

title: 统一支付平台网关接口文档 date: 2019-10-23

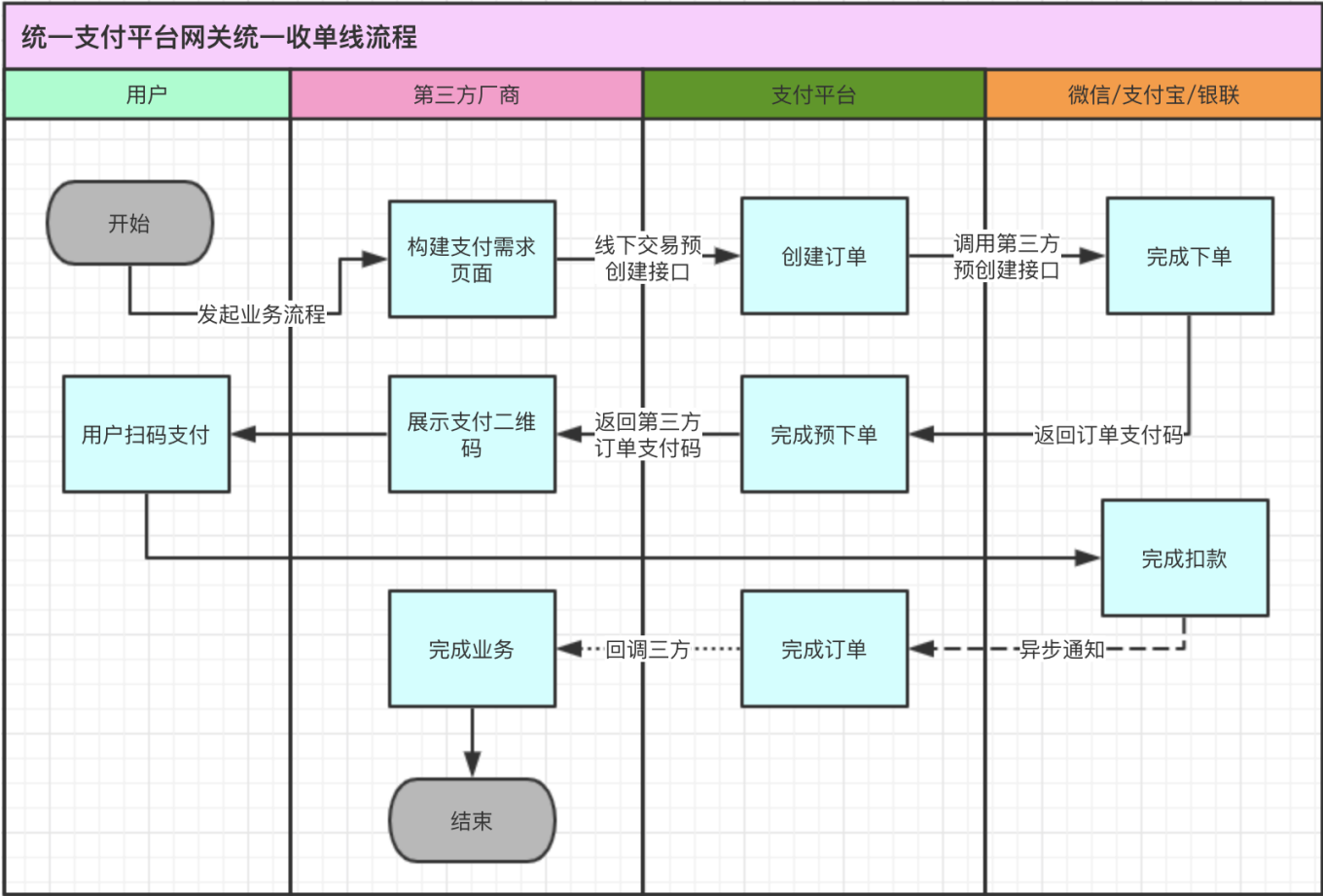
1.1文档说明

本文档用于描述了统一支付平台提供第三方支付网关接口文档，供第三方系统接入对接参考。

1.2约定

1. 传输编码统一为utf-8
2. RSA 加密算法为本接口采用的非对称加密算法，`SIGN_ALGORITHMS ="SHA1WithRSA"`;
3. RSA公钥由本系统提供，本系统返回信息的签名数据，第三方系统得到后通过公钥校验算法，验证返回数据的合法性
4. HMAC加密算法为用户请求本系统采用的加密算法，`SIGN_ALGORITHMS ="HMAC-SHA1"`;
5. 具体签名生成参考后面的签名章节
6. retcode等于success表示成功，其他表示失败，失败具体信息查看retmsg

1.3 流程、数据交互



2.1 统一支付平台网关统一收单线下交易预创建接口

请求URL:

- `https://ip:port/webgate/precreateorder`

请求方式/格式:

- POST
- application/x-www-form-urlencoded

请求参数:

参数名	类型	必选	说明
partner_id	String	是	本系统分配给各个接入应用的合作伙伴id号
notify_url	String	否	统一支付平台主动通知商户系统指定的回调地址
timestamp	String	是	时间戳格式为yyyyMMddhh24miss
sign	String	是	签名,参见附录
sign_method	String	是	参数的加密方法选择, 可选值是: HMAC 具体加密方式为HMAC-SHA1
out_trade_no	String(20)	是	商户网站的唯一订单号, (确保商户系统中唯一)
out_trade_name	String	是	交易名称,用户显示的支付信息
total_amount	String	是	订单金额 (rmb) , 单位分
trade_route	String	是	支付途径 可选值: alipay
remark	String	否	备注信息
stuempno	String	否	用户唯一标识: 学工号
openid	String	否	微信支付需要传入用户的openid

请求内容示例:

```
URI: https://ip:port/webgate/precreateorder

partner_id:10001
notify_url:http://***.***.edu.cn/receive_notify.htm
timestamp:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:HMAC
out_trade_no:2016062115020100000001
out_trade_name:***打印费
total_amount:200
remark:打印费
stuempno:99100210291
openid:oW_0ystmvku==
```

返回示例:

- 成功

```
{
  "retcode": "success",
  "retmsg": "扫码成功成功",
  "qrcode": "https://qr.alipay.com/bax06824wnqpo0erskqs202e",
  "refno": "2019080910201002000001"
}
```

- 失败

```
{
  "retcode": "illegal_param",
  "retmsg": "参数错误"
}
```

- 注意：

1. 此接口原则上只支持 https 请求；
2. 请按照“签名机制”中的签名方法对输入参数进行签名，该接口请求才能够被本系统接收；
3. 此接口支持重复调用，前提是交易基本信息（订单号、交易金额等）在多次调用中保持一致，且交易尚未完成支付。

返回参数说明:

参数名	类型	说明
retcode	String	返回码（success=成功，其他为失败）
retmsg	String	返回消息
refno	String	交易参考号
qrcode	String	二维码内容，第三方自己转成二维码图片

2.2 统一支付平台服务器异步通知参数说明

含义:

统一支付平台对商户的请求数据处理完成后，会将处理的结果数据通过服务器主动通知的方式通知给商户系统。这些处理结果数据就是服务器异步通知参数。

请求方式/格式:

- POST
- application/x-www-form-urlencoded

请求参数:

参数名	类型	必选	说明
notify_time	String	是	时间戳格式为yyyyMMddhh24miss
sign	String	是	签名,参见附录
sign_method	String	是	参数的加密方法选择, 可选值是: RSA
out_trade_no	String	是	商户系统的唯一订单号, (确保商户系统中唯一)
out_channel_trade_no	String	是	第三方支付渠道的唯一流水号
trade_no	String	是	易支付流水号
pay_time	String	是	交易完成时间
trade_status	String	是	交易状态, 成功: TRADE_FINISHED、失败: TRADE_FAIL
total_amount	String	是	订单金额 (rmb) , 单位分
out_channel	String	是	支付渠道, (alipay、wechat、ips)
remark	String	否	备注信息

请求内容示例:

```
URI: http://***.nyu.net/receive_notify.htm

notify_time:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:RSA
out_trade_no:2016062115020100000001
out_channel_trade_no:2016062115020112903920
trade_no:2016062115020100000002
pay_time:20150119130901
trade_status:TRADE_FINISHED
total_amount:20000
out_channel:alipay
remark:打印
```

- 注意:
1. 请按照“签名机制”中的签名方法对输入参数进行验签, 确保请求为本系统发送;
 2. 必须保证服务器异步通知页面 (notify_url) 上无任何特殊字符, 如空格、HTML标签、开发系统自带抛出的异常提示信息等;
 3. 第一次交易状态改变 (即时到账中此时交易状态是交易完成) 时, 服务器异步通知地址会收到本系统发来的处理结果通知
 4. 程序执行完后必须打印输出success, 否则本系统认为回调失败, 会继续回调, 直到次数限制。

2.3 统一支付平台订单查询接口

请求URL:

- <https://ip:port/webgate/precreateorderquery>

请求方式/格式:

- POST
- application/x-www-form-urlencoded

请求参数:

参数名	类型	必选	说明
partner_id	String	是	本系统分配给各个接入应用的合作伙伴id号
pageno	String	否	页码, 默认1
pagesize	String	否	每页行数,默认10, 范围10-500
timestamp	String	是	时间戳格式为yyyyMMddhh24miss
sign	String	是	签名,参见附录
sign_method	String	是	参数的加密方法选择, 可选值是: HMAC 加密方式为HMAC-SHA1
out_trade_no	String	二选一	商户网站的唯一订单号, 单条查询 (确保商户系统中唯一)
order_date	String	二选一	查询日期, 日对账批量查询时使用

请求内容示例:

```
URI: https://ip:port/webgate/precreateorderquery

partner_id:10001
pageno:1
pagesize:10
timestamp:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:HMAC
out_trade_no:2016062115020100000001
```

返回示例:

- 成功

```
{
  "retcode": "success",
  "retmsg": "查询成功",
  "page": {
    "totalCount": 1,
    "pageSize": 10,
    "pageNo": 1,
    "list": [
```

```

        {
            "trade_no": "2016062115020100000002",
            "out_trade_no": "2016062115020100000001",
            "out_channel_trade_no": "2016062115020112903920",
            "pay_time": "20150119130901",
            "trade_status": "TRADE_FINISHED",
            "total_amount": "20000",
            "out_channel": "alipay",
            "remark": "打印",
        },
        ],
        "firstResult": 0,
        "firstPage": true,
        "lastPage": true,
        "nextPage": 1,
        "totalPage": 1,
        "prePage": 1
    }
}

```

- 失败

```

{
    "retcode": "illegal_param",
    "retmsg": "查询失败"
}

```

返回参数说明:

参数名	类型	说明
retcode	String	返回码 (success=成功, 其他为失败)
retmsg	String	返回消息
page	Pagination	Pagination分页

Pagination分页说明:

参数名	类型	说明
totalCount	int	流水记录总数
pageSize	int	每页记录数
pageNo	int	页码
list	List	流水明细数据集
totalPage	int	总页码

参数名	类型	说明
firstResult	int	第一条数据位置
firstPage	boolean	是否第一页
lastPage	boolean	是否最后一页
nextPage	int	下一页
prePage	int	上一页

流水明细说明:

参数名	类型	说明
tradeno	String	交易流水号
out_trade_no	String	第三方交易流水号
out_channel_trade_no	String	外部渠道流水号
pay_time	String	交易时间 yyyyMMddhh24miss
trade_status	String	状态 TRADE_FINISHED-交易完成 TRADE_INIT-交易未完成
total_amount	Inteer	交易金额(分)
out_channel	String	外部渠道标识, alipay
remark	String	交易备注

- 注意:

1. 此接口只支持 https请求;
2. 请按照“签名机制”中的签名方法对输入参数进行签名, 该接口请求才能够被本系统接收;

附录A-用户请求HMAC签名算法

- 签名方式: **hmac-sha1**
- 签名密钥由本系统统一线下提供
- **签名校验的通用步骤如下:**

****第一步,** **设所有发送或者接收到的数据为集合M, 将集合M内非空参数值的参数按照参数名ASCII码从小到大的排序(字典序), 使用URL键值对的格式(即key1=value1&key2=value2...) 拼接成字符串stringA。

假设传送的参数如下:

```
partner_id:10000
stuempno:09893092
tradeno:20160607000001
```

```
trandename:printfee
amount: 2000
timestamp:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:HMAC
```

对参数按照key=value的格式，并按照参数名ASCII字典序排序如下：

```
amount=2000&partner_id=10000&sign_method=HMAC&stuempno=09893092
&timestamp=20150119130901&tradeno=20160607000001&trandename=printfee
```

****特别注意以下重要规则：****

- 参数名ASCII码从小到大排序（字典序）；
- 如果参数的值为空不参与签名；
- 参数名区分大小写；
- 传送的sign参数不参与签名，用该sign值作校验。

****第二步，****用密钥secretkey对stringA字符串，进行hmac-sha1签名，得到sign值signValue。signValue最后采用十六进制小写hex编码生成签名字符串。

附录B-服务端返回数据RSA签名校验算法

- 签名方式：SHA1withRSA
- 签名校验的公钥key为本系统统一线下提供。
- 签名校验的通用步骤如下：

****第一步，****设所有发送或者接收到的数据为集合M，将集合M内非空参数值的参数按照参数名ASCII码从小到大排序（字典序），使用URL键值对的格式（即key1=value1&key2=value2...）拼接成字符串stringA。

特别注意以下重要规则：

- 参数名ASCII码从小到大排序（字典序）；
- 如果参数的值为空不参与签名；
- 参数名区分大小写；
- 传送的sign参数不参与签名，用该sign值作校验。

****第二步，****对sign值进行base64解码，用本系统提供的公钥key对sign签名值解码后的数据基于stringA字符串，进行SHA1withRSA签名验证

举例：

假设传送的参数如下：

```
retcode:1  
retmsg:账户余额不足  
timestamp:20160513155100  
sign_mehtod:RSA
```

对参数按照key=value的格式，并按照参数名ASCII字典序排序如下：

```
retcode=1&retmsg=账户余额不足&timestamp=20160513155100&sign_mehtod=RSA
```