица A.5: Excluded Currency Code and Country Code Values

| ISO Code | Value Not Permitted for 3-D Secure | Definition |
|------------|------------------------------------|--|
| ISO 4217 | 955 | European Composite Unit |
| ISO 4217 | 956 | European Monetary Unit |
| ISO 4217 | 957 | European Unit of Account 9 |
| ISO 4217 | 958 | European Unit of Account 17 |
| ISO 4217 | 959 | Gold |
| ISO 4217 | 960 | I.M.F |
| ISO 4217 | 961 | Silver |
| ISO 4217 | 962 | Platinum |
| ISO 4217 | 963 | Reserved for testing |
| ISO 4217 | 964 | Palladium |
| ISO 4217 | 999 | No currency is involved |
| ISO 3166-1 | 901–999 | Reserved by ISO to designate country names not otherwise defined |

3DSecure v1 API

В зависимости от карты (поддерживает 3DSecure или нет) есть два варианта аутентификации.

Первый вариант схемы 3DSecure операции описан в разделе Card with 3DSecure.

Второй вариант схемы аутентификации по заблокированной сумме RND_AMOUNT описан в разделе Card without 3DSecure.

Card with 3DSecure

В текущей схеме, на шаге аутентификации EGW отдает шаблон cardauth, данные из этого шаблона не отображаются напрямую пользователю, а сначала обрабатываются на стороне торговца, т.е. торговец управляет аутентификацией пользователя - перенаправляет его на сторону эмитента, получает PaRes и MD и затем передает их на сторону EGW.

Параметры cardauth:

| Название параметра | Код поле | Тип | Описание |
|--------------------|----------|----------|---|
| MD | 39 | Цифровое | Ссылочный/защитный код сообщения (используется в многоступенчатых транзакциях) |
| TermUrl | 124 | Строка | https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link |
| PaReq | 125 | Цифровое | Тело XML-сообщения. Используется модулем 3D Secure MPI. |
| redirect | 126 | Строка | URL ACS. Используется модулем 3D Secure MPI. |

Пример операций покупки с картой, который поддерживает 3DSecure

1. Со стороны торговца отправляется POST запрос авторизации на URL https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link.

```
{
  "TRTYPE": 1,
  "CARD": "4899887654084306",
  "EXP": "07",
  "EXP_YEAR": "21",
  "CVC2": "423",
  "CVC2_RC": 1,
  "AMOUNT": "52.0",
  "CURRENCY": 398,
  "ORDER": "500000060000300353963527",
  "DESC": "500000060000300353963527",
  "MERCHANT": "TEST",
  "MERCH_GMT": "+6",
  "BACKREF": "https://testdomain.kz",
  "LANG": "ru",
  "TERMINAL": "81140825",
  "TIMESTAMP": "20201103104240",
  "NONCE": "99ff708e185024dd6c8d",
  "P_SIGN": "368062114e2f3452948d9f5add2e2f4128fb07d"
}
```

2. Торговец получает ответ шаблон cardauth.

```
{
  "redirect": "https://3DSecure.qiwi.com/acs/pareq/4d234a6306cc46cb88f430124374a213",
  "PaReq": "eJxVUttSwjAQ/RWm75JN05adgDl81b...yd7MHhqSKZpDmDTusmB1+hbb+/ZYv4w3EaA==",
  "TermUrl": "https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link",
  "MD": "7262990-28C0BF61C0E9209C"
}
```

3. Торговец перенаправляет клиента на 3DSecure верификацию "redirect":"https://3DSecure.qiwi.com/acs/pareq/4d234a6306cc46cb88f430124374a213" с параметрами PaReq и MD.
4. После завершения 3DSecure клиент возвращается на URL торговца с параметрами MD и PaRes.

```
{
  "MD": "7262990-28C0BF61C0E9209C",
  "PaRes": "eJzNWVnvo0iSfx9pvkOp5tH7...FwQoVAX75WeeP/f7+Dfv+Tu73t3Wv+A/fg+Cy+XVvU="
}
```

5. Данные параметры торговец передает POST методом на URL https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link.
6. Торговец получает ответ про успешную авторизацию средств.

```
{
  "AMOUNT": "52.0",
  "ORG_AMOUNT": "",
  "CURRENCY": "398",
  "ORDER": "500000060000300353963527",
  "DESC": "500000060000300353963527",
  "MERCH_NAME": "",
  "MERCHANT": "TEST",
  "TERMINAL": "81140825",
  "EMAIL": "",
  "TRTYPE": "1",
  "TIMESTAMP": "20201103104312",
  "NONCE": "99ff708e185024dd6c8d",
  "BACKREF": "https://testdomain.kz",
  "RESULT": "0",
  "RC": "00",
  "RCTEXT": "Завершено успешно",
  "EXT_DIAG_CODE": "NONE",
  "AUTHCODE": "KOD3BY",
  "RRN": "030885774289",
  "INT_REF": "06ABFC6FB8D39400",
  "CARD": "4899XXXXXXXXX4306",
  "TOKEN_ID": "",
  "P_SIGN": "FDA9E1591F6E92FE12BADB1AD2478C1D38BFFE27"
}
```

Card without 3DSecure

Второй вариант аутентификации (или дополнительный, в случае с картой, который не поддерживает 3DSecure) - аутентификация по заблокированной сумме. В этом случае EGW отдает набор полей (otrauth). В ответ ожидается получить введенную клиентом случайную сумму из авторизации на отображенной в браузере форме от торговца, так как взаимодействие с клиентом контролирует торговец. Проверка суммы будет выполнена на стороне EGW.

Пример операций покупки с картой, который не поддерживает 3Dsecure (RND_AMOUNT)

1. Со стороны торговца отправляется POST запрос авторизации на URL https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link.

```
{
  "TRTYPE": 1,
  "CARD": "5104450033134199",
  "EXP": "04",
  "EXP_YEAR": "21",
  "CVC2": "270",
  "CVC2_RC": 1,
  "AMOUNT": "55.0",
  "CURRENCY": 398,
  "ORDER": "500000060000300353952336",
  "DESC": "500000060000300353952336",
  "MERCHANT": "TEST",
  "MERCH_GMT": "+6",
  "BACKREF": "https://testdomain.kz",
  "LANG": "ru",
  "TERMINAL": "81140825",
  "TIMESTAMP": "20201103082425",
  "NONCE": "eff550ad314f83377e12",
  "P_SIGN": "d6dd6c12f9e6118d105dd8293daffea022a3b945"
}
```

2. Торговец получает ответ шаблон cardauth.

```
{
  "redirect": "https://cap.attempts.securecode.com/acspage/cap?RID=8&VAA=A",
  "PaReq": "eJxVUm1vgjAQ/iuGr2a2wGBiji74ss2YKRO2bH...1FQCiaMh1xeTyK6T177d8A3krxjw=",
  "TermUrl": "https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link",
  "MD": "7255762-03CB848A8CCEEF8B"
}
```

3. Торговец перенаправляет клиента на 3DSecure верификацию "redirect": "https://cap.attempts.securecode.com/acspage/cap?RID=8&VAA=A" с параметрами PaReq и MD.
4. После завершения 3DSecure клиент возвращается на URL торговца с параметрами MD и PaRes.

```
{
  "MD": "7255762-03CB848A8CCEEF8B",
  "PaRes": "eJzVWMmyq8aynZ+vcPgOFtatkOTQ2RFFjx...zme+nNu/H0e8H5q8T1B8P0v8Nau+3iQ=="
}
```


5. Данные параметры торговец передает POST методом на URL [https://3dsecure.bcc.kz:5443/cgi-bin/cgi link](https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link).
6. Торговец получает от EGW набор полей (otrauth) данные для дальнейшего запроса.

```
{
  "TERMINAL": "81140825",
  "TRTYPE": "1",
  "ORDER": "500000060000300353952336",
  "COUNTRY": "",
  "MERCH_GMT": "+6",
  "TIMESTAMP": "20201103082425",
  "LANG": "ru",
  "PANM": "5104XXXXXXXX4199",
  "TRAMOUNT": "55.00",
  "TRCUR": "KZT",
  "DESC": "500000060000300353952336",
  "MERCH_NAME": "",
  "MERCH_URL": ""
}
```

7. Полученные данные необходимо отправить на URL https://3dsecure.bcc.kz:5443/cgi-bin/cgi_link включая параметр RND_AMOUNT. Значение параметра RND_AMOUNT задает клиент. Это значение клиент получает в виде SMS или сможет видеть у себя в аккаунте. **Внимание, значение проверочной суммы должен указываться с точкой. Например, если держатель карты ввел проверочную сумму с символом запятой "1,6", то у вас должен быть функционал, который изменяет на символ точки "1.6".** Пример замены символа запятой на точку показан ниже на языке JavaScript:

```
<script type="text/javascript">
  function CheckAll()
  {
    var checkBool = true;
    var value = document.getElementById('check_blocked_input').value;
    value = value.replace(/,/g, '.');
    document.getElementById('check_blocked_input').value = value;
    return checkBool;
  }
</script>
```

```
{
  "TERMINAL": "81140825",
  "TRTYPE": "1",
  "ORDER": "500000060000300353952336",
  "COUNTRY": "",
  "MERCH_GMT": "+6",
  "TIMESTAMP": "20201103082425",
  "LANG": "ru",
  "PANM": "5104XXXXXXXX4199",
  "TRAMOUNT": "55.00",
  "TRCUR": "KZT",
  "DESC": "500000060000300353952336",
  "MERCH_NAME": "",
  "MERCH_URL": ""
}
```

```
"RND_AMOUNT": "1.6"  
}
```

8. Торговец получает ответ про успешную авторизацию средств.

```
{  
  "AMOUNT": "55.0",  
  "ORG_AMOUNT": "",  
  "CURRENCY": "398",  
  "ORDER": "500000060000300353952336",  
  "DESC": "500000060000300353952336",  
  "MERCH_NAME": "",  
  "MERCHANT": "TEST",  
  "TERMINAL": "81140825",  
  "EMAIL": "",  
  "TRTYPE": "1",  
  "TIMESTAMP": "20201103082425",  
  "NONCE": "eff550ad314f83377e12",  
  "BACKREF": "https://testdomain.kz",  
  "RESULT": "0",  
  "RC": "00",  
  "RCTEXT": "Завершено успешно",  
  "EXT_DIAG_CODE": "NONE",  
  "AUTHCODE": "DCA5BY",  
  "RRN": "030885771568",  
  "INT_REF": "06AB056FB8D39486",  
  "CARD": "5104XXXXXXXX4199",  
  "TOKEN_ID": "",  
  "P_SIGN": "D6DD6C12F9E6118D105DD8293DAFFEA022A3B945"  
}
```

ТЕСТИРОВАНИЕ В СРЕДЕ SOAP UI

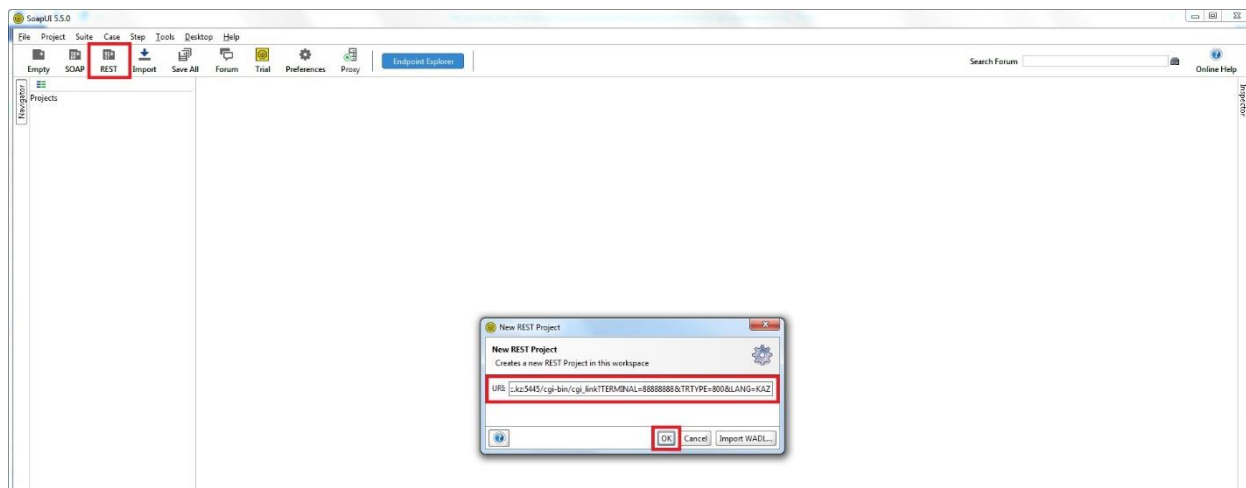
Внимание!

При тестировании с макированием использовать SOAP UI, ставить строку запроса из примера в браузер и отправлять запрос не рекомендуется, так как не соблюдается правила макирования!

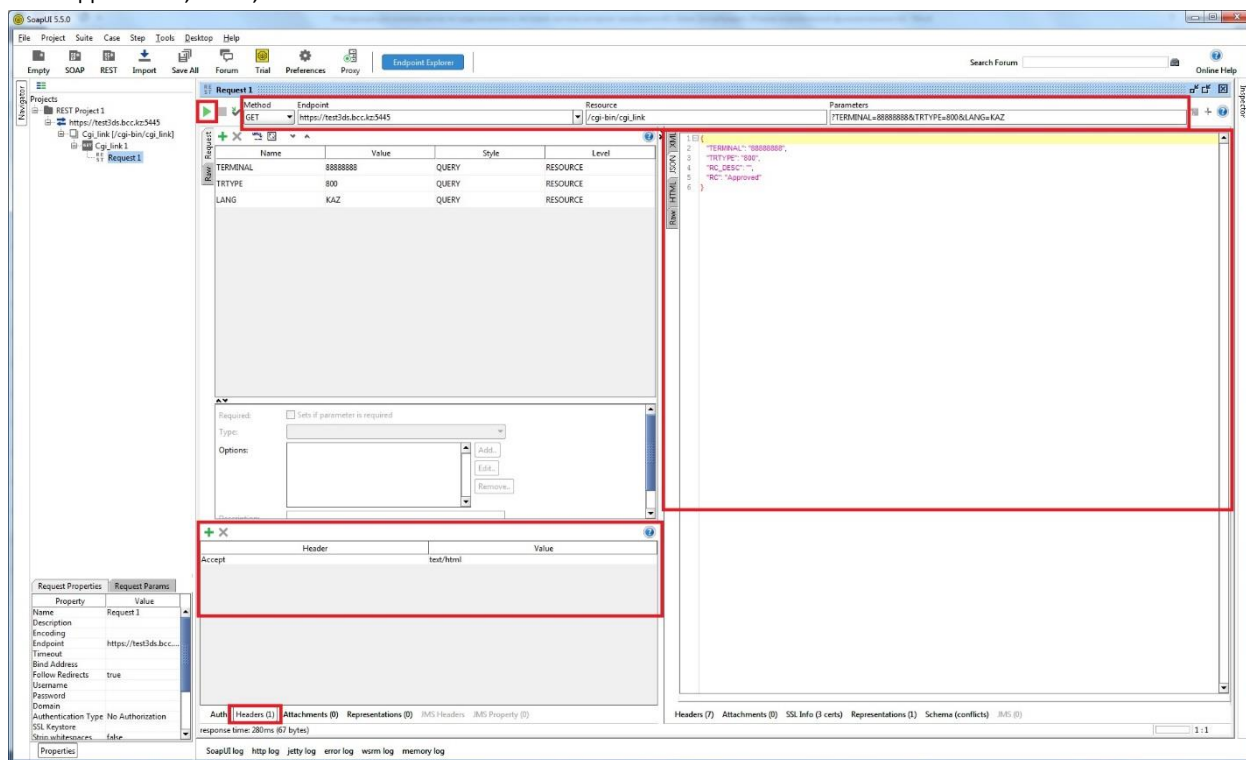
Вначале выбираем REST. В появившемся окне вводим строку запроса, который мы хотим протестировать.

Например, https://test3ds.bcc.kz:5445/cgi-bin/cgi_link?TERMINAL=81140826&TRTYPE=800&LANG=kz

Нажимаем ОК.



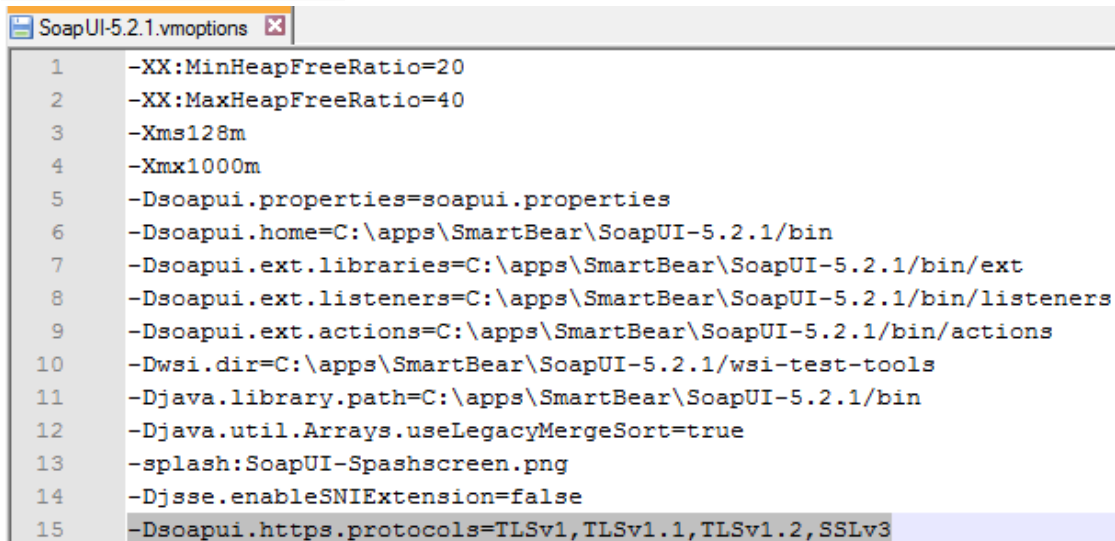
Система само распределит строку запроса в нужные поля. Выбираем Method (GET | POST). При выборе метода POST, **Media Type** выбираем **application/x-www-form-urlencoded** и отметить checkbox **Post QueryString**. В окне **Header** добавляем строку *Accept: text/html* как показано на рисунке внизу. После нажимаем Submit Request to specified endpoint URL. В окне слева видны параметры, которые передаются. В окне справа получаем ответ в вкладках XML, JSON, HTML и Raw.



Настройка инструмента SOAP UI для проведения тестовых операций

В файле конфигурации "C:\APPS\SmartBear\SoapUI-5.2.1\bin\SoapUI-5.2.1.vmoptions"

Добавить следующую строку: -Dsoapui.https.protocols=TLSv1,TLSv1.1,TLSv1.2,SSLv3



```
1 -XX:MinHeapFreeRatio=20
2 -XX:MaxHeapFreeRatio=40
3 -Xms128m
4 -Xmx1000m
5 -Dsoapui.properties=soapui.properties
6 -Dsoapui.home=C:\apps\SmartBear\SoapUI-5.2.1\bin
7 -Dsoapui.ext.libraries=C:\apps\SmartBear\SoapUI-5.2.1\bin\ext
8 -Dsoapui.ext.listeners=C:\apps\SmartBear\SoapUI-5.2.1\bin\listeners
9 -Dsoapui.ext.actions=C:\apps\SmartBear\SoapUI-5.2.1\bin\actions
10 -Dwsi.dir=C:\apps\SmartBear\SoapUI-5.2.1\wsi-test-tools
11 -Djava.library.path=C:\apps\SmartBear\SoapUI-5.2.1\bin
12 -Djava.util.Arrays.useLegacyMergeSort=true
13 -splash:SoapUI-Splashscreen.png
14 -Djsse.enableSNIExtension=false
15 -Dsoapui.https.protocols=TLSv1,TLSv1.1,TLSv1.2,SSLv3
```

ИНФОРМАЦИЯ ПО КОДАМ ОТВЕТА

| Код ответа | Описание |
|------------|---|
| -1 | В запросе не заполнено обязательное поле |
| -2 | Запрос не прошел CGI- проверку |
| -3 | Хост эквайера (NS) не отвечает либо неверный формат файла шаблона ответа модуля e-Gateway |
| -4 | Нет соединения с хостом эквайера (NS) |
| -5 | Ошибка соединения с хостом эквайера (NS) во время обработки транзакции |
| -6 | Ошибка настройки модуля e-Gateway |
| -7 | Некорректный ответа хоста эквайера (NS), например, отсутствуют обязательные поля |
| -8 | Ошибка в поле "Card number" запроса |
| -9 | Ошибка в поле "Card expiration date" запроса |
| -10 | Ошибка в поле "Amount" запроса |
| -11 | Ошибка в поле "Currency" запроса |
| -12 | Ошибка в поле "Merchant ID" запроса |
| -13 | IP-адрес источника транзакции (обычно IP торговца) не соответствует ожидаемому |
| -14 | Нет соединения с PIN-клавиатурой Интернет-терминала либо программа-агент на компьютере/рабочей станции Интернет-терминала не запущена |
| -15 | Ошибка в поле "RRN" запроса |
| -16 | На терминале выполняется другая транзакция |
| -17 | Терминалу отказано в доступе к модулю e-Gateway |
| -18 | Ошибка в поле "CVC2" или "CVC2 Description" запроса |
| -19 | Ошибка в запросе на аутентификационную информацию либо аутентификация |
| -20 | Превышен допустимый временной интервал (по умолчанию – 1 час) между значением поля "Time Stamp" запроса и временем модуля e-Gateway |
| -21 | Транзакция уже выполнена |
| -22 | Транзакция содержит ошибочную аутентификационную информацию |
| -23 | Ошибка в контексте транзакции |
| -24 | Транзакция прервана пользователем |
| -25 | Транзакция прервана пользователем |
| -26 | Неверный BIN карты |
| -27 | Ошибка в имени продавца |
| -28 | Ошибка в дополнительных данных |
| -29 | Ошибка в ссылке аутентификации (повреждена или дублируется) |
| -30 | Транзакция отклонена как мошенническая |
| -31 | Транзакция в процессе выполнения |
| -32 | Повторная отклоненная транзакция |
| -33 | Транзакция в процессе аутентификации клиента с помощью авторизации случайной суммы или одноразового случайного кода |
| -34 | MasterCard Installment транзакция в процессе выбора пользователем способа оплаты |
| -35 | MasterCard Installment транзакция в процессе выбора пользователем способа оплаты была отклонена автоматически после превышения лимита времени на эту операцию |
| -36 | MasterCard Installment транзакция в процессе выбора пользователем способа оплаты была отклонена самим пользователем |
| -37 | Ошибка в поле "Дата окончания периодических платежей" запроса |

FAQ

Если в бою MAC-подпись обязательна, зачем проводить тесты на 81140825?

Это сделано для того чтобы мерчант мог изначально проверить запрос без макирования. Бывает ситуации, когда мерчант отправляет запрос с терминалом поддерживающее макирование и при возникновении ошибки не знает причину ошибки. Связано ли это с макированием или в сам запрос неправильно сформирован или значение параметров неправильно указаны и т.д. Также если используют терминал с макированием 81140825, то в строке запроса при каждом запросе такие параметры как ORDER, TIMESTAMP, NONCE и соответственно P_SIGN должны быть актуализированы. У каждого типа операции могут быть еще параметры, которые должны быть актуализированы при каждом запросе. Поэтому для начала тестируют без макирования и только после успешной операции с макированием. Это дает понять, что последующие ошибки связаны скорее всего с макированием. Если мерчант уверен, что может тестировать сразу с макированием то без проблем может сразу использовать терминал с макированием 81140825.

Возможные ошибки при проведении оплаты

Код ответа банка: 05 – Transaction declined

Код ответа банка: 05 – Не оплачивать

Ошибка может быть со стороны эмитента. Держателю карты рекомендуется обратиться банку выпустившую карту клиента. Либо неправильно ввели карточные данные. Карта клиента может не поддерживать 3DSecure.

Код ответа банка: 13 – Invalid account

Ошибка связанное с суммой. Может быть сумма была минимальной. Попробуйте указать другую побольше сумму.

Код ответа банка: 42 – No universal account

Мерчант при тестировании операции использует не тестовые карты из инструкции, а другую. Рекомендуется при тестировании использовать тестовые карты.

Код ответа банка: 51 – Недостаточно средств

У держателя карты на карте недостаточно средств.

Код ответа банка: 54 – Expired card

Клиент либо ввел неверную дату истечения срока карты, либо карта просрочена.

Код ответа банка: 57 – Транзакция запрещена

Может быть ошибка со стороны банка, что неправильно указан MCC мерчанта или операции проходят неправильно (Unique вместо Retail).

Ошибка может быть со стороны эмитента. Держателю карты рекомендуется обратиться банку выпустившую карту клиента.

Код ответа банка: 61 – Превышен лимит на сумму

Сработал ограничитель по карте. Нужно обратиться в банку эмитенту.

Код ответа банка: 65 – Exceeds frequency limit

Код ответа банка: 65 – Превышен лимит операций

Если клиент совершает более двух транзакции на одном и том же устройстве, может сработать лимит операции SameIP на стороне банка. Рекомендуется попробовать провести транзакцию с другого устройства. Может также сработать лимит операции SameEMail.

Ошибка может быть связано с ограничением лимита по карте клиента. Держатель карты сам должен разрешить проведение операции.

Код ответа банка: 91 – Issuer unavailable

Ошибка может быть связано с картой эмитента. Рекомендуется в тесте попробовать использовать другие тестовые карты.

Error message: Authentication failed

Error message: Ошибка аутентификации

Возможно клиент при попытке оплаты ввел некорректные данные карты. В противном случае необходимо обратиться в банк.

Error message: Duplicate transaction

Произвести повторную оплату с теми же реквизитами карты и с тем же параметром ORDER, в случае ошибки при первой попытке возможна только после 3 часов.

Error message: Ошибка в номере карты

Неправильно введен номер карты.

Error message: Ошибка в формате запроса

Ошибка может быть связана с значениями полей в строке запроса, что неправильно либо тип, либо длина допустимых значения, либо формат значения, либо не соблюдены правила, описанные в описаниях полей. Рекомендуется внимательно смотреть значения полей в строке запроса и правило этих полей в текущей инструкции.

Может быть не заполнены значения полей или пропущены значения полей в строке запроса.

Клиент мог пропустить поле, где вводится карточные данные. (Данная проблема решена со стороны банка. Те поля, где вводятся карточные данные теперь сделаны обязательными для заполнения. В противном случае запрос не будет уходить.)

Error message: Отказано в доступе

Ошибка может быть связана с макированием операции. Это может значить, что неправильно собирается значение поля P_SIGN. Подробное описание как собирается данное поле указан выше в пункте МАКИРОВАНИЕ ОПЕРАЦИИ. Есть вероятность, что строка источника для макирования собран некорректно.

Error message: Транзакция просрочена

Ошибка может быть связана с превышением лимита временной отметкой транзакции в поле TIMESTAMP. Временная отметка транзакции (по времени GMT), присвоенная торговцем: ГГГММДДЧММСС. Разница между временной отметкой Интернет-магазина и модуля e-Gateway не должна превышать 1 час, иначе модуль e-Gateway отклонит транзакцию. Например, если время транзакции было 20200529160735, то в строке запроса учитывая сдвиг часового пояса торговца относительно UTC/GMT (по Алматы + 6 ч.) передается TIMESTAMP=20200529100735. Всегда в каждом запросе в поле TIMESTAMP надо использовать сдвиг часового пояса Алматы + 6 ч.

Возможные ошибки при заполнении полей

ORDER=456321598733 (указан пример)

Если у вас выходит ошибка в поле ORDER, там есть основная вероятность. Вы неправильно учли размер символов. По документации **размер с 6 до 32** и тип должен быть **числовое**.

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|----------|----------|----------|---------------------------|--|
| ORDER | 27 | Цифровое | 6-32 | Идентификатор заказа Интернет-торговца входящей транзакции |

TIMESTAMP=201903141125 (указан пример)

Если у вас выходит ошибка в поле TIMESTAMP, там есть основная вероятность. Вы неправильно учли размер символов. По документации **размер 14** и тип должен быть ГГГГММДДЧЧММСС по времени GMT.

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|-----------|----------|----------------|---------------------------|--|
| TIMESTAMP | 47 | ГГГГММДДЧЧММСС | 14 | Временная отметка транзакции по времени GMT (формат: ГГГГММДДЧЧММ) |

NONCE=1344d7e1752b99 (указан пример)

В поле NONCE указываются шестнадцатеричные символы, поэтому его длина должна быть более 16 символов.

| Имя поля | Код поле | Тип | Длина допустимых значений | Описание |
|----------|----------|--------|---------------------------|--|
| NONCE | 61 | Строка | 8-32 | Случайный идентификатор транзакции. Случайная комбинация длиной в 8-32 байт в шестнадцатеричном формате. |

RECUR_EXP=20260617 (указан пример)

RECUR_EXP не должна быть позже истечения срока действия карты.

| Имя поля | Код поле | Длина допустимых значений | Описание |
|-----------|----------|---------------------------|--|
| RECUR_EXP | 180 | 8 | Дата окончания периодических платежей. После этой даты ни одна авторизация не будет обслужена. |