**Приложение №11**

**Описание протокола информационного взаимодействия по on-line запросам ЕПС к серверу Клиента №1**

# Контактные данные

|  |  |  |
| --- | --- | --- |
| **Специалист** | **E-mail** | **Телефон** |
| **Банк** | | |
| Кочнев Дмитрий Александрович | [DAKochnev.SBT@sberbank.ru](mailto:DAKochnev.SBT@sberbank.ru) |  |
| Клюквин Александр Михайлович | [AMKlyukvin.SBT@sberbank.ru](mailto:AMKlyukvin.SBT@sberbank.ru) |  |
| **Клиент** | | |
|  |  |  |

# Требования к интерфейсу Клиента

1. Интерфейс должен принимать запросы по протоколу HTTPS/HTTP с фиксированных IP-адресов Банка и Клиента.
2. Диапазоны адресов ЕПС: 194.186.207.0/24 и 194.54.14.0/24
3. Адрес (URL) промышленного web-сервера клиента: <https://service.someprovider.ru/pay.pl>

IP-адрес промышленного сервера клиента: XX.XXX.XXX.XX

1. Для авторизации Банка в биллинговой системе Клиента при регистрации платежа используются логин и пароль. Также предусмотрена возможность авторизации Банка в биллинговой системе Клиента без логина и пароля. В этом случае используется двустороннее SSL-соединение. Порядок обмена ключевой информацией для организации двустороннего SSL приведен ниже.
2. Интерфейс должен обрабатывать параметры, передаваемые Банком методом GET/ POST.
3. Интерфейс должен формировать ответ Банку в формате XML в кодировке UTF-8/windows-1251 (если ответ содержит символы национальных алфавитов).
4. Обмен информацией ведется в режиме запрос-ответ, при этом скорость ответа не должна превышать 7 секунд, в ином случае Банк разрывает соединение по таймауту.
5. Если планируемое количество платежей за услуги Клиента ожидается интенсивным (10 платежей в минуту и более), необходимо, чтобы интерфейс Клиента выдерживал многопотоковую коммуникацию до 10-15 одновременных соединений.
6. В случае, если любой из запросов Клиенту завершается ошибкой, то Клиент возвращает код ошибки в соответствии с таблицей, приведенной ниже. Все ошибки имеют признак фатальности. Для системы Банка фатальная ошибка означает, что повторная отправка запроса с теми же параметрами приведет к 100% повторению той же ошибки – следовательно, система Банка прекращает обработку клиентского запроса и завершает его с ошибкой. Нефатальная ошибка означает для системы Банка, что повторение запроса с теми же параметрами через некоторый промежуток времени, возможно, приведет к успеху. Система Банка будет повторять запросы, завершающиеся нефатальной ошибкой, постоянно увеличивая интервал, пока операция не завершится успехом или фатальной ошибкой, либо пока не истечет срок жизни запроса.

# Параметры запросов платёжной системы

| **Параметр** | **Значение** | **Назначение** | **Примечание** | **check** | **payment** |
| --- | --- | --- | --- | --- | --- |
| **ACTION** | Предопределенная строка. Возможные значения: **check, payment,** | Определяет тип запроса | **check** – поиск Плательщика (проверка номера); **payment** – создание платёжной транзакции; | + | + |
| **ACCOUNT** | Строка до 15 символов | Лицевой счет Плательщика |  | + | + |
| **AMOUNT** | Число | Сумма платежа | Разделитель “.” (точка). |  | + |
| **PAY\_ID** | Число | Идентификатор платежной транзакции | Положительное длинное целое число. Генерируется платёжной системой и используется для идентификации платёжных транзакций. |  | + |
| **PAY\_DATE** | Дата и время | Дата и время операции в ЕПС | Дата и время операции в ЕПС по часовому ЕПС в формате “**DD.MM.YYYY\_HH24:MI:SS**”. Здесь между датой и временем стоит символ “\_” (подчеркивание). |  | + |

# Формат ответа сервера Клиента

## Ответы сервера Клиента возвращаются в виде XML-сообщений. Атрибут “encoding” должен иметь значение UTF-8/windows-1251 и соответствовать кодировке, используемой в XML-сообщении.

## Атрибуты, используемые в ответах сервера Клиента на запросы ЕПС

| **Атрибут** | **Значение** | **Назначение** | **Примечание** | **check** | **payment** |
| --- | --- | --- | --- | --- | --- |
| **CODE** | Целое число | Код статуса операции |  | + | + |
| **FIO** | Текст | Фамилия Плательщика |  | + |  |
| **ADDRESS** | Текст | Адрес Плательщика |  | + |  |
| **MESSAGE** | Текст до 512 символов | Текстовое сообщение о статусе операции | Для ошибок, может содержать текстовое описание. | + | + |
| **ACCOUNT\_BALANCE** | Число со знаком | Остаток на счёте Плательщика | Сумма остатка на счёте Плательщика в рублях с копейками. Разделитель целой и дробной части «.» (точка). Отрицательная сумма обозначает задолженность Плательщика. | + |  |
| **REG\_DATE** | Дата и время | Дата и время операции в биллинговой системе | Дата и время регистрации операции в Организации по часовому поясу Организации в формате “**DD/MM/YYYY HH:MI:SI +HH:MM** ”. Здесь между датой и временем вставлен символ «\_» (подчёркивание). |  | + |
| **SYS\_DATE** | Дата и время | Дата и время операции в ЕПС | Дата и время Банка, полученные в первом успешном запросе на оплату по уникальному идентификатору платежной транзакции в исходном формате. |  |  |

**Значения кодов возврата (CODE)**

| **Код ответа** | **Назначение** | **Примечание** | **check** | **payment** |
| --- | --- | --- | --- | --- |
| **-1** | Внутренняя ошибка Организации |  | + | + |
| **0** | Успешное завершение операции | Операция прошла успешно. Для операции проверки состояния транзакции означает, что транзакция подтверждена и платежи в системе Клиента созданы. | + | + |
| **2** | Неизвестный тип запроса | Неизвестное значение поля “**ACTION**”. | + | + |
| **3** | Плательщик не найден |  | + | + |
| **4** | Неверная сумма платежа | Недопустимое значение для поля платежа (“**AMOUNT**”). |  | + |
| **5** | Неверное значение идентификатора транзакции | Недопустимое значение поля идентификатора платёжной транзакции в платёжной системе (”**PAY\_ID**”). |  | + |
| **6** | Неверное значение даты | Недопустимое значение поля даты платежа (“**PAY\_DATE**”). |  | + |
| **8** | Дублирование транзакции | Транзакция с указанным идентификатором уже была введена в систему. |  | + |
| **12** | Транзакция не подтверждена |  |  |  |

# Шаблоны ответов сервера Клиента

## Ответ сервера Клиента на запрос проверки номера (check) должен подчиняться следующему шаблону DTD

**<?xml version=”1.0” encoding=”windows-1251”?>**

**<!DOCTYPE response [**

**<!ELEMENT response (CODE, MESSAGE, FIO,ADDRESS, ACCOUNT\_BALANCE)>**

**]>**

## Ответ сервера Клиента на запрос создания транзакции платежа (payment) должен подчиняться следующему шаблону DTD

**<?xml version=”1.0” encoding=”windows-1251”?>**

**<!DOCTYPE response [**

**<!ELEMENT response (CODE, MESSAGE, REG\_DATE)>**

**]>**

## Ответ сервера Клиента на запрос подтверждения транзакции (commit) должен подчиняться следующему шаблону DTD

**<?xml version=”1.0” encoding=”windows-1251”?>**

**<!DOCTYPE response [**

**<!ELEMENT response (CODE, MESSAGE, REG\_DATE, PAY\_ID\_EXT\*)>**

**] >**

# Примеры обменов сообщениями «запрос-ответ»

# Поиск Плательщика по номеру телефона

|  |  |
| --- | --- |
| Запрос | https://<host>/<path>?ACTION=check&**ACCOUNT**=8462333333 |
| Ответ | <?xml version=”1.0” encoding=”windows-1251”?>  <response>  <CODE>0</CODE>  <MESSAGE>ОК</MESSAGE>  <FIO>Иванов Иван Иванович</FIO>  <ADDRESS>Москва</ADDRESS>  <ACCOUNT\_BALANCE>-34.27</ACCOUNT\_BALANCE>  </response> |
| Запрос | https://<host>/<path>?ACTION=check&**ACCOUNT**=24 |
| Ответ | <?xml version=”1.0” encoding=”windows-1251”?>  <response>  <CODE>3</CODE>  <MESSAGE>Плательщика не найден</MESSAGE>  </response> |

## Создание транзакции платежа

|  |  |
| --- | --- |
| Запрос | https://<host>/<path>?ACTION=payment&**ACCOUNT**=8462333333&AMOUNT=340.24&PAY\_ID=11223344&PAY\_DATE=12.12.2005\_12:45:18 |
| Ответ | <?xml version=”1.0” encoding=”windows-1251”?>  <response>  <CODE>0</CODE>  <MESSAGE></MESSAGE>  <REG\_DATE>10/10/2016 14:34:54.438 +03:00</REG\_DATE>  <SYS\_DATE>12.12.2005\_12:46:03 </SYS\_DATE>  </response> |
| Запрос | https://<host>/<path>?ACTION=payment&**ACCOUNT**=8462333333&TYPE=15&AMOUNT=340.24&PAY\_ID=11223344&PAY\_DATE=12.12..2005\_12:45:18 |
| Ответ | <?xml version=”1.0” encoding=”windows-1251”?>  <response>  <CODE>6</CODE>  <MESSAGE>Не верное значение даты платежа</MESSAGE>  </response> |

**Порядок использования SSL-сертификатов**

1. Клиент предоставляет Банку корневой сертификат Центра сертификации Клиента (для обеспечения доверия сертификатам, выданным Центром сертификации Клиента) в виде, пригодном для установления его принадлежности Клиенту, то есть в виде base-64 кодированного файла формата «.pem» и на бумажном носителе, заверенном собственноручной подписью руководителя и оттиском печати Клиента.
2. При истечении срока действия корневого сертификата, Центра сертификации Клиента, Клиент не позднее, чем за 5 (пять) рабочих дней до окончания срока действия активного корневого сертификата предоставляет Банку новый корневой сертификат в соответствии с п.1.
3. При компрометации или подозрении на компрометацию закрытого ключа сертификата Центра сертификации Клиента (то есть при ознакомлении или подозрении на ознакомление неуполномоченного лица с закрытым ключом сертификата, а также при несанкционированном использовании или подозрении на несанкционированное использование закрытого ключа сертификата) Банк извещается в простой письменной форме о прекращении действия указанного сертификата. С момента уведомления Клиент прекращает электронный документооборот с Банком с использованием указанного сертификата;
4. Банк после получения сообщения о компрометации сертификата выводит соответствующий сертификат из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации;
5. Клиент имеет право в любое время производить замену собственных сертификатов.
6. Банк предоставляет Клиенту запрос на сертификат Банка в виде, пригодном для установления его принадлежности Банку, то есть в виде base-64 кодированного файла формата PKCS#10 и на бумажном носителе, заверенном собственноручной подписью уполномоченного представителя и оттиском печати Банка.
7. Центр сертификации Клиента выпускает сертификат Банка, Клиент передает сертификат Банку.
8. Клиент регистрирует сертификат Банка для аутентификации Банка при открытии SSL-сессии в моде с взаимной аутентификацией (2-х сторонний SSL).
9. При истечении срока действия сертификата Банка Банк не позднее, чем за 5 (пять) рабочих дней до окончания срока действия активного сертификата предоставляет Клиенту запрос на новый сертификат в соответствии с п.6.
10. При компрометации или подозрении на компрометацию закрытого ключа сертификата Банка (то есть при ознакомлении или подозрении на ознакомление неуполномоченного лица с закрытым ключом сертификата, а также при несанкционированном использовании или подозрении на несанкционированное использование закрытого ключа сертификата) Клиент извещается в простой письменной форме о прекращении действия указанного сертификата. С момента уведомления Банк прекращает электронный документооборот с Клиентом с использованием указанного сертификата;
11. Клиент после получения сообщения о компрометации сертификата выводит соответствующий сертификат из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации;
12. Банк имеет право в любое время производить замену собственных сертификатов.