钱包提现接口文档

目录

1. 前言

- 本文档如果有疑义，请及时与对接人员联系
- 所有签名示例均只是方法示例，参数不完全相符

2. 请求说明

- 接口需要 Http 请求，支持 Post 方式。
- Post 方式：Http 的 Post 请求，使用 form 表单的提交方式，提交数据。
- 请求的参数，需要 MD5 与 RSA 加密；返回的参数，需要 RSA 解密，并使用 MD5 加密方式验签
- 编码为 UTF-8

3. 签名说明

- 为了保证数据传输过程中的数据真实性、完整性与安全性，所有接口的数据，都要进行加密。

3.1 MD5 加密

- 加密步骤
  - 步骤 1：将所有参数按照参数名升序。
    - 参数列表为：abc=value1 bcd=value2 bad=value3
    - 排序结果为：abc=value1 bad=value3 bcd=value2
  - 步骤 2：将所有参数用&连接，得到待签名字符串。
    - abc=value1&bad=value3&bcd=value2
  - 步骤 3：将待签名的字符串与开发者的 Key 拼。
    - abc=value1&bad=value3&bcd=value2&key=keyvalue
  - 步骤 4：将拼接起来的字符串做 MD5 运算。
    - MD5(abc=value1&bad=value3&bcd=value2&key=keyvalue)
  - 步骤 5：将计算得出的签名值，转为大写

3.2 RSA 加密

- 加密步骤
  - 待加密串：所有需要传输的参数（去除空字段），按字母表升序排列成 key-value 格式(例: abc=value1&bad=value3...，建议 sign 放在最后)。
  - 接入方用接口提供方的公钥，把待加密串用 RSA 公钥加密算法加密(填充方式为 PKCS#1)，再做 BASE64 编码，将得到的值作为 encrypt_data 字段传输。

- 注意：
  - 接口提供方公钥：由 OpenSSL 根据接口提供方的私钥生成得到，PEM 公钥格式为：a、开头为（-----BEGIN PUBLIC KEY-----）；b、长度为 1024 位；c、填充方式为 PKCS#1；d、无加密。(在开通账号时，接口提供方会将公钥提供给接入方)
  - 如果待加密串长度大于 117 字节，需要分段加密(每 117 字节分为一段，加密后长为 128 字节)，再按顺序拼接成密串(长度为 128 的整数倍字节)。

3.3 RSA 解密

- 加密步骤
  - 待解密串：接口请求返回 data 字段中的数据。
  - 接收方用商户私钥把待解密串先做 BASE64 解码，再用 RSA 私钥解密算法解密(填充方式为 PKCS#1)，得到所有字段组成的 key-value 格式的源串。
  - 注意：
    - 商户私钥：由 OpenSSL 生成得到，PEM 私钥格式为：开头为（-----BEGIN RSA PRIVATE KEY-----)；b、长度为 1024 位；c、填充方式为 PKCS#1；d、无加密。
    - 如果待解密串长度大于 128 字节，需要分段解密(每 128 字节分为一段，解密后长小于等于 117 字节)，再按顺序拼接成源串。

4. 接口说明

4.1 提现接口

4.1.1 参与签名的参数

参数名	是否必传	说明
sign	否	签名
out_sn	是	外部流水号（需保证唯一）
account_name	是	开户名称
bank_type	是	账户类型：对私
card_type	是	卡类型：储蓄卡
account_no	是	银行卡号
amt	是	金额，单位分
head_bank_name	是	总行名称

noncestr	是	随机串，长度固定 16 位
bank_brch	否	支行名称
bank_prov	否	支行所在省
bank_city	否	支行所在市
subbranch_name	否	分行名称
mobile	否	手机号

4.1.2 加密计算

- MD5 签名：以上列表中传输的**非空数据**，**除了 sign** 外，其他的参数，按照 MD5 加密步骤进行签名，得出 sign 值
  - 示例（内容不完全符合上述参数，只是签名方法示例）：
    - 签名原串：account_name=测试&account_no=12313123123123&amt=10&bank_brch=五道口支行&bank_city=北京市&bank_prov=北京&bank_type=对私&card_type=储蓄卡&head_bank_name=中国农业银行&idnumber=13123123&mobile=1851004XXXX&out_sn=15030420 19&subbranch_name=北京分行&key=yrplbrbXdh1502105016WjSS8JSfz8W
    - MD5 结果：FE5C476945E34AB5CBF7366A9A243B03
- RSA 加密：以上列表中传输的**非空数据**，**包括 sign**，按照 RSA 加密步骤进行签名，得出 **encrypt_data** 值
  - 示例（内容不完全符合上述参数，只是签名方法示例）：
    - RSA 加密原串：account_name=测试&account_no=12313123123123&amt=10&bank_brch=五道口支行&bank_city=北京市&bank_prov=北京&bank_type=对私&card_type=储蓄卡&head_bank_name=中国农业银行&idnumber=13123123&mobile=1851004XXXX&out_sn=15030420 19&sign=FE5C476945E34AB5CBF7366A9A243B03&subbranch_name=北京分行
    - RSA 加密后，并进行 BASE64 编码结果：i48aS0BGJ9STiI7/+ZhIYWsiBbJQtlg/j4mqX44dKmQfjREaxbGe8QB42aoYEIpMTdVy6EoE2q4oqGTX7CskGaMNkSEeF/67TFNVRgi+MiTBFrs49uSYW5W3X95ZGphtQwOJleeZkza8zmaP4HpxHb0NDcTiB6Yn0rIpdGNS0viZZpnzd9eFcC3OaFjBQ+GnwzPbe7c8Bi7Buah8qrSJ+Z2eDpszoUZSkRBOQJNX7hEQAPJPXqfQ8uFtogD/6k0rdvHfO4V/wOJ0pgzzkDea5hKEH6YqTEMLUnLvQ9oJfjUZlFpFKMxR+WxhPRZX/mJgYatdvF43YKcUbRCw+U9g/g==

4.1.3 请求接口

- 基本信息

请求方式	请求地址	描述信息
Http 的 Post 方式	/wallet/withdraw	发起提现

- 请求参数

参数名	是否必传	说明
src_code	是	平台唯一标识
encrypt_data	是	RSA 加密后的结果

- **注意：接口请求前，需将 RSA 加密后的结果进行 BASE64 编码，编码后，再发起接口请求。**

- 返回参数

参数名	说明
respcd	返回状态码，0000 为成功，其他即为失败
respmsg	返回信息
data	加密数据

- 返回示例


```
{
    "respcd": "0000",
    "respmsg": "成功",
    "data": "n78+LIvWwGJggzUne04EvZX9ewOpqR0TDUudte26Zr0vVnUGy9AbvWF
oeByV4IKR+I5HKiBnUQF4QpYPSwA2k/9703uccMUc4TJaXGqiRrh6/PSqVxPqM9qYOe
hPCg6l09DHiWfsxx8Zb5oM0MNVWmTuHuXc5abOVOyqkJqxKd8="
}
```


4.1.4 验签

- 将返回的 data 的数据，进行 BASE64 编码
- 编码后，将返回的 data 的数据，根据 RSA 解密方法，进行解密，解密后数据如下

  status=1&sign=F53AC13AEEEF56754CF9782DE7918D79&src_code=xm_1&out_sn=121323123332&biz_sn=20170728135783408

- 解密后，参数说明

参数名	说明
status	提现状态->0：初始化；1：处理中；2：处理成功；3：处理失败；4：退票
sign	签名
src_code	平台唯一标识

out_sn	外部流水号
biz_sn	业务流水号

- 根据 MD5 加密步骤，将以上非空参数（sign 除外）进行签名，得出 sign 值，与返回的 sign 值校验是否一致
- **平台返回的应答或通知消息可能由于升级增加参数，请签名时注意允许这种情况**

4.2 提现状态查询接口

4.2.1 参与签名的参数

参数名	是否必传	说明
noncestr	是	随机串，长度固定 16 位
sign	否	签名
biz_sn	否	业务流水号，注意:biz_sn 与 out_sn 两个参数必须传一个
out_sn	否	外部流水号，注意:biz_sn 与 out_sn 两个参数必须传一个

4.2.2 加密计算

- MD5 签名：以上列表中传输的**非空数据，除了 sign** 外，其他的参数，按照 MD5 加密步骤进行签名，得出 sign 值
- RSA 加密：以上列表中传输的**非空数据，包括 sign**，按照 RSA 加密步骤进行签名，得出 **encrypt_data** 值

4.2.3 请求接口

- 基本信息

请求方式	请求地址	描述信息
Http 的 Post 方式	/wallet/realtime/query	提现状态查询

- 请求参数

参数名	是否必传	说明
src_code	是	平台唯一标识
encrypt_data	是	RSA 加密后的结果

- **注意：接口请求前，需将 RSA 加密后的结果进行 BASE64 编码，编码后，再发起接口请求**

- 返回参数

参数名	说明
respcd	返回状态码，0000 为成功，其他即为失败
respmsg	返回信息
data	加密数据

- 返回示例

{
"respcd": "0000",
"respmsg": "成功",
"data": "XM0XZCNT3Oh0hbBVXSwL2K3asgJcvSm3xGIwdtJ7W36Pxnjj6UsQBMDyPjLpQ8bcRzjHYVcSdOyQbq0/AhC6cJ1ekkFOyyRyJ7to1psjyfrKQiAi7th7HOSuAGmoR+lZMy3NvP4dpLibJzCWCFzDWKPuuDFO6xwSMOsMOALF1mg="
}

4.2.4 验签

- 将返回的 data 的数据，进行 BASE64 编码
- 编码后，将返回的 data 的数据，根据 RSA 解密方法，进行解密，解密后数据如下：

  amt=1000&biz_sn=20170728135783408&out_sn=121323123332&status=2&sign=8C471F7E7426F42A91CD6E9227498AF3

- 解密后，参数说明

参数名	说明
amt	交易总金额（单位分）
biz_sn	业务流水号
out_sn	外部流水号
status	提现状态->0：初始化；1：处理中；2：处理成功；3：处理失败；4：退票
sign	签名

- 根据 MD5 加密步骤，将以上非空参数（sign 除外）进行签名，得出 sign 值，与返回的 sign 值校验是否一致
- **平台返回的应答或通知消息可能由于升级增加参数，请签名时注意允许这种情况**

4.3 余额查询接口

4.3.1 参与签名的参数

参数名	是否必传	说明
noncestr	是	随机串，长度固定 16 位
sign	否	签名

4.3.2 加密计算

- MD5 签名：以上列表中传输的**非空数据，除了 sign** 外，其他的参数，按照 MD5 加密步骤进行签名，得出 sign 值
- RSA 加密：以上列表中传输的**非空数据，包括 sign**，按照 RSA 加密步骤进行签名，得出 **encrypt_data** 值

4.3.3 请求接口

- 基本信息

请求方式	请求地址	描述信息
Http 的 Post 方式	/wallet/query	余额查询

- 请求参数

参数名	是否必传	说明
src_code	是	平台唯一标识
encrypt_data	是	RSA 加密后的结果

- **注意：接口请求前，需将 RSA 加密后的结果进行 BASE64 编码，编码后，再发起接口请求**

- 返回参数

参数名	说明
respcd	返回状态码，0000 为成功，其他即为失败
respmsg	返回信息
data	加密数据

- 返回示例


```
{
    "respcd": "0000",
    "respmsg": "成功",
    "data": "sJFvhzOXktGrSQ//VBDwk1GqYYQO2qhMhvsJREaRrkOWGLGHFSt4wQa
62JOLbIf9u6pFS4Saie8ULEcfAJe34O64h+rlOTkcKM+nWuetfT19bmzpZzXuSN0EqXDrD
```

qJzZK4onSQ7mAe3XUdGMgaBECJyhPkzwXx45s++1Copc3A="
}

4.3.4 验签

- 将返回的 data 的数据，进行 BASE64 编码
- 编码后，将返回的 data 的数据，根据 RSA 解密方法，进行解密，解密后数据如下：

  available=3010&unavailable=0&sign=BACC8C7CE924FAD326CA2899741ED093

- 解密后，参数说明

参数名	说明
available	可用余额（单位分）
unavailable	不可用余额（单位分）
sign	是

- 根据 MD5 加密步骤，将以上非空参数（sign 除外）进行签名，得出 sign 值，与返回的 sign 值校验是否一致
- **平台返回的应答或通知消息可能由于升级增加参数，请签名时注意允许这种情况**
-

5. 返回码说明

5.1 错误码对照

5.1.1 提现发起时 错误码 详细原因见返回值

错误码	错误描述
101	请求参数异常, 下游渠道异常或系统维护, 内部流水号存在,

	余额不足，提现失败
201	提现记录创建失败
401	请求 IP 受限
500	提现记录信息回执失败
600	明文串校验失败， 下游公钥未配置或者格式不正确

补充：1.提现发起失败的错误码 ：101, 401, 600

2.提现发起状态未知的错误码: 201, 500 建议当提现发起成功来处理，等待查询结果

3.提现发起成功的返回码: 0000

5.1.2 提现记录查询时

错误码	错误描述
101	请求参数异常， 下游渠道异常或系统维护， 请求数据无法解密
103	提现记录不存在
401	请求 IP 受限
600	明文串签名验证失败， 下游公钥未配置或者格式不正确， 系统异常
500	提现记录信息回执失败， 秘钥信息初始化失败， 查询失败

补充：1.提现记录查询发起成功的返回码 0000

2.提现记录状态未知返回码 101， 401， 600， 500

3.提现记录不存在的返回码 103

5.2 提现状态的判定

成功：只有当返回码是 0000 并且 data 里面的 status 等于 2 才代表提现成功了

失败：（当返回码是 0000 并且 data 里面的 status 等于 3） 或者（返回码是 103） 才代表提现失败了

待确认：剩下的返回码都需要待确认才可以知道提现记录的最终状态