*Последнее обновление: 14/05/2018. Версия документа: 1.0.*

**Спецификация протокола взаимодействия между системой**

**«alif.pro» и агентами по приему платежей с web ресурсов**

**Формат передачи данных**

**Протокол:**

Передача данных между «alif.pro» (**далее Алиф**) и агентами по приёму платежей (**далее Партнер**) построена на основе протокола HTTPS (RFC 2818: HTTP/1.1).

**Метод передачи данных:**

Для передачи данных используется метод POST – поток данных передается в теле запроса, отправляемого Партнером Алифу.

**Формат данных:**

Данные передаются в формате JSON (JavaScript Object Notation). JSON API является программным интерфейсом, который позволяет автоматизировать процессы авторизации, отправки платежей и проверки статуса. Формат и структура данных в JSON API разработана на концепции открытого стандарта JavaScript.

Подробнее о формате запроса и ответа смотрите ниже.

**Организация протокола**

Взаимодействие Алиф и Партнера происходит следующим образом:

1. Партнер формирует запрос в формате JSON, включая в него необходимые действия, и передает его по протоколу HTTPS на сервер Алифа по адресу <https://alifpay.tj/web> Пример запроса в php можно увидеть в файле sample.php.

2. Сервер осуществляет авторизацию клиента и разбор JSON .

3. В случае успешной авторизации сервер выполняет действия. Сервер возвращает клиенту ответ в формате JSON, в том числе результат выполнения запроса (ОК или код ошибки в случае ошибки).

**Безопасность:**

1. Интерфейс должен принимать запросы с IP адресов, которые были предварительно переданы техническим сотрудникам Алиф.

2. В обмене используется набор полей:

1. Аутентификационный токен($token) – Генерируется Партнером. Состоит из хэшированной (**sha256**) строки текста (конкатенация строк Ключ, ID заказа, Сумма платежа и номера телефона отправителя), которая подписывается **секретным словом**. Этот **token** будет использоваться во всех запросах как часть процесса аутентификации.
2. Ключ ($key) и Пароль ($pass) - Генерируется и передается приватно Партнеру со стороны Алиф.
3. Обратный адрес ($сallbackUrl) – URL, по которому Алиф ответить о статусе платежа.
4. Возврат на сайт Торговца ($returnUrl) – URL, по которому можно вернуться к Торговцу.
5. Сумма платежа ($amount) – сумма вводимая плательщиком в интерфейсе продавца. Смотрите правила преобразования данного поля.
6. ID заказа ($orderID) – Уникальный номер заказа. Генерируется и передается со стороны Партнёра. Может быть использован для проверки статуса платежа.
7. Информационное поле ($info) - инфо платежа. например - "Оплата за телефон".
8. Номер телефона ($phone) – Номер телефона отправителя платежа.
9. Адрес электронной почты ($email) -
10. Секретное слово ($secretkey) - Генерируется и передается приватно Партнеру со стороны Алиф.
11. Пример тела запроса и ответа:

Запрос:

<form name="AlifPayForm" action="https://alifpay.tj/web/" method="POST" id="alifPayForm">

<input type="hidden" name="token" id="token" value="<?php echo $token;?>">

<input type="hidden" name="key" id="key" value="<?php echo $a->key;?>">

<input type="hidden" name="callbackUrl" id="callbackUrl" value="<?php echo $a->callbackUrl;?>">

<input type="hidden" name="returnUrl" id="returnUrl" value="<?php echo $a->returnUrl;?>">

<input type="hidden" name="amount" id="amount" value="<?php echo $a->amount;?>">

<input type="hidden" name="orderId" id="orderId" value="<?php echo $a->orderid;?>">

<input type="hidden" name="info" id="info" value="<?php echo $a->info;?>">

<input type="hidden" name="email" id="email" value="<?php echo $a->email;?>">

<input type="hidden" name="phone" id="phone" value="<?php echo $a->phone;?>">

<input type="submit" value="Пардохт бо корти милли">

</form>

Ответ:

{

"orderId": "12345678",

"transactionId": "92938922",

"status": "ok",

"token": "3792cujidwjkd87867818dj19djdad32d23f2f",

"amount": 10,

"phone": "+992931234455"

}

**orderId:** Номер заказа, по которому вы отправили запрос на проведение платежа

**transactionId:** уникалный ID транзакции, генерируется Алифом и передается Партнёру.

**status:** статус платежа "ok" или "failed"

**token:** аутентификационный токен для проверки валидности ответа. Смотрите порядок проверки валидности токена для ответа.

**amount:** сумма платежа. Смотрите порядок создания суммы.

**phone:** номер телефон плательщика

1. Порядок создания token-ов и ключей

2. 1. Token для проведения платежа

Перед созданием token-а следует преобразовать сумму в нужный формат:

*$amount = sprintf('%.2f',$amount);*

Только после этого создать token:

*$token = hash\_hmac('sha256', $key.$orderid.$amount.$callbackUrl, $secretkey);*

* 1. Секретный ключ для создания token

*$secretkey = hash\_hmac('sha256', $pass, $key);*

*$pass and $key: Генерируется и передается приватно со стороны Алиф*

* 1. Token для использования в ответе и его проверка

*$token = hash\_hmac('sha256', $orderid.$status.$transactionId, $secretkey);*

*if ($token == $resp->token) {*

*// do something*

*}*

1. Проверка статуса оплаты

Для проверки статуса транзакции следует отправить запрос на:

<https://alifpay.tj/web/checktxn>

Пример тела запроса:

{

"orderId": "12345678",

"key": "334122",

"token": "32l1hejldksldj378yd32nidh32uih32d23d2ioj23d"

}

**orderId**: для которого вы хотите проверить статус.

**key:** генерируется и передается приватно со стороны Алиф.

**token:** аутентификационный token.

Создание token-а для проверки статуса транзакции:

*hash\_hmac('sha256', $key.$orderid, $secretkey);*

Пример тела ответа:

{

"orderId": "12345678",

"transactionId": "92938922",

"status": "ok",

"token": "3792cujidwjkdj981uj918dj19djdad32d23f2f",

"amount": 10,

"phone": "+992931234455"

}

Детальный пример запросов можно посмотреть в файле sample.php, который предоставляется вместе с SDK.