快捷-有短信

接口文档

2016年7月

修订记录

| 版本 | 日期 | 修订人 | 说明 |
| --- | --- | --- | --- |
| 1.0 | **2016-7-20** | 朱恒 | 初稿 |
| 1.1 | **2017-8-24** | 朱恒 | 增加订单状态描述 |
| 2.0 | **2017-8-31** | 朱恒 | 针对敏感字段进行加密传输 |
| 2.2 | **2017-12-27** | 陈勇 | 改为新接口 |

目录

[1 引言 4](#_Toc502680814)

[1.1 文档概述 4](#_Toc502680815)

[2 通讯协议 4](#_Toc502680816)

[3 交易密钥 4](#_Toc502680817)

[3.1 签名说明 4](#_Toc502680818)

[3.2 原签名串 4](#_Toc502680819)

[3.3 签名算法 5](#_Toc502680820)

[3.4 数据加密 5](#_Toc502680821)

[4 补单机制 5](#_Toc502680822)

[5 接口定义 6](#_Toc502680823)

[5.1 快捷支付下单 6](#_Toc502680824)

[5.1.1 请求地址 6](#_Toc502680825)

[5.1.2 请求参数列表 6](#_Toc502680826)

[5.1.3 响应结果 6](#_Toc502680827)

[5.2 快捷支付提交 7](#_Toc502680828)

[5.2.1 请求地址 7](#_Toc502680829)

[5.2.2 请求参数列表 7](#_Toc502680830)

[5.2.3 响应结果 7](#_Toc502680831)

[5.3 异步通知 8](#_Toc502680832)

[5.3.1 通知参数 8](#_Toc502680833)

[5.3.2 应答数据 8](#_Toc502680834)

[5.4 订单查询 8](#_Toc502680835)

[5.4.1 请求地址 8](#_Toc502680836)

[5.4.2 请求参数列表 9](#_Toc502680837)

[5.4.3 响应结果 9](#_Toc502680838)

[5.5 业务流程 9](#_Toc502680839)

[6 注意事项 10](#_Toc502680840)

[7 附录 10](#_Toc502680841)

[7.1 银行列表 10](#_Toc502680842)

# 引言

## 文档概述

# 通讯协议

采用 HTTP 标准的 POST 协议，为了保证接收方数据的准确性，传输数据必须签名

# 交易密钥

交易密钥分为：传输密钥（加密密钥）、签名密钥。传输密钥使用AES对敏感字段进行加密，签名密钥使用MD5对组装后的报文进行签名。

来源注册商户返回：传输加密的密钥：dataKey，签名密钥：secretKey

## 签名说明

1、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

## 原签名串

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、签名原始串中，字段名和字段值都采用原始值，不进行任何加密操作（先签名后加密）

3、返回的应答或通知消息可能会由于升级增加参数，请验证应答签名时注意允许这种情况。

## 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 charset 一致。

MD5 签名计算公式：

sign = Md5(原字符串&key= 签名密钥).toUpperCase

## 数据加密

在提交数据之前，需要把报文规范中传输需加密的字段使用传输密钥进行加密，并替换掉报文中的明文再提交。数据加解密算法如下：



如果不使用文档提供的AES加密工具类，加密注意事项如下：

加密密钥：使用系统提供的加密密钥的前16位做为密钥

字符集：UTF-8

算法：AES/ECB/PKCS5PADDING

加密结果：转换为16进制的大写字符串

# 补单机制

注意：对后台通知交互模式，如果系统收到商户的应答不是“SUCCESS”或超时，系统认为通知失败，系统会通过一定的策略定期重新发起通知，尽可能提高通知的成功率，但系统不保证通知最终能成功。

由于存在重新发送后台通知的情况，因此同样的通知可能会多次发送给商户系统。商户系统必须能够正确处理重复的通知。推荐的做法是，当收到通知进行处理时，首先检查对应业务数据的状态，判断该通知是否已经处理过，如果没有处理过再进行处理，如果处理过直接返回“SUCCESS”。在对业务数据进行状态检查和处理之前，要采用数据锁进行并发控制，以避免数重入造成的数据混乱。

# 接口定义

## 快捷支付下单

发起快捷支付时调用此接口，银行会发送动态验证码到持卡人手机，若持卡人未收到短信验证码，需要重新下单

### 请求地址

|  |  |
| --- | --- |
| **请求URL** | /gate/epay/epapply |

### 请求参数列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 商户号 | mch\_id | 是 | String(32) | 由系统分配的商户号 |
| 商户订单号 | out\_trade\_no | 是 | String(32) | 商户订单号，确保唯一 |
| 总金额 | total\_fee | 是 | String(12) | 订单总金额，单位为分 |
| 商品名称 | body | 是 | Stirng(500) | 商品名称 |
| 通知地址 | notify\_url | 是 | String | 快捷支付提交成功后回调的通知地址：务必确保外网可以访问 |
| 卡类型 | card\_type | 是 | String | DEBIT-借记卡  CREDIT-贷记卡 |
| 银行编码 | bank\_code | 是 | String | 银行编码[银行列表](#_银行列表) |
| 开户行名称 | bank\_name | 是 | String | 银行卡所在支行名称 |
| 持卡人名称 | card\_name | 是 | String | 持卡人姓名, 传输需加密 |
| 卡号 | card\_no | 是 | String | 卡号, 传输需加密 |
| 证件类型 | id\_type | 是 | Strting | ID\_CARD 身份证 |
| 证件号码 | id\_no | 是 | String | 证件号码，传输需加密 |
| 预留手机号 | bank\_mobile | 是 | String | 银行预留手机号, 传输需加密 |
| 信用卡有效期 | card\_valid\_date | 否 | String | 当卡类型为：CREDIT 必填, 传输需加密 |
| CVV | cvv2 | 否 | String | 当卡类型为：CREDIT 必填, 传输需加密 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

### 响应结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 受理标识 | status | 是 | String(20) | SUCCESS 受理成功  FAIL 受理失败 |
| 错误代码 | code | 否 | String(20) | 受理失败时返回 |
| 错误描述 | message | 否 | String(200) | 受理失败时返回 |
| 以下字段在 status 为 SUCCESS 的时候有返回 | | | | |
| 系统订单号 | ch\_trade\_no | 是 | String(32) | 系统订单号 |
| 下单状态 | trade\_state | 是 | String(20) | NOTPAY 下单成功  FAIL 下单失败 |
| 状态码 | err\_code | 是 | String(20) | 下单状态对应响应码 |
| 状态说明 | err\_msg | 是 | String(200) | 下单状态对应响应码描述 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

## 快捷支付提交

用户输入银行验证码后，发送支付提交请求，完成快捷支付

### 请求地址

|  |  |
| --- | --- |
| **请求URL** | /gate/epay/epsubmit |

### 请求参数列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 商户号 | mch\_id | 是 | String(32) | 由系统分配的商户号 |
| 商户订单号 | out\_trade\_no | 是 | String(32) | 商户订单号 |
| 动态口令 | password | 是 | String | 银行发送的动态口令 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

### 响应结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 受理标识 | status | 是 | String(20) | SUCCESS 受理成功  FAIL 受理失败 |
| 错误代码 | code | 否 | String(20) | 受理失败时返回 |
| 错误描述 | message | 否 | String(200) | 受理失败时返回 |
| 以下字段在 status 为 SUCCESS 的时候有返回 | | | | |
| 系统订单号 | ch\_trade\_no | 是 | String(32) | 系统订单号 |
| 订单状态 | trade\_state | 是 | String(20) | SUCCESS 成功  FAIL 失败  PROCESSING 处理中 |
| 状态码 | err\_code | 是 | String(20) | 订单状态对应响应码 |
| 状态说明 | err\_msg | 是 | String(200) | 订单状态对应响应码描述 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

## 异步通知

用户快捷支付成功以后，系统会自动推送异步通知结果至下单时提交的notify\_url地址，异步通知可能会重复发送，接入方需要做好防重处理。

### 通知参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 服务商号 | sp\_id | 是 | String(32) | 系统分配的服务商号 |
| 商户号 | mch\_id | 是 | String(32) | 系统分配的商户号 |
| 商户订单号 | out\_trade\_no | 是 | String(32) | 商户订单号 |
| 系统订单号 | trade\_no | 是 | String(32) | 系统订单号 |
| 订单状态 | trade\_state | 是 | String(32) | SUCCESS 成功 |
| 订单金额 | total\_fee | 是 | String(32) | 订单金额，单位分 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

### 应答数据

|  |  |
| --- | --- |
| **应答内容** | **说明** |
| SUCCESS | 成功，返回其它为失败，系统会继续发起通知请求 |

注意：系统只认大写SUCCESS为通知成功，不能带有其它任何字符，否则全部认为通知失败，后续会重新发起通知，总计通知次数为6次，达到上限6次以后，系统将不再发起通知

## 订单查询

通过此接口查询订单的交易状态及清算状态

### 请求地址

|  |  |
| --- | --- |
| **请求URL** | /gate/spsvr/order/qry |

### 请求参数列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 商户号 | mch\_id | 是 | String(32) | 系统分配的商户号 |
| 商户订单号 | out\_trade\_no | 是 | String(32) | 商户内部的订单号 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

### 响应结果

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 受理标识 | status | 是 | String(20) | SUCCESS 受理成功，  FAIL 受理失败 |
| 错误代码 | code | 否 | String(20) | 受理失败时返回 |
| 错误描述 | message | 否 | String(200) | 受理失败时返回 |
| 以下字段在 status 为 SUCCESS 的时候有返回 | | | | |
| 系统订单号 | ch\_trade\_no | 是 | String(32) | 系统订单号 |
| 订单状态 | trade\_state | 是 | String(32) | SUCCESS 成功  FAIL 失败  PROCESSING 处理中  NOTPAY 未支付  CLOSED 已关闭 |
| 状态码 | err\_code | 是 | String(20) | 订单状态对应响应码 |
| 状态说明 | err\_msg | 是 | String(200) | 订单状态对应响应码描述 |
| 结算状态 | settle\_state | 否 | String(20) | 订单状态为成功时返回  SUCCESS 结算成功  FAIL 结算失败  PROCESSING 正在结算  NOTPAY 未结算 |
| 结算状态说明 | settle\_state\_desc | 否 | String(200) | 订单状态为成功时返回 |
| 随机字符串 | nonce\_str | 是 | String(32) | 随机字符串，不长于 32 位 |
| 签名 | sign | 是 | String(32) | MD5 签名结果，详见“签名说明” |

## 业务流程

1. 第一步：调快捷支付下单接口，并发送验证码给持卡人
2. 第二部：调快捷支付提交接口，完成支付，注：1，2两步的商户订单号要一致
3. 第三部：提交订单后系统会发通知给商户

# 注意事项

1、所有涉及到金额的单位都是分，最小的单位是 1 分，不能有小数出现

2、 notify\_url是系统服务器从后台直接发起请求到商户服务器， 商户处理时不能检查用户的cookie或session；

商户更新 DB 等发货流程需要在 notify\_url 完成后，以确保掉单时，系统补单能成功补上

3、 notify\_url 有可能重复通知，商户需要做去重处理，避免多次发货

4、 notify\_url 收到的通知，商户处理成功或检查订单已经处理，需要返回处理成功的标志“SUCCESS”，以告知系统不再通知

5、 其它注意事项

（1） 参数大小写问题

请留意文档中要求的字符大小写问题， 如 “md5 运算后， 字符串的字符要转换为大写” 。

（4） 同一商户订单号支付问题

商户的 out\_trade\_no 必须全局唯一，调试和生产环境，都需要使用唯一的订单号。注意：当商户的同一个商户号绑定了多种支付方式也需要加标识来区分，不能出现重复。商户平台自己保证同一笔订单重复支付的情况

（5）测试环境是虚拟交易

测试环境交易时：银行卡号最后一位：1成功，2：失败，其他处理中，验证码默认：123456

# 附录

## 银行列表

|  |  |  |
| --- | --- | --- |
| 银行编码 | 银行名称 | 备注 |
| 01020000 | 工商银行 | 工商银行 |
| 03080000 | 招商银行 | 招商银行 |
| 03010000 | 交通银行 | 交通银行 |
| 01040000 | 中国银行 | 中国银行 |
| 03030000 | 光大银行 | 光大银行 |
| 03050000 | 民生银行 | 民生银行 |
| 03090000 | 兴业银行 | 兴业银行 |
| 03020000 | 中信银行 | 中信银行 |
| 03060000 | 广发银行 | 广发银行 |
| 03100000 | 浦发银行 | 浦发银行 |
| 03070000 | 平安银行 | 平安银行 |
| 04083320 | 宁波银行 | 宁波银行 |
| 03200000 | 东亚银行 | 东亚银行 |
| 01000000 | 中国邮储银行 | 中国邮储银行 |
| 04243010 | 南京银行 | 南京银行 |
| 65012900 | 上海农商银行 | 上海农商银行 |
| 04031000 | 北京银行 | 北京银行 |
| 01030000 | 农业银行 | 农业银行 |
| 03040000 | 华夏银行 | 华夏银行 |