

title: 允许脱机消费二维码设计 date: 2017-12-19
tags: x

- version : 1.0

接口描述

接口形式

接口约束

1. 传输编码统一为utf-8
2. retcode等于0表示成功，非0表示失败，失败具体信息查看retmsg

附录A-用户二维码定义

二维码生成规则

- 二维码原始信息串格式为 "学校代码：学号：totp:两位随机码"

```
459:200019201:33893932:11
```

- **totp规则**
- totp采用标准的算法，加密算法采用HMAC-SHA256，步长定为30s，返回长度定为8位，种子采用激活接口中返回的seed32，时钟需要进行偏移矫正，如果客户端始终和服务器始终有偏差，需要记录偏移量。每次计算totp时需要加入偏移量因素。
- **第一步：**
- 对原始信息串使用AEScfb192加密算法进行加密base64输出
- $encdata = \text{base64}(\text{AEScfb192}(\text{pkey}, \text{原始信息串}, \text{iv}))$;
- pkey为激活接口服务端返回的pkey,返回的值为公钥加密后的值，原始key需要用本地RSA私钥解密获得，RSA私钥为信息注册时客户端自己生成
- 算法为“AES/CFB/NoPadding”
- **第二步：**
- 对加密后的数据使用AES加密算法二次加密，最后进行base64输出
- $\text{paymentToken} = \text{base64}(\text{AEScfb192}(\text{rootkey}, \text{schoolcode} + ':' + \text{gid} + ':' + \text{feetype} + ':' + \text{balance} + ':' + \text{totp} + ':' + \text{sign} + ':' + \text{encdata}, \text{iv}))$

- schoolcode为学校代码6，不足6位的前补0
- 其中gid为激活接口返回的“系统分配唯一标识”
- rootkey为约定密钥串,iv为约定向量
- balance为账户余额单位为分
- 算法为“AES/CFB/NoPadding”
- sign签名算法见附录b
- totp为6位数字，seedkey为预定密钥串，步长为30s 有效期为前后3分钟

附录B-签名sign定义

- $sign = MD5 (schoolcode+'.'+gid+'.'+feetype+'.'+balance+'.'+totp +'{' + Kp+'})$
- kp为单用户的分散密钥，由系统的卡片根密钥kr，通过分散因子schoolcode+gid 进行分散获得，分散算法为cpu卡密钥3DES分散算法

附录C-手机端安全控制

- 1、手机进入付款二维码界面时首先要检查网络是否连接，连接则需要到后台更新余额、账户状态等信息，如果余额不足或账户状态异常，则不能生成付款二维码，提示异常
- 2、手机更新了余额、状态信息后需要记录最后更新时间，10分钟内刷新二维码可以不用持续更新
- 3、手机断网后，如果app记录的最后更新时间戳超过4个小时，则不能生成付款二维码，提示需要联网更新后才能使用

附录D-pos端安全控制

- 1、psam卡存储有系统根密钥kr，需要能通过分散算法分散出用户Kp
- 2、pos存储的流水需要通过kp计算出一个tac校验码，用以保证流水不能串改和伪造，tac的计算方法为 $Hmac(terminal_id+termdate+termtime+amount+schoolcode+gid,kp)$
- 3、pos读取二维码后使用rootkey和iv先进行解密，获得基本信息schoolcode,gid,feetype,balance,totp和sign，校验totp确认二维码的有效性，有效期为前后3分钟，pos机通过psam卡以及schoolcode+gid分散获得用户kp，通过kp重新计算sign进行比对，校验信息的合法性。