

---

title: 易支付Web网关接口文档-纽大基金会

date: 2016-06-21

update: 2018-05-21

tags:

---

## 1.1 文档说明

---

本文档用于描述了一卡通易支付系统作为统一支付通道提供纽约大学基金会网关接口文档，供基金会系统接入对接参考。

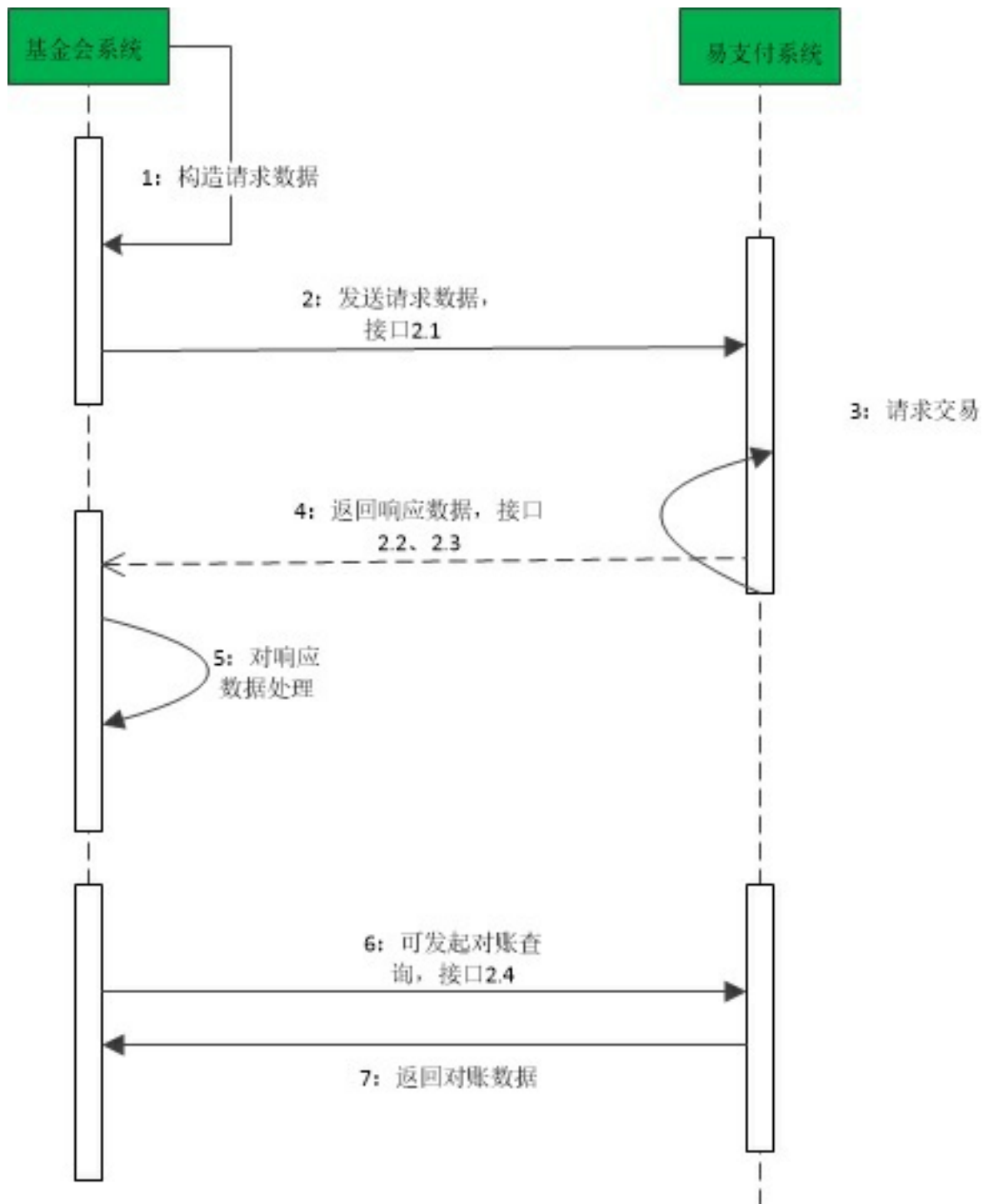
## 1.2 约定

---

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0表示成功，非0表示失败，失败具体信息查看retmsg

## 1.3 流程、数据交互

---



## 2.1 易支付Web网关接口

请求URL:

- <https://ip:port/epay/webgate/donate>

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	易支付主动通知商户里指定的http地址
return_url	String	否	当易支付处理完毕后当前页面跳转到商户网站指定的http路径
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	是	商户网站的唯一订单号, (确保商户系统中唯一)
total_amount	String	是	订单金额 (rmb) , 单位分
remark	String	否	备注信息

请求内容示例:

```
URI: https://ip:port/epay/webgate/donate

partner_id:10001
notify_url:http://***.nyu.net/receive_notify.htm
return_url:http://***.nyu.net/receive_return.htm
timestamp:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:HMAC
out_trade_no:2016062115020100000001
total_amount:20000
remark:donate
```

- 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；
- 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。

## 2.2 易支付页面跳转同步通知参数说明

含义:

易支付对商户的请求数据处理完成后，会将处理的结果数据通过系统程序控制客户端页面自动跳转的方式通知给商户网站。这些处理结果数据就是页面跳转同步通知参数。

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
is_success	String	是	表示接口调用是否成功，并不表明业务处理结果。成功：T、失败：F)
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：RSA
out_trade_no	String	是	商户网站的唯一订单号，（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
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_return.htm

is_success:T
timestamp:20150119130901
sign:5195f9b9116e4adf67eeebc9935d33dc683f677d
sign_method:RSA
out_trade_no:2016062115020100000001
out_channel_trade_no:2016062115020112903920
trade_no:2016062115020100000002
trade_status:TRADE_FINISHED
total_amount:20000
out_channel:alipay
remark:donate
```

- 注意:
1. 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；
  2. 买家在支付成功后会看到一个易支付提示交易成功的页面，该页面会停留几秒，然后会自动跳转回商户指定的同步通知页面（参数 return\_url），如果return\_url为空则不跳转。
  3. 该方式仅仅在买家付款完成以后进行自动跳转，因此只会进行一次。

## 2. 设置页面跳转同步通知页面（return\_url）的路径时，不要在页面文件的后面再加上自定义参数

### 2.3 易支付服务器异步通知参数说明

含义:

易支付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网站。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	商户网站的唯一订单号, (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:donate

- 注意：
  1. 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；
  2. 必须保证服务器异步通知页面（notify\_url）上无任何字符，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，不仅页面跳转同步通知页面会启用，而且服务器异步通知页面也会收到易支付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。

## 2.4 易支付Web查询订单

请求URL:

- `https://ip:port/epay/webgate/orderquery`

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	否	查询日期，日对账批量查询时使用

#### 请求内容示例:

```
URI: https://ip:port/epay/webgate/orderquery

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": "0",
  "retmsg": "查询成功",
  "data": null,
  "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": "donate",
      }
    ],
    "firstResult": 0,
    "firstPage": true,
    "lastPage": true,
    "nextPage": 1,
    "totalPage": 1,
  }
}
```



```
    "prePage": 1
  }
}
```

- 失败

```
{
  "retcode": "1",
  "retmsg": "查询失败"
```

- 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
tradenno: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&tradenno=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
```