**ПРОТОКОЛ 1**

# Лист регистрации изменений

|  |  |  |  |
| --- | --- | --- | --- |
| **Версия** | **Описание изменений** | **Автор** | **Дата** |
| 1.00 | Начальная версия | Федулин А.С. | 19.09.2019 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Данные сторон для подключения**
   1. Контактные данные

|  |  |  |
| --- | --- | --- |
| **ФИО** | **E-mail** | **Телефон** |
| **Банк** | | |
|  |  |  |
|  |  |  |
| **Клиент** | | |
|  |  |  |
|  |  |  |

* 1. Адрес ссылки Клиента URL, вида:

<https://service.someprovider.ru:port/pay.pl> либо <https://xxx.xxx.xxx.xxx:port/pay.pl>, где

**service.someprovider.ru** – доменное имя или xxx.xxx.xxx.xxx – ip адрес сервера Клиента

**port** – поддерживаются порты 443, 1443, 3443, 4443, 5443, 7443, 8443, 9443, 8080, 8081, 8181, 8444.

**pay.pl** – указание сервиса платежной системы.

* 1. Диапазоны адресов серверов ЕПС:

194.186.207.0/24

194.54.14.0/24

1. **Основные принципы работы интерфейса**
   1. Клиент идентифицирует Плательщика по уникальному номеру в своей системе (идентификатор Плательщика, лицевой счет, номер договора, телефона, и т.д.).
   2. Оплата услуг Клиента производится системой в 2 этапа – проверка состояния Плательщика и передача информации о платеже. Для этого используются две команды «**check**» и «**pay**».
   3. При проверке статуса (запрос «**check**») Клиент должен проверить в своей базе наличие Плательщика с указанным идентификатором и выполнить внутренние проверки идентификатора Плательщика.
   4. При проведении платежа (запрос «**payment**») Клиент должен произвести пополнение баланса Плательщика.
   5. Запрос **payment** выполняется после того, как Плательщику печатается чек об оплате.
   6. В методе POST отправляются запросы с такими же параметрами, как в методе GET.
   7. Для авторизации Банка в биллинговой системе Клиента при регистрации платежа можно использовать логин и пароль (basic-auth).
   8. Системой Банка поддерживается SSL-соединение версии TLS 1.0, 1.2.
   9. Интерфейс должен обрабатывать параметры, передаваемые Банком методом GET/POST и формировать ответ Банку в формате XML в кодировке UTF-8/Windows-1251.
   10. Если количество платежей за услуги Клиента ожидается интенсивным (10 платежей в минуту и более), необходимо, чтобы интерфейс Клиента поддерживал многопотоковую коммуникацию до 15 одновременных соединений.
2. **Параметры запросов платёжной системы**

| **Параметр** | **Значение** | **Назначение** | **Примечание** | **check** | **payment** |
| --- | --- | --- | --- | --- | --- |
| **ACTION** | Возможные значения: **check**,**payment** | Определяет тип запроса | **check** – поиск Плательщика (проверка идентификатора); **payment** – создание платёжной транзакции | + | + |
| **ACCOUNT** | Строка (определяется сценарием платежа) | 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 платежной системе | Дата и время операции в платежной системе по часовому поясу платежной системы в формате “DD.MM.YYYY\_HH24:MI:SS”. Между датой и временем стоит символ “\_” (подчеркивание) |  | + |

1. **Пример запроса на проверку**

Платежное приложение Клиента payment\_app.cgi, располагается по адресу service.someprv.ru, сервер поддерживает HTTPS соединения на порт 443. Для проверки состояния Плательщика система Банка генерирует запрос вида (команда **check**, метод GET):

**https://service.someprovider.ru:8443/payment\_app.cgi?ACTION=check&ACCOUNT=49578**

Запрос «**check**» содержит переменные:

**ACTION**=**check** – запрос на проверку состояния Плательщика

**ACCOUNT**=49578 – идентификатор Плательщика в информационной системе Клиента

Ответ Клиента на запрос «**check**» должен выглядеть так:

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

<response>

<CODE>0</CODE>

<MESSAGE>account exist</MESSAGE>

</response>

<response> – тело ответа

<CODE> – код результата завершения запроса (Клиент всегда возвращает код на запрос Банка, коды результата запроса/ошибок приведены в Параграфе 5).

<MESSAGE> – комментарий завершения операции.

Возвращение result=0 на запрос «**check**» говорит о том, что лицевой счет Плательщика найден иможет быть пополнен.

*Если у Клиента есть ограничения на пополнение баланса, об этом необходимо сообщить менеджеру Банка.*

Также при ответе на запрос «**check**» можно передавать следующие данные:

<FIO> – ФИО Плательщика (текстовое поле, длина символов)

<ADDRESS> – адрес (текстовое поле, длина символов)

<BALANCE> – текущий баланс (число, разделитель точка «.»,длина символов)

<REC\_SUM> – рекомендуемая сумма пополнения счета (строго положительное число, разделитель точка «.», длина символов)

<INFO> – информационный параметр для отображения Плательщику (текстовое поле)

Пример ответа с дополнительными параметрами запрос «**check**»:

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

<response>

<CODE>0</CODE>

<MESSAGE>account exist</MESSAGE>

<FIO>Яковлев Петр</FIO>

<ADDRESS>Москва, Курская 19, кв.125</ADDRESS>

<BALANCE>100.00</BALANCE>

<REC\_SUM>500.00</REC\_SUM>

<INFO>Оплата интернет услуг, тариф 100мб/с</INFO>

</response>

1. **Пример запроса на Оплату**

Для проведения платежа система Банка генерирует запрос вида (команда **payment**, метод GET):

**https://service.someprovider.ru:8443/payment\_app.cgi?ACTION=payment&ACCOUNT=49578&AMOUNT=340.24& PAY\_ID=123456789012& PAY\_DATE=12.06.2018\_12:45:18**

Запрос содержит переменные:

**ACTION**=payment – запрос на пополнение баланса Плательщика

**PAY\_ID**=123456789012 – внутренний номер платежа в системе Банка

**PAY\_DATE** =12.06.2018\_12:45:18 – дата учета платежа в системе Банка

**ACCOUNT**=49578 – идентификатор Плательщика в информационной системе Клиента

**AMOUNT**=340.24 – сумма к зачислению на лицевой счет Плательщика (дробное число с точностью до сотых, в качестве разделителя используется «.» точка)

Клиент возвращает ответ на запрос «**payment**» Банка в формате XML со структурой:

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

<response>

<CODE>0</CODE>

<MESSAGE>payment Successful</MESSAGE>

</response>

<response> – тело ответа

<CODE> – код результата завершения запроса

<MESSAGE> – комментарий завершения операции.

Возвращение result=0 на запрос «**payment**» означает, что платеж подтвержден в системе Клиента и баланс Плательщика пополнен.

Пример ответа с дополнительными параметрами запрос «**payment**»:

<**EXT\_ID**> – уникальный номер операции пополнения баланса Плательщика (в базе Клиента), целое число длиной до 20 знаков. Клиент должен возвращать <EXT\_ID> только в ответ на пополнение баланса (запрос «pay»).

<**REG\_DATE**> – дата регистрации в системе Клиента.

<**AMOUNT**> – сумма пополнения баланса Плательщика.

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

<response>

<EXT\_ID>9876543210<EXT\_ID>

<REG\_DATE>12.06.2018\_12:45:22</REG\_DATE>

<AMOUNT>340.24</AMOUNT>

<CODE>0</CODE>

<MESSAGE>payment Successful</MESSAGE>

</response>

1. **Коды ответов (ошибок)**

Клиент в ответе на запрос банка должен сопоставить все возникающие в его приложении ошибки с приведенным ниже списком и возвращать соответствующие коды в элементе <CODE>. Знак «+» показывает, на каком запросе можно возвращать код ответа (ошибку).

*Пример: Система Банка отправляет запрос «****payment****», но ответ Клиента не укладывается в 7 секунд. При этом Клиент регистрирует платеж в своей системе. Через некоторое время Банк повторно отправит идентичный запрос «****payment****» и будет ожидать ответ Клиента с CODE=8 и комментарием «Дублирование транзакции».*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Код ответа** | **Назначение** | **Примечание** | **check** | **payment** | **Сторона ошибки** |
| **0** | Успешное завершение операции | Операция прошла успешно. Транзакция подтверждена, платеж в системе Клиента создан | + | + |  |
| **1** | Временная ошибка. Повторите запрос позже |  | + | + | ПУ |
| **2** | Неизвестный тип запроса | Неизвестное значение поля | + | + | Банк |
| **3** | Абонент не найден |  | + | + | Клиент |
| **4** | Неверный формат идентификатора Плательщика |  | + | + | Клиент |
| **5** | Счет Плательщика не активен |  | + | + | ПУ |
| **6** | Неверное значение идентификатора транзакции | Недопустимое значение поля идентификатора платёжной транзакции в платёжной системе  (” **PAY\_ID**”) |  | + | Банк |
| **7** | Прием платежа запрещен по техническим причинам |  |  | + | ПУ |
| **8** | Дублирование транзакции | Операция прошла успешно. Транзакция подтверждена, платеж в системе Клиента создан ранее |  | + |  |
| **9** | Неверная сумма платежа | Недопустимое значение для поля платежа (“**AMOUNT**”) |  | + | Банк |
| **10** | Сумма слишком мала |  |  | + | Банк |
| **11** | Сумма слишком велика |  |  | + | Банк |
| **12** | Неверное значение даты | Недопустимое значение поля даты платежа  (“ **PAY\_DATE**”) |  | + | Банк |
| **300** | Внутренняя ошибка Организации | Иная ошибка с обязательным указанием причины отказа в поле <MESSAGE> | + | + | ПУ |

1. **Порядок использования SSL-Сертификатов**
   1. **Сертификат Клиента**
      1. Клиент предоставляет Банку корневой сертификат Клиента в виде, пригодном для установления его принадлежности Клиенту (в виде base-64 кодированного файла руководителя и оттиском печати Клиента).
      2. По истечении срока действия корневого сертификата 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 Клиент извещает Банк о прекращении действия указанного сертификата по электронной почте. С момента получения уведомления Банком Клиент прекращает электронный документооборот с Банком с использованием указанного сертификата.
      4. Банк выводит компрометированный сертификат из действия после получения сообщения о компрометации от Клиента не позднее рабочего дня, следующего за днём получения сообщения о компрометации.
      5. В случае необходимости замены собственных сертификатов Клиент должен уведомить Банк по электронной почте не позднее, чем за 5 (пять) рабочих дней.
   2. **Сертификат Банка**
      1. Банк предоставляет Клиенту электронный запрос на получение сертификата (CSR) по стандарту ISO с алгоритмом шифрования RSA, хэширования SHA2 и длиной сеансового ключа не менее 1024 байт.
      2. Клиент возвращает Банку обработанный на стороне Клиента сертификат Банка и предоставляет свой корневой сертификат в формате CRT.
      3. Клиент регистрирует сертификат Банка для аутентификации Банка при открытии SSL-сессии в режиме взаимной аутентификации (2-хсторонний SSL).
      4. По 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.
      5. При компрометации или подозрении на компрометацию закрытого ключа сертификата Банк извещает Клиента о прекращении действия указанного сертификата по электронной почте. С момента получения уведомления Клиентом Банк прекращает электронный документооборот с Клиентом с использованием указанного сертификата.
      6. Клиент выводит компрометированный сертификат из действия после получения сообщения о компрометации от Банка не позднее рабочего дня, следующего за днём получения сообщения о компрометации.
      7. В случае необходимости замены собственных сертификатов Банк должен уведомить Клиента по электронной почте не позднее, чем за 5 (пять) рабочих дней.