

ПРИЛОЖЕНИЕ 16. ПРОТОКОЛ 2

1. ДАННЫЕ СТОРОН ДЛЯ ПОДКЛЮЧЕНИЯ

1.1. Контактные данные

ФИО	E-mail	Телефон
Банк		
Клиент		

1.2. 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.

1.3. Диапазоны адресов серверов ЕПС:

194.186.207.0/24

194.54.14.0/24

2. ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ ИНТЕРФЕЙСА

2.1. Клиент идентифицирует Плательщика по уникальному номеру в своей системе (идентификатор Плательщика, лицевой счет, номер договора, телефона, и т.д.).

2.2. Оплата услуг Клиента производится системой в 2 этапа – проверка состояния Плательщика и передача информации о платеже. Для этого используются две команды «**check**» и «**pay**».

2.3. При проверке статуса (запрос «**check**») Клиент должен проверить в своей базе наличие Плательщика с указанным идентификатором и выполнить внутренние проверки идентификатора Плательщика.

2.4. При проведении платежа (запрос «**pay**») Клиент должен произвести пополнение баланса Плательщика.

2.5. Запрос «**pay**» выполняется после того, как Плательщику печатается чек об оплате.

2.6. В методе POST отправляются запросы с такими же параметрами, как в методе GET.

2.7. Для авторизации Банка в биллинговой системе Клиента при регистрации платежа можно использовать логин и пароль (basic-auth).

2.8. Системой Банка поддерживается SSL-соединение версии TLS 1.0, 1.2.

2.9. Интерфейс должен обрабатывать параметры, передаваемые Банком методом GET/POST и формировать ответ Банку в формате XML в кодировке UTF-8/Windows-1251.

2.10. Если количество платежей за услуги Клиента ожидается интенсивным (10 платежей в минуту и более), необходимо, чтобы интерфейс Клиента поддерживал многопоточную коммуникацию до 15 одновременных соединений.

3. ПАРАМЕТРЫ ЗАПРОСОВ ПЛАТЁЖНОЙ СИСТЕМЫ

Параметр	Значение	Назначение	Примечание	check	pay
command	Возможные значения: check, pay.	Определяет тип запроса	check – поиск Плательщика (проверка идентификатора); pay – создание платёжной транзакции	+	+
account	Строка (определяется сценарием платежа)	Лицевой счет Плательщика		+	+
sum	Число	Сумма платежа	Разделитель “.” (точка)	+	+
txn_id	Число (содержит только цифры, длина максимум 20 знаков)	Идентификатор платёжной транзакции	Положительное длинное целое число. Генерируется платёжной системой и используется для идентификации платёжных транзакций.	+	+
txn_date	Дата и время	Дата и время операции в платёжной системе	Дата и время операции в платёжной системе (формат ГГГГММДДЧЧММСС, часовой пояс всегда МСК UTC+3)	-	+

4. ПРИМЕР ЗАПРОСА НА ПРОВЕРКУ

Платёжное 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 следующего вида (команда «**check**», метод GET):

`https://service.someprovider.ru:443/payment_app.cgi?command=check&txn_id=1&account=49578&sum=1.00`

Запрос «**check**» содержит переменные:

command=check – запрос на проверку состояния Плательщика

txn_id=1 – внутренний номер платежа в системе Банка, используется для сверки платежей и решения спорных вопросов

account=49578 – идентификатор Плательщика в информационной системе Клиента

sum=1.00 – сумма к зачислению на лицевой счет Плательщика

При запросе «**pay**» в параметрах **txn_id** и **sum** передаются константы (требование протокола OSMP), при запросе «**pay**» формируются реальные данные из системы Банка.

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>0</result>
<comment>account exists</comment>
</response>
```

<response> – тело ответа

<result> – код результата завершения запроса (клиент всегда возвращает код на запрос Банка, коды результата запроса/ошибок приведены ниже).

<comment> – комментарий завершения операции.

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

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 клиенту (текстовое поле)

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

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<response>
```

```
<txn_id>1</txn_id>
```

```
<result>0</result>
```

```
<comment>account exists</comment>
```

```
<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>
```

5. ПРИМЕР ЗАПРОСА НА ОПЛАТУ

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

https://service.someprovider.ru:443/payment_app.cgi?command=pay&txn_id=123456789012&txn_date=20180619120133&account=49578&sum=10.45

Запрос содержит переменные:

command=pay – запрос на пополнение баланса Плательщика

txn_id=123456789012 – внутренний номер платежа в системе Банка

txn_date=20180619120133 – дата учета платежа в системе Банка

account=49578 – идентификатор Плательщика в информационной системе Клиента

sum=10.45 – сумма к зачислению на лицевой счет Плательщика (дробное число с точностью до сотых, в качестве разделителя используется «.» точка)

Клиент возвращает ответ на запрос **pay** Банка в формате XML со структурой:

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<result>0</result>
<comment>payment successful</comment>
</response>
```

<response> – тело ответа

<sum> – 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»

<result> – код результата завершения запроса.

<comment> – комментарий завершения операции.

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

При ответе на запрос «**pay**» можно передавать следующие данные:

<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.

<sum> – сумма пополнения баланса Плательщика

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

```
<?xml version="1.0" encoding="UTF-8"?>
<response>
<ext_id>9876543210</ext_id>
<reg_date>20180619120137</reg_date>
<sum>10.45</sum>
<result>0</result>
<comment>payment successful</comment>
</response>
```

6. 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 **<result>**. Знак «+» показывает, на каком запросе можно возвращать код ответа (ошибку).

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

Код ответа	Назначение	Примечание	check	pay
0	Успешное завершение операции	Операция прошла успешно. Транзакция подтверждена, платеж в системе клиента создан	+	+
1	Временная ошибка. Повторите запрос позже		+	+
2	Неизвестный тип запроса	Неизвестное значение поля	+	+
3	Платательщик не найден		+	+
4	Неверный формат идентификатора Плательщика		+	+
5	Счет Плательщика не активен		+	+
6	Неверное значение идентификатора транзакции	Недопустимое значение поля идентификатора платёжной транзакции в платёжной системе ("txn_id").		+
7	Прием платежа запрещен по техническим причинам			+
8	Дублирование транзакции	Операция прошла успешно. Транзакция подтверждена, платеж в системе клиента создан ранее		+
9	Неверная сумма платежа	Недопустимое значение для поля платежа ("sum").		+
10	Сумма слишком мала	Сумма слишком мала		+
11	Сумма слишком велика	Сумма слишком велика		+
12	Неверное значение даты	Недопустимое значение поля даты платежа ("txn_date").		+
300	Внутренняя ошибка Организации	Иная ошибка с обязательным указанием причины отказа в поле <comment>.	+	+

7. ПОРЯДОК ИСПОЛЬЗОВАНИЯ SSL-СЕРТИФИКАТОВ

7.1. Сертификат Клиента

7.1.1. 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).

7.1.2. 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.

7.1.3. 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.

7.1.4. Банк выводит компрометированный сертификат из действия после получения сообщения о компрометации от Клиента не позднее рабочего дня, следующего за днём получения сообщения о компрометации.

7.1.5. В случае необходимости замены собственных сертификатов Клиент должен уведомить Банк по электронной почте не позднее, чем за 5 (пять) рабочих дней.

7.2. Сертификат Банка

7.2.1. 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.

7.2.2. Клиент возвращает Банку обработанный на стороне Клиента сертификат Банка и предоставляет свой корневой сертификат в формате CRT.

7.2.3. Клиент регистрирует сертификат Банка для аутентификации Банка при открытии SSL-сессии в режиме взаимной аутентификации (2-хсторонний SSL).

7.2.4. 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.

7.2.5. 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.

7.2.6. Клиент выводит компрометированный сертификат из действия после получения сообщения о компрометации от Банка не позднее рабочего дня, следующего за днём получения сообщения о компрометации.

7.2.7. В случае необходимости замены собственных сертификатов Банк должен уведомить Клиента по электронной почте не позднее, чем за 5 (пять) рабочих дней.