Subin优惠券二维码接口定义

# 数字签名

为了保证数据传输过程中的数据真实性和完整性，我们需要对数据进行数字签名，在接收签名数据之后进行签名校验。

数字签名有两个步骤，先按一定规则拼接要签名的原始串，再选择具体的算法和密钥计算出签名结果。

一般失败的结果不签名。

## 签名原始串

**无论是请求还是应答，签名原始串按以下方式组装成字符串：**

1、除sign字段外，所有**必填参数**按照字段名的ascii码从小到大排序后使用QueryString的格式（即key1=value1&key2=value2…）拼接而成，空值不传递，不参与签名组串。

2、所有参数是指通信过程中实际出现的所有非空参数.

3、签名原始串中，字段名和字段值都采用原始值，不进行URL Encode。

**举例：**

调用某个接口，接口有如下字段：system=0218, seller=fzd01, time=20160826100455, price=1000.00, id=6f8d452a6b3611e68b7786f30ca893d3, msg=

正确的签名原始串是：

id=6f8d452a6b3611e68b7786f30ca893d3&price=1000.00&seller=fzd01&system=0218&time=20160826100455

## 签名算法

目前暂只支持MD5签名

### MD5签名

MD5 是一种摘要生成算法，通过在签名原始串后加上商户通信密钥的内容，进行MD5运算，形成的摘要字符串即为签名结果。为了方便比较，签名结果统一转换为大写字符。

**注意：签名时将字符串转化成字节流时指定的编码字符集应与参数input\_charset一致。**

MD5签名计算公式：

sign = **Md5**(**原字符串&key=商户密钥). toUpperCase**

如：

签名原始串是：

id=6f8d452a6b3611e68b7786f30ca893d3&price=1000.00&seller=fzd01&system=0218&time=20160826100455

商户密钥是：8934e7d15453e97507ef794cf7b0519d

签名的结果为：

sign=md5(id=6f8d452a6b3611e68b7786f30ca893d3&price=1000.00&seller=fzd01&system=0218&time=20160826100455&key=8934e7d15453e97507ef794cf7b0519d)=DC50CD75F862926853E98270ED7977A7

# 2 二维码数据

http://www.subinwechat.com/p/ParkingShopReceiptAuthorize.html?system=system\_id&seller=seller\_id&time=sale\_time&price=sale\_price&id=guid&msg=XXXXX& sign=signature

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 解释 | 参数是否必须 | 参数值是否必须 |
| system | 车场ID(由西图系统分配) | 是 | 是 |
| seller | 商户ID（由西图平台分配） | 是 | 是 |
| time | 用户到商铺消费的时间，  格式yyyyMMddHHmmss | 是 | 是 |
| price | 用户到商铺消费的金额 | 是 | 是 |
| id | 二维码唯一ID，由32位字符组成的guid | 是 | 是 |
| msg | 扩展数据 | 是 | 否 |

样例：

<http://itooler.cn/p/ParkingShopReceiptAuthorize.html?id=6f8d452a6b3611e68b7786f30ca893d3&price=1000.00&seller=fzd01&system=0218&time=20160826100455&msg=&sign=DC50CD75F862926853E98270ED7977A7>

