
title: 一卡通v5二维码H5对接接入 date: 2019-10-10 tags:

1.1 文档说明

本文档用于描述了一卡通二维码H5对接接入，供第三方系统（前置和应用）对接参考。

1.2 约定

1. 传输编码统一为utf-8
2. HMAC加密算法为用户请求本系统采用的加密算法，`SIGN_ALGORITHMS ="HMAC-SHA1"`;
3. 具体签名生成参考后面的签名章节
4. retcode等于0表示成功，非0表示失败，失败具体信息查看retmsg

2.1 二维码H5对接

请求URL:

- `https://ip:port/epayapi/services/thirdconsume/app/qrcode`

请求方式/格式:

- GET

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
uid	String	是	学号
timestamp	String	是	时间戳格式为yyyyMMddhh24miss
nonce	String	是	随机数
ip	String	是	客户端ip地址
codetype	String	是	二维码类型，H5,O5
codeversion	String	是	二维码版本，2.0
sign	String	是	签名
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

请求内容示例:

```
URI: https://ip:port/epayapi/services/thirdconsume/app/qrcode?
partner_id=100001&uid=200001&timestamp=2019090910202019&nonce=abc123&ip=19
2.10.10.1&codetype=05&codeversion=2.0&sign_method=HMAC&sign=5195f9b9116e4a
df67eeebc9935d33dc683f677d
```

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
uid:20001
nonce:abc123
ip:192.10.10.10
codetype:05
codeversion:2.0
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:

```
codeversion=2.0&codetype=05&ip=192.10.10.10&nonce=abc123&partner_id=10000&
sign_method=HMAC&timestamp=20150119130901&uid=20001
```

****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。