Table of Contents

Правила работы с подписью сообщений

Подготовка к работе с подписью

- Создание ключей для подписи сообщений

Чтобы сгенерировать хранилище ключей и ключи выполняем следующую команду, заполняя параметры в угловых скобках:

```
keytool -genkeypair -alias <putalias> -keyalg RSA -keysize 2048 -keystore <keystore-name>.jks -validity 3650
```

После запуска этой команды, нужно будет ввести пароль для кейстора и информацию о владельце кейстора.

- Из созданного кейстора необходимо извлечь публичный ключ, которым будет проверяться подпись. Для этого выполняется команда в терминале

```
keytool -list -rfc --keystore ./<keystore-name>.jks | openssl x509 -inform pem -pubkey
```

После выполнения команды, попросят ввести пароль от кейстора. Если пароль верный, то будет выведен публичный ключ в терминал. Нам необходимо скопировать всё то, что находится между ----BEGIN PUBLIC KEY ----- и ----- END PUBLIC KEY -----. После этого удалить пробелы (переходы на новую строку) из этого текста. Это base64 кодированный публичный ключ. Его необходимо выслать, для возможности проверки подписи запросов.

Пример как оно должно выглядеть в терминале:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlx+NktOTbyRZIIgvHTcB
6P7eaSrwxHtcODspTKlorE9DTMSdjJfxF8qI41GUZUZmN2U2Oa9O/7eiw6KTTz4i
R5Yqn49gBm0hWq2FT2hVqK7l7pzGy1QR1jO/uayJSPxRbFuL1RZ34vnmjm7/4LtJ
EAM00Ctd6t84DAReaeRqdnGZB46xvXsL1svS+v+0IKE+loNuVGQ+0XM02C+yLW+h
QkehEJXOL30VFYtKL31V0nKgHIyDTWdaODcdOlD8SGF4BDQtvLSXQOKE5B9RTLJd
xprz+jh4qe2ErurzHiNdPCquOPINuXaNxIDnMlOlwnTMvw+3GPLhFSDm+sg5qgLY
XQIDAQAB
-----END PUBLIC KEY-----
```

Подписание запросов.

Работа со строками производится в кодировке UTF-8

Запрос подписывается по следующим правилам:

1) Значения всех полей запроса склеиваются в одну строку, в порядке следования их в документе Interaction.html. Пустые и null поля пропускаются. (в кодировке UTF-8)

2) Далее полученное значение шифруется с помощью приватного ключа по алгоритму SHA256withRSA

3) Полученное значение переводится в base64 строку и отправляется в параметре sign.

Проверка подписи.

Работа со строками производится в кодировке UTF-8

Проверка подписи происходит по следующим правилам:

1) Значения всех полей запроса склеиваются в одну строку, в порядке следования их в документе Interaction.html СБП Мастера. Пустые и null поля пропускаются.

2) Полученное значение расшифровывается по алгоритму SHA256withRSA(с публичным ключом подписавшего) и сравнивается со строкой из параметра sign.

3) При совпадении запрос продолжает работу. При не совпадении возвращается сообщение с ошибкой.

Пример формирования строки для подписи:

```
{
   "legalId":"LF000s000001",
   "account":"45202569874125369 8",
   "merchantId":"MF0000q00001",
   "templateVersion":"01",
   "qrcType":"01",
   "amount":"1000.00",
   "currency":"RUB",
   "paymentPurpose":"sadasdasdas",
   "paymentDetails":{
      "dateTime":"2019-06-10T14:26:40.066Z",
      "code":0,
      "kktRegId":"123qe2311",
      "shiftNumber":0,
      "requestNumber":0,
      "operator":"adsda",
      "retailAddress":"adasda",
      "user":"adsasdas",
      "items":[
         {
            "quantity":0,
            "productCode":"adasd",
            "price":"1000.00",
            "name":"dasdasdsa",
            "sum":0
         }
      ]
   },
   "callbackMerchantNotifications":"asdasdasdsa"
}
```

Поля склеиваются как строки, числа переводятся в соответствующие строки. Если в запросе присутствуют вложенные объекты - из них извлекаются только поля. Для массивов склеиваются значения всех полей элементов. Пример строки для этого запроса:

```
LF000s000001452025698741253698MF0000q0000101011000.00RUBsadasdasdas2019-06-
10T14:26:40.066Z0123qe231100adsdaadasdaadsasdas0adasd1000.00dasdasdsa0asdasdasdsa
```

Last updated 2022-08-25 16:10:41 +03:00