**chinatelecom1**

**中国电信企业标准**

**2006/09/10**

**收银台Http接口和Web接入**

版本号：1.0

**天翼电子商务有限公司**

**2015年8月**

**版本历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **作者** | **参与者** | **日期** | **描述** |
| 1.0.1 | 王俊 |  | 2015/8/20 | 初始版本，接口编写。 |
| 1.0.2 | 王俊 |  | 2015/9/10 | 增加通用Http接口。 |
| 1.0.3 | 张鹏飞 |  | 2015/9/14 | 接口梳理，增加接口使用场景及字段批注 |
| 1.0.4 | 王俊 |  | 2015/9/15 | 按照会议讨论进行接口修改 |
| 1.0.5 | 王俊 |  | 2015/9/21 | 修改下单等接口 |
|  |  |  |  |  |

目录

[1. H5通用Http接口 3](#_Toc433833314)

[1.1 定义 3](#_Toc433833315)

[1.2 通信方式 3](#_Toc433833316)

[1.3 报文编码 4](#_Toc433833317)

[1.4 响应定义 4](#_Toc433833318)

[1.5 接口描述 4](#_Toc433833319)

[1.6 接口列表 5](#_Toc433833320)

[1.6.1 获取公钥接口 5](#_Toc433833321)

[1.6.2 登陆短信验证码下发接口 6](#_Toc433833322)

[1.6.3 短信验证码登陆接口 6](#_Toc433833323)

[2. 收银台Web接入 7](#_Toc433833324)

[2.1 含义 7](#_Toc433833325)

[2.2 请求参数说明 7](#_Toc433833326)

[2.3 请求示例 8](#_Toc433833327)

[2.4 MD5签名 9](#_Toc433833328)

[2.5 Web收银台请求地址 9](#_Toc433833329)

[3. 附录A 9](#_Toc433833330)

[3.1 资金源类型bankTypeKey 9](#_Toc433833331)

[3.2 资金源支持类型supportType 10](#_Toc433833332)

# aaH5通用Http接口

## 定义

外部系统接入收银台Http功能调用必须遵循的请求和响应参数。

## 通信方式

|  |  |  |
| --- | --- | --- |
| 请求参数名 | 描述 | 必填 |
| keyIndex | 公私钥索引，服务端用于检索私钥； | 必填 |
| encryKey | 客户端使用RSA对32位密钥进行加密，服务端使用keyIndex检索到RSA私钥对32位密钥进行解密； | 必填 |
| encryStr | 客户端使用AES对原串进行加密，服务端使用AES对加密串进行解密；  如请求“短信验证码下发”接口，组装数据为：{"accId":"18055177348","merId":"18055177348","orderAmt":"1","orderSeq":"123423"}，加密后是：  lAgzgBMFtryNPlGzViUTyuuT01wrnPzkMCPU4qRdl+WwCgR+8orY/7jIhKTPIzGay7m9tkbDxIb9jUX4/KcafE4Zs/m5XpHAfIwQnlXLWX3t/oMrbsQzrVkoQ6B7r5MR2pOfnTs1Gs+y2y2LDREDRRSh+tuiy5JGi6OuoUZazI8= | 必填 |
| interCode | 接口编码 | 必填 |
| sessionId | 会话ID | 必填 |
| channelSource | 收银台渠道来源，【ios、android】 | 必填 |
| channelVersion | 收银台渠道版本，【3.0、1.0...】 | 必填 |

目前支持json格式的HttpPost请求，请求参数json格式，如 请求“短信验证码下发”，组装数据为：{"accId":"18055177348","merId":"18055177348","orderAmt":"1","orderSeq":"123423"}

通过加密组装后，转成json字符串为：

{"keyIndex":"00","encryKey":"lAgzgBMFtryNPlGzViUTyuuT01wrnPzkMCPU4qRdl+WwCgR+8orY/7jIhKTPIzGay7m9tkbDxIb9jUX4/KcafE4Zs/m5XpHAfIwQnlXLWX3t/oMrbsQzrVkoQ6B7r5MR2pOfnTs1Gs+y2y2LDREDRRSh+tuiy5JGi6OuoUZazI8=","encryStr":"TM2B61bIkv13uzTSUVoRy2MryKgWMrT5AMJwtuYNhWq8hBB6SHXQ3mMBQhuEAS9CHjdO0m9hzff9SCY+WRMtNxIuc1swtx0zL9i0Ki92ik9PWP6R/jvl6QMp2utJ5ReQ","interCode":"INTER.ACCOUNT.001","sessionId":"IESDSDFWERDSFDSFDFDSFDSFDSF","channelSource":"ios","channelVersion":"1.01"}

## 报文编码

报文使用UTF-8编码。

## 响应定义

响应报文如：{"errorCode":"HTTP\_RESULT\_ERROR","errorMsg":"转换失败","result":"","success":false," sign":"JjOmJHL2tb657P/gfVcv32uJ4nSmpKLJzB2skfiF6JNOhXVuzeQzy9vz1/1Wpl3vIQmqG7dAa0PAeybF4RwFIMLbmTHUZby9SUCYg9p4OTcq3N9hcMHACvq6k/63lHV+dPeKf+T7/tOddAexMEcMAvIs39CB8l/vHgdYRCf6rQg="}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| success | 响应码 | boolean | 20 | M | true成功，false失败 |
| result | 响应类 | T |  | O | 见方法应答参数 |
| errorCode | 响应码描述 | String | 6 | O |  |
| errorMsg | 响应码描述 | String | 30 | O | errorCode不为空时存在 |
| sign | 签名串 | String |  | M | RSA签名，对响应字符串（不包含sign字段），如：{"errorCode":"HTTP\_RESULT\_ERROR","errorMsg":"转换失败","success":false}，是用RSA签名，请求方可以使用RSA公钥进行验签 |

## 接口描述

|  |  |
| --- | --- |
| 接口名称 | H5通用Http接口 |
| 接口地址(综测) | http://116.228.151.160:6001/h5-cashier/common/interface |
| 接口地址(生产) |  |
| 接口提供者 | 收银台H5 |
| 接口使用者 | 外部系统 |
| 接口类型 | HttpPost json |
| 应用场景 |  |
| 备注 | 接口超时时间：60秒 |

## 接口列表

|  |  |  |  |
| --- | --- | --- | --- |
| 接口编码 | 接口描述 | 详细参数 | token校验 |
| 系统接口 | | |  |
| INTER.SYSTEM.001 | 获取公钥接口（含超时） | [参见 5.2.1 章节](#_获取公钥接口) |  |
| 账号接口 | | |  |
| INTER.ACCOUNT.007 | 登陆短信验证码下发接口 | [参见 5.2.3 章节](#_用户校验并下发验证码接口) |  |
| INTER.ACCOUNT.002 | 短信验证码登陆接口 | [参见 5.2.4 章节](#_短信验证码校验接口_1) |  |

### 获取公钥接口

**使用场景：**

外部商户通过SDK或大厅调起收银台时，首先通过此接口获取公钥及会话信息。

**请求参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
|  |  |  |  |  |  |

**注：此接口不进行加密，内部无子参数，返回消息也不需要进行验签**

示例：

{

"keyIndex": "",

"encryKey": "",

"encryStr": "",

"interCode": "INTER.SYSTEM.001",

}

**应答参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| keyIndex | 公钥索引 | String | 3 | 不可空 |  |
| pubKey | 公钥 | String | 128 | 不可空 |  |
| sessionId | 会话 | String | 64 | 不可空 |  |
| aesRandomId | 加密随机数 | String | 32 | 不可空 | 供密码控件加密因子使用 |
| sign | 签名串 | String | 128 | 不可空 |  |

示例：

{

"result": {

"keyIndex": "72",

"pubKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKDaL+E6dQJsZLwOboYqZmHsFZtuBBtUIb2NSQlcHP6kUPG0bGS4Ld3GwFm78sXLEu/1l07Wh3yF/nolarnw5JYhu4PrXHYMFmbwV0CeE39mV39CEUDo/kwny2KIH3W5jUdxB42O/LUbBA6kjgRvjq5m2u8+1rItoFWz2mtn8pHwIDAQAB",

"sessionId":"ESDFDSFDSFDSFSDFDSFDSF",

"sign":"

},

"success": true

}

### 登陆短信验证码下发接口

**使用场景：**

登录界面，获取短信验证码时，调用此接口；

如果用户未注册，报错误反馈，errorCode是NOT\_EXISTS\_CUSTOMER，此时不下发。

**请求参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| merId | 签约商户号 | String | 32 | 必填 |  |
| orderSeq | 请求订单号 | String | 32 | 必填 |  |
| orderAmt | 订单金额 | String | 32 | 必填 |  |
| accId | 翼支付账户号 | String | 32 | 必填 |  |

**应答参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| result | ok或者验证失败描述 | String |  | 选填 |  |

例如：{"success":true,"result":"OK","errorCode":null,"errorMsg":null}

### 短信验证码登陆接口

**使用场景：**

登录界面，对获取的短信验证码进行校验,同时验证用户信息是否存在

校验短信验证码

**请求参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| merId | 签约商户号 | String | 32 | 必填 |  |
| orderSeq | 请求订单号 | String | 32 | 必填 |  |
| orderAmt | 订单金额 | String | 32 | 必填 |  |
| accId | 翼支付账户号 | String | 32 | 必填 |  |
| smsVerifyCode | 短信验证码 | String | 6 | 必填 |  |

**应答参数：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **长度** | **必填** | **备注** |
| productNo | 翼支付登陆账号 | String |  | 必填 |  |
| token | 登录Token | String |  | 必填 |  |
| keyIndex | RSA索引号 | String |  | 必填 |  |

# 收银台Web接入

## 含义

请求参数是商户在与翼支付进行数据交互时，提供给翼支付的请求数据，以便翼支付根据这些数据进一步处理。

## 请求参数说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 参数 | 参数说明 | 类型 | 长度 | 可空 |
| 基本参数 | | | | |
| SERVICE | 接口名称  mobile.securitypay.pay | String |  | 不可空 |
| MERCHANTID | 签约商户号 | String | 30 | 不可空 |
| MERCHANTPWD | 签约商户密码 | String | 6 | 不可空 |
| SUBMERCHANTID | 签约子商户号 | String | 30 | 可空 |
| BEFOREMERCHANTURL | 支付结果前台通知地址 | String | 128 | 不可空 |
| BACKMERCHANTURL | 支付结果后台通知地址 | String | 128 | 不可空 |
| SIGNTYPE | 签名方式：MD5、RSA、CA | String |  | 可空，暂用MD5 |
| SIGN | MAC签名，请参见“8 签名机制” | String |  | 不可空 |
| WAPCHANNEL | 接入渠道(交付助手:01,微信：02，易信：03) | String |  | 可空 |
| 业务参数 | | | | |
| ORDERSEQ | 订单号 | String | 64 | 不可空 |
| ORDERREQTRANSEQ | 流水号 | String | 64 | 不可空 |
| ORDERTIME | 订单请求时间格式yyyyMMddHHmmss | String | 14 | 不可空 |
| ORDERVALIDITYTIME | 订单有效时间 | String |  | 可空 |
| ORDERAMOUNT | 订单金额／积分扣减（单位：分，保留小数点后两位） | String | 12 | 不可空 |
| CURTYPE | 币种（默认填 RMB ） | String | 4 | 不可空 |
| PRODUCTID | 业务标识，默认值为：04（纯业务支付） | String | 4 | 不可空 |
| PRODUCTDESC | 产品描述，商品的标题/交易标题/订单标题/订单关键字等  该参数最长为128个汉子 | String | 128 | 不可空 |
| SUBJECT | 商品的标题 | String | 128 | 不可空 |
| PRODUCTAMOUNT | 产品金额 | String | 12 | 不可空 |
| ATTACHAMOUNT | 附加金额 单位0.01元 | String | 12 | 不可空 |
| ATTACH | 附加信息 | String | 128 | 可空 |
| DIVDETAILS | 分账明细，分账商户必填,格式见说明 | String | 256 | 可空 |
| ACCOUNTID | 翼支付账户号 | String | 11 | 可空 |
| CUSTOMERID | 用户手机号 | String | 128 | 不可空 |
| USERIP | 用户IP | String | 128 | 可空 |
| BUSITYPE | 业务类型，默认为“04” | String |  | 不可空 |
| SWTICHACC | 是否可切换用户 | String |  | 不可空 |
| 免登陆参数 | | | | |
| tid | 免登陆信息-手机号 | String | 128 | 可空 |
| key\_index | 免登陆信息-RSA公钥索引 | String | 128 | 可空 |
| key\_tid | 免登陆信息-token令牌 | String | 128 | 可空 |

注：上述免登陆参数中tid，key\_index，key\_tid是从通过 “短信验证码验证”接口获取，分别对应（productNo、keyIndex、token）

## 请求示例

MERCHANTID=03310101101078000&SUBMERCHANTID=&MERCHANTPWD=538419&ORDERSEQ=1446040125198&ORDERAMOUNT=0.01&ORDERTIME=20151028214845&ORDERVALIDITYTIME=20151028214845&PRODUCTDESC=测试商品描述&CUSTOMERID=18055177348&PRODUCTAMOUNT=0.01&ATTACHAMOUNT=0&CURTYPE=RMB&BEFOREMERCHANTURL=http://www.baidu.com&BACKMERCHANTURL=http://127.0.0.1:8040/wapBgNotice.action&ATTACH=&PRODUCTID=04&USERIP=192.168.11.130&DIVDETAILS=&ACCOUNTID=18055177348&BUSITYPE=04&ORDERREQTRANSEQ=144604012519800001&SERVICE=mobile.securitypay.pay&SIGNTYPE=MD5&SIGN=82843D2EC8326B1B17BED09603B33538&SUBJECT=测试商品0000001&ORDERAMOUNT=0.01&SWTICHACC=false&tid=18055177348&key\_index=46&key\_tid=KVlTDR1VY+9tGnydi30v9GQRlD1pSunVUnA/XbhV9RYrjjP7CVgw4QdpOBfDly7SSVJZiAKa/4mz6KQuGclWRRTC6INbBsW61SqMBJC3Lrq2AniY55bU3EFLEB9n7zOBp33oqBe8oE3m9nv/QX9iUxLYL+3Tx0WXwOXc9d5dlE4=

## MD5签名

**上述SIGN签名字段原字符串：**

SERVICE=mobile.securitypay.pay&MERCHANTID=03310101101078000&MERCHANTPWD=538419&SUBMERCHANTID=&BACKMERCHANTURL=http://127.0.0.1:8040/wapBgNotice.action&ORDERSEQ=1446040125198&ORDERREQTRANSEQ=144604012519800001&ORDERTIME=20151028214845&ORDERVALIDITYTIME=20151028214845&CURTYPE=RMB&ORDERAMOUNT=0.01&SUBJECT=测试商品0000001&PRODUCTID=04&PRODUCTDESC=测试商品描述&CUSTOMERID=18055177348&SWTICHACC=false&KEY=

**签名后：**

82843D2EC8326B1B17BED09603B33538

## Web收银台请求地址

对于2.3节的请求参数，同1.2节通行方式中加密方式一样，生成如下字符串：

http://116.228.151.160:6001/h5-cashier/gateway.pay?platform=wap\_3.0&encryStr=&keyIndex=67&encryKey=c85iUZ92VN/9YS8YlAl8YpWwwRr6SNSXwz8YE/iehhY8CwDmnowoyQhbCvIjABZ0zDC/bnEQenBNQWEQwzZgB8yHEWMN1ZJlI8mLuQx8+i/diShKXBAwYqlw0JaoIzYMpHSxrqOL1ksCXhehhlWkIhWtSIYaBBN9XH5Jh8HRQwc=

上述url即web免登陆字符串，同时可自动下单。如果有不明白的地方，请参照UnitTest.java单元测试。

## 同步通知参数说明

如果上面的“前台通知地址”BEFOREMERCHANTURL配置了 <http://127.0.0.1/test.html>

那么我们会在支付成功或者取消支付时，页面跳转至 http://127.0.0.1/test.html&resultCode=-1& result=支付成功& orderSeq=13002420032222&orderAmt=0.01

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **含义** | **类型** | **备注** |
| resultCode | 状态码 | String | -1 支付成功；  0 取消支付；  512 已受理；  其他 支付失败 |
| orderSeq | 订单号 | String |  |
| orderAmt | 订单金额 | String |  |
| result | 支付消息 | String |  |