# 扫码支付接入指引

1. 范围

本文档规定了扫码支付平台的报文接口，包括扫码下单、支付查询、支付通知接口的处理流程和异常处理流程、消息域说明、消息格式以及交易报文格式说明。

1. 报文结构及通讯安全
2. 2.1 通讯方式和通讯协议

**本平台交易报文的所有报文域以json的表单方式通过HTTPS POST方法提交，响应报文在HTTPS会话中同步返回。**

**请注意把http头文件中的Content-Type类型改成application/json**

1. 2.2 签名与验签要求

对于报文的签名处理机制如下：

首先，对报文中约定的数据元采用key=value的形式按照名称排序，然后以&作为连接符拼接成待签名串。其次，对待签名串使用MD5算法做摘要，将得到的摘要信息转成16进制字符串。

对于报文的验签处理机制如下：

首先，对报文中约定的数据元采用key=value的形式按照名称排序，去除sign (请求报文签名域)，然后以&作为连接符拼接成待签名串。其次，对待签名串使用MD5算法做摘要，将得到的摘要信息转成16进制字符串，与sign(请求报文签名域)对比，如一致则验签成功，反之失败。

1. 报文域说明

本部分明确各个报文元素的定义，名称参照互联网的规范，后续修改。

1. 3.1报文域的属性说明

在平台与各商户的报文中，各报文域的数据类型、长度属性及格式如下表所示：

1. 报文域数据类型、长度属性及格式含义表

| 字符 | 含义 |
| --- | --- |
| Ax | x字节定长的字母字符 |
| Ax..y | 长度为x-y字节的变长字母字符 |
| ANx | x字节定长的字母和/或数字字符 |
| ANx..y | 长度为x-y字节的变长字母和/或数字字符 |
| ANSx | x字节定长的字母、数字和/或特殊符号字符 |
| ANSx..y | 长度为x-y字节的变长字母、数字和/或特殊符号字符 |
| ASx | x字节定长的字母和/或特殊符号字符 |
| ASx..y | 长度为x-y字节的变长字母和/或特殊符号字符 |
| Nx | x字节定长的整型数值，若表示金额，则以分为单位 |
| Nx..y | 长度为x-y字节的整型数值，若表示金额，则以分为单位 |
| NSx | x字节定长的数字符和/或特殊字符 |
| NSx..y | 长度为x-y字节的数字字符和/或特殊字符 |
| Sx | x字节定长的特殊符号字符 |
| Sx..y | 长度为x-y字节的变长特殊符号字符 |
| ss | 秒 |
| DD | 日 |
| hh | 时 |
| MM | 月 |
| mm | 分 |
| YY | 年（2字节） |
| YYYY | 年（4字节） |
| VARx | 个数为x的复合数据元集，数据元内使用|分割，数据元之间使用逗号,分割 |

1. 3.2报文消息域说明

详见具体接口

1. 接口报文说明

4.1符号及域约定

1、**必输说明**：M-必须填写的域,C-某条件成立时必须填写的域。

2、**数据元格式说明**：A-字母，N-数字，S-其它字符，x-最小长度，y-最大长度，部分接口中已转为中文描述。

3、**对于报文的签名处理(sign域)**：

首先，对报文中约定的数据元采用key=value的形式按照名称排序，然后以&作为连接符,再拼接商户加密key（......&key=商户加密key）,最终拼接成待签名串。

其次，对待签名串使用MD5算法做摘要，将得到的摘要信息转成16进制字符串。

4.2扫码支付 1007

| 数据元名称 | 数据元标识 | 数据元格式 | 请求 | 响应 | 数据元取值说明 |
| --- | --- | --- | --- | --- | --- |
| 交易类型 | transType | N4 | M |  | 1007 |
| 机构号 | instCode | 任意(1,10) | M |  | 平台机构号 |
| 证件类型 | certType | 数字(1,2) | M |  | 目前只支持0-平台商户号 1-身份证 2-营业执照,9-其他  **固定送0** |
| 证件号码 | certId | 任意(8,20) | M |  | 平台商户号 |
| 金额 | transAmt | 数字(1,20) | M |  | 整数，以分为单位 |
| 支付类型 | payType | 数字(2) | M |  | 03-支付宝 04-微信 05-QQ钱包扫码 06-京东扫码 07-京东钱包 08-银联钱包 |
| 购物明细 | goodsDesc | 任意(1,1024) | M |  |  |
| 交易日期 | transDate | 日期(8,8) | M |  | yyyyMMdd |
| 订单号 | orderNo | 任意(1,20) | M |  | 商户号+订单号+商户日期唯一标示一笔交易 |
| 后台通知地址URL | backUrl | 任意(1,256) | M |  | 平台通知支付结果地址,支持交易中上送或预配置 |
| 签名 | sign | 任意32) | M |  | MD5签名 |
| 交易流水 | tranSerno | 任意(1,30) |  | C | 交易流水号 |
| 通讯应答码 | ret\_code | 任意(1,20) |  | M | 0000-成功，非0000-失败，失败原因看通讯描述。 |
| 通讯描述 | ret\_msg | 任意(1,1024) |  | M | **成功时返回二维码扫码地址**，失败时为失败原因 |

4.3支付结果通知 1020

| 数据元名称 | 数据元标识 | 数据元格式 | 请求 | 响应 | 数据元取值说明 |
| --- | --- | --- | --- | --- | --- |
| 交易金额 | transAmt | 数字(1,20) | M |  | 整数，以分为单位 |
| 交易日期 | transDate | 日期(8,8) | M |  | yyyyMMdd |
| 订单号 | orderNo | 任意(1,20) | M |  | 商户号+订单号+商户日期唯一标示一笔交易 |
| 订单状态 | orderStatus | 数字(1) | M |  | 0-待支付 1-支付成功 2-支付失败 其它-待确认 |
| 交易流水 | tranSerno | 任意(1,30) | M |  | 交易流水号 |
| 签名 | sign | 任意(1,1024) | C |  | 签名 |
| 通讯应答码 | ret\_code | 任意(1,20) | M | M | 0000-成功，非0000-失败，失败原因看通讯描述。 |
| 通讯描述 | ret\_msg | 任意(1,1024) | M | M | 通讯描述 |

**注：在用户确认支付成功后马上回发送通知，请在接收并处理后返回json：**

**{"ret\_msg":"交易成功","ret\_code":"0000"}**

**给平台以示通知成功。否则，平台会每隔1分钟继续发最多5次的通知。**

# 附录一 签名算法

签名生成的通用步骤如下：

第一步，设所有发送或者接收到的数据转为集合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，则不参与签名；

◆ 参数名区分大小写；

◆传送的sign参数不参与签名，将生成的签名与sign值作校验。

第二步，在stringA最后拼接上**&key=商户具体key值**，得到stringSignTemp字符串，并对stringSignTemp进行MD5运算，得到sign值。