提现

接口文档

2016年12月

修订记录

| 版本 | 日期 | 修订人 | 说明 |
| --- | --- | --- | --- |
| 1.0 | **2016-12-20** | 朱恒 | 建立初稿 |
| 1.1 | **2017-03-21** | 朱恒 | 提现请求接口指定收款账户相关的字段.  提现接口中为否的字段若不填写，则默认提现至商户的默认结算账户  如果不明白联调时请与技术沟通 |
| 2.0 | **2017-08-31** | 朱恒 | 针对敏感字段进行加密传输 |
| 2.2 | **2017-12-28** | 陈勇 | 改为新接口 |

目录

[1 引言 4](#_Toc502681755)

[1.1 文档概述 4](#_Toc502681756)

[2 通讯协议 4](#_Toc502681757)

[3 数据格式 4](#_Toc502681758)

[4 交易密钥 4](#_Toc502681759)

[4.1 签名说明 4](#_Toc502681760)

[4.2 原签名串 4](#_Toc502681761)

[4.3 签名算法 5](#_Toc502681762)

[4.4 数据加密 5](#_Toc502681763)

[5 接口定义 6](#_Toc502681764)

[5.1 余额提现 6](#_Toc502681765)

[5.1.1 请求地址 6](#_Toc502681766)

[5.1.2 请求参数列表 6](#_Toc502681767)

[5.1.3 响应结果 6](#_Toc502681768)

[5.2 订单查询 7](#_Toc502681769)

[5.2.1 请求地址 7](#_Toc502681770)

[5.2.2 请求参数列表 7](#_Toc502681771)

[5.2.3 响应结果 7](#_Toc502681772)

[5.3 余额查询 8](#_Toc502681773)

[5.3.1 请求地址 8](#_Toc502681774)

[5.3.2 请求参数列表 8](#_Toc502681775)

[5.3.3 响应结果 8](#_Toc502681776)

[6 注意事项 8](#_Toc502681777)

# 引言

## 文档概述

供内部开发人员和外部机构接入技术人员使用

# 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

# 数据格式

请求格式：请求数据以请求Http请求参数以x-www-form-urlencode的形式传递

响应格式：响应数据以Json格式返回

通知格式：通知接口以Json格式返回

# 交易密钥

交易密钥分为：传输密钥、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。

## 签名说明

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

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

# 接口定义

## 余额提现

### 请求地址

|  |  |
| --- | --- |
| **请求URL** | /gate/rtp/distillpay |

### 请求参数列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名称** | **字段名** | **是否必填** | **类型** | **说明** |
| 服务商号(机构号) | 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，32个字符内，确保唯一 |
| 提现描述 | body | 是 | String(100) | 提现描述 |
| 总金额 | total\_fee | 是 | String | 订单金额，以分为单位，不允许包含任何字符或小数点 |
| 账户类型 | settle\_acc\_type | 是 | String | PERSONNEL：对私  CORPORATE：对公 |
| 银行名称 | bank\_name | 是 | String | 收款账户的银行名称 |
| 联行号 | bank\_no | 是 | String | 12位的联行号， |
| 账户名称 | card\_name | 是 | String | 收款账户名称，传输需加密 |
| 账户号 | card\_no | 是 | String | 收款账户号，传输需加密 |
| 证件类型 | id\_type | 否 | String | ID\_CARD：身份证，对私必填 |
| 证件号码 | id\_no | 否 | String | 身份证号码，对私必填，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** |
| 返回状态码 | status | 是 | String(16) | SUCCESS 受理成功，FAIL 受理失败 |
| 错误码 | code | 否 | String(32) | 受理失败时返回 |
| 错误消息 | message | 否 | String(128) | 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 | 系统订单号 |
| 订单状态 | trade\_state | 是 | String | SUCCESS 成功  FAIL 失败  PROCESSING 处理中 |
| 状态码 | err\_code | 是 | String | 状态码 |
| 状态说明 | err\_msg | 是 | String | 状态说明 |
| 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” |

## 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 | | | | |
| 服务商订单号 | out\_trade\_no | 是 | String(32) | 服务商订单号 |
| 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 |
| 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” |

## 余额查询

### 请求地址

|  |  |
| --- | --- |
| **请求URL** | /gate/rtp/balance/qry |

### 请求参数列表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |
| 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** |
| 返回状态码 | status | 是 | String(16) | SUCCESS 表示成功，FAIL 表示失败 |
| 返回信息 | message | 否 | String(128) | 返回信息，如非空，为错误原因 |
| 以下字段在 status 为 SUCCESS 的时候有返回 | | | | |
| 账户余额 | total\_fee | 是 | Int | 账户余额 |
| 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” |

# 注意事项

1、代收请求不同银行返回的代收响应有实时和非实时之分，如果接口返回的订单状态为PROCESSING，则需要商户端调用代收结果查询接口来查询代收订单的最终端状态，对于PROCESSING状态的订单银行反馈一般2小时内会有明确的答复。

2、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

3、 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