**Приложение №12**

**Описание протокола информационного взаимодействия по онлайн запросам ЕПС к серверу Клиента №2**

# 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** | **pay** |
| --- | --- | --- | --- | --- | --- |
| **command** | Предопределенная строка. Возможные значения: **check, pay,** | Определяет тип запроса | **check** – поиск Плательщика (проверка номера); **pay**– создание платёжной транзакции; | + | + |
| **account** | Строка до 15 символов | Лицевой счет Плательщика |  | + | + |
| **sum** | Число | Сумма платежа | Разделитель “.” (точка). |  | + |
| **txn\_id** | Целое число | Идентификатор платежной транзакции | Целое число длиной до 20 знаков. По этому идентификатору производится дальнейшая сверка взаиморасчетов и решение спорных вопросов |  | + |
| **txn\_date** | Дата и время | Дата и время операции в ЕПС | Дата платежа (дата получения запроса от клиента). Передается в формате ГГГГММДДЧЧММСС |  | + |

# 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** | **pay** |
| --- | --- | --- | --- | --- | --- |
| **osmp\_txn\_id** | Число | номер транзакции в системе Банка | номер транзакции в системе Банка, который передается Клиенту в переменной txn\_id | + | + |
| **result** | Число | код результата завершения запроса | код результата завершения запроса. | + | + |
| **comment** | текст | комментарий завершения операции | необязательный элемент – комментарий завершения операции | + | + |
| **prv\_txn** | Целое число | уникальный номер операции пополнения баланса Абонента | уникальный номер операции пополнения баланса Абонента (в базе Клиента). Этот элемент должен возвращаться Клиентам после запроса на пополнение баланса (запроса «pay»). При ответе на запрос на проверку состояния Абонента (запрос «check») его возвращать не нужно – он все равно не обрабатывается. |  | + |
| **sum** | Число со знаком | сумма платежа | дробное число с точностью до сотых, в качестве разделителя используется «.» (точка). Если сумма представляет целое число, то оно все равно дополняется точкой и нулями, например – «152.00». | + |  |

**Список кодов завершения**

При обработке запросов от системы Банка, Клиент должен сопоставить все возникающие в его приложении ошибки с приведенным ниже списком и возвращать соответствующие коды в элементе <result>. Знак «+» в столбце фатальность показывает то, как система будет интерпретировать данную ошибку.

|  |  |  |
| --- | --- | --- |
| **Код** | **Комментарий** | **Фатальность** |
| 0 | ОК |  |
| 1 | Временная ошибка. Повторите запрос позже |  |
| 4 | Неверный формат идентификатора Плательщика | + |
| 5 | Идентификатор Плательщика не найден (Ошиблись номером) | + |
| 7 | Прием платежа запрещен провайдером | + |
| 8 | Прием платежа запрещен по техническим причинам | + |
| 79 | Счет Плательщика не активен | + |
| 90 | Проведение платежа не окончено |  |
| 241 | Сумма слишком мала | + |
| 242 | Сумма слишком велика | + |
| 243 | Невозможно проверить состояние счета | + |
| 300 | Другая ошибка провайдера | + |

**Примеры обменов сообщениями «запрос – ответ»**

Платежное приложение Клиента payment\_app.cgi, располагается по адресу service.someprv.ru, сервер поддерживает HTTPS соединения на порт 8443.

**Поиск плательщика по лицевому счету:**

|  |  |
| --- | --- |
| Запрос | https://service.someprovider.ru:8443/payment\_app.cgi?command=check&txn\_id=1234567&account=4957835959&sum=10.45 |
| Ответ | <?xml version="1.0" encoding="UTF-8"?>  <response>  <osmp\_txn\_id>1234567</osmp\_txn\_id>  <result>0</result>  </response>  *При наличии комментария к коду результата завершения запроса ответ будет выглядеть следующим образом:*  <?xml version="1.0" encoding="UTF-8"?>  <response>  <osmp\_txn\_id>1234567</osmp\_txn\_id>  <result>0</result>  <comment>account exists</comment>  </response> |

**Пример запроса на пополнение лицевого счета**

|  |  |
| --- | --- |
| Запрос | https://service.someprovider.ru:8443/payment\_app.cgi?command=pay&txn\_id=1234567&txn\_date=20050815120133&account=4957835959&sum=10.45 |
| Ответ | <?xml version="1.0" encoding="UTF-8"?>  <response>  <osmp\_txn\_id>1234567</osmp\_txn\_id>  <reg\_date>10/10/2016 14:34:54.438 +03:00</reg\_date>  <prv\_txn>2016</prv\_txn>  <sum>10.45</sum>  <result>0</result>  </response>  *При наличии комментария к коду результата завершения запроса ответ будет выглядеть следующим образом:*  <?xml version="1.0" encoding="UTF-8"?>  <response>  <osmp\_txn\_id>1234567</osmp\_txn\_id>  <prv\_txn>2016</prv\_txn>  <sum>10.45</sum>  <result>0</result>  <comment>OK</comment>  </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.