支付服务平台

支付接口

[V1.1]

2018年04月

目录

1. 文档简介

1.1. 文档概述

本开发手册对支付产品进行详细描述，通过该文档可以对本系统有全面的了解，使商户技术人员尽快掌握本系统的接口，并能够与本系统上进行对接。

1.2. 阅读对象

支付商户的技术人员及维护人员。

2. 商户密钥

2.1. 加密算法

请求使用到了 MD5 加密算法，主要是为了防止中途被篡改数据。(下单或查询)

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）；
- ◆ 如果参数的值为空不参与签名；
- ◆ 参数名区分大小写；
- ◆ 验证调用返回或主动通知签名时，传送的 sign 参数不参与签名，将生成的签名与该 sign 值作校验。

第二步，在 stringA 最后拼接上 key 得到 stringSignTemp 字符串，并对 stringSignTemp 进行 MD5 运算，再将得到的字符串所有字符转换为大写，得到 sign 值 signValue。

举例：

假设传送的参数如下：

mch_id： 10000000

subject： 商品名称

detail: 详细描述

nonce： wmg9sL00qFEPdk6M

第一步：对参数按照 key=value 的格式，并按照参数名 ASCII 字典序排序如下：

stringA="detail=详细描述&mch_id=10000000&nonce=wmg9sL00qFEPdk6M&subject=商品名称";

第二步：拼接 API 密钥：

stringSignTemp=stringA+"&key=sWlINU9hyWZvdcDZPnyIhVCRdmgRDqmw" // 注：key 为商户平台设置的接口密钥 api_key

sign=MD5(stringSignTemp).toUpperCase()="D0F7DBB5574FB2C64AE5ABCA66950A3D" //注：MD5 签名方式

sign=hash_hmac("sha256",stringSignTemp,key).toUpperCase()="D+bTXco2gUquvKIjxWNqEIgLgIlOSkyZApubJb+1Bp8=" // 注：HMAC-SHA256 签名方式

请求响应、异步通知使用RSA2 验证签名:

RSA 验签明文拼接字符串stringA 的 MD5 值 // 注：算法 SHA256WithRSA , *MD5 值为小写*，请使用平台 RSA 公钥进行签名校验(PHP 版本需要 5.5 以上)

举例：

响应内容如下：

{"pay_url":"HTTPS://QR.ALIPAY.COM/FKX09161NK1RJUSZQBAU98?t=1531223954449","mch_id":1525399982,"nonce":"72c73310646147d2ba385eee40e7e729","trade_type":"ALIH5","sign":"RsMUdHkkzVnmuAmBdCJk5S+zWihqD48Ggfmg+mLGdFLTCVaouCX+/7j7v/qLFw6w7WVAvhT5LIYnpntQtie25bptJcCQoRjSaDYapmq08f5JbPRVuq4nooXiH6J4rL9Bk+2sPNuiqy7Uhk7cq4z78NrbLZI4ZA1JnHbnvlf0cE0Va7Myb7ZMhxBB+g4KOt/PQIxUXOsvyKPeCPsAUGTY5K5EmPr/ztsgJg2kqOGdxm1ZZbi9VZ5qzbx0O9wccQ8MHCTv7KcG1h3/dch9bmKWXxKJYZL+nGGMQkJTq1zJ6XNjGu1REr1YIk1obgaQVlzfZEU2qw5yANJAXyxbxV3rzA=="}

第一步拼接字符串：

StringA = mch_id=1525399982&nonce=72c73310646147d2ba385eee40e7e729&pay_url=HTTPS://QR.ALIPAY.COM/FKX09161NK1RJUSZQBAU98?t=1531223954449&trade_type=ALIH5

第二步：MD5 加密

plaintext = MD5(StringA) = dc4da653b2c751852bfa71a1e0878d3c

第三步：RSA2 验签

RSA2.verify(plaintext , sign, publickKey)

2.2. 密钥详解

mch_id：商户号，随机生成
api_key：API 密钥，随机生成
rsa_public_key：平台 RSA 公钥，用于校验签名

2.3. 举例

3. 接口详述

3.1 支付下单

请求

生产地址	https://接口域名/pay/unifiedorder				
接口技术	HTTP/HTTPS				
传输格式	**HTTP POST JSON**				
名 称	**字段名称**	**数据类型**	**必填**	**示例值**	**字段描述**
商户号	mch_id	String(32)	是	1234567890	平台分配的商户号
交易类型	trade_type	String(10)	是	ALIH5	详见附录支付类型
随机字符串	nonce	String(32)	是	7VS264I5K850 2SI8ZNMTM6L TKCH16CQ2	随机字符串，不长于 32 位
用户 ID	user_id	String(32)	否		商户端的用户 ID
时间戳	timestamp	String(32)	是	1524822584	UNIX 时间戳
订单名称	subject	String(200)	是		商品标题/交易标题/订单标题
商品详情	detail	String(500)	否		商品详情

商户订单号	out_trade_no	String(32)	是	20150806125346	商户系统内部的订单号，32个字符内
总金额	total_fee	Int	是	8	订单总金额，单位为分
终端 IP	spbill_create_ip	String(32)	是	123.12.12.123	
过期时长	timeout	String(32)	否		
异步地址	notify_url	String(100)	是		异步通知地址
返回地址	return_url	String(100)	否		**保留参数**
签名类型	sign_type	String(32)	否	MD5	签名类型，目前支持 MD5，默认为 MD5
签名信息	sign	String(32)	是	D0F7DBB5574FB2C64AE5ABCA66950A3D	**签名，详见签名生成算法**

响应

名 称	字段名称	数据类型	必填	示例值	字段描述
商户号	mch_id	String(32)	是	1234567890	平台分配的商户号
交易类型	trade_type	String(10)	是	ALIH5	详见附录支付类型
随机字符串	nonce	String(32)	是	7VS264I5K8502SI8ZNMTM6LTKCH16CQ2	随机字符串，不长于 32 位
支付地址	pay_url	String(100)	是		支付地址
签名信息	sign	String(32)	是	D0F7DBB5574FB2C64AE5ABCA66950A3D	**签名，详见 RSA 签名生成算法**

3.2 支付异步通知

接口技术	HTTP/HTTPS				
传输格式	HTTP POST FORM 表单				
名 称	**字段名称**	**数据类型**	**必填**	**示例值**	**字段描述**
业务结果	result_code	String(16)	是	SUCCESS	SUCCESS/FAIL
商户号	mch_id	String(32)	是	1234567890	平台分配的商户号
交易类型	trade_type	String(10)	是	ALIH5	详见附录支付类型
随机字符串	nonce	String(32)	是	7VS264I5K8502SI8ZNMTM6LTKCH16CQ2	随机字符串，不长于 32 位
时间戳	timestamp	String(32)	是	1524822584	UNIX 时间戳
商户订单号	out_trade_no	String(32)	是	20150806125346	商户系统内部的订单号，32 个字符内
总金额	total_fee	Int	是	8	订单总金额，单位为分
交易流水号	trade_no	String(32)	是		交易流水号
平台交易单号	platform_trade_no	String(32)	是		平台交易单号
支付时间	pay_time	String(14)			订单支付时间，格式为 yyyyMMddHHmmss，如 2009 年 12 月 25 日 9 点 10 分 10 秒表示为 20091225091010。

签名信息	sign	String	是		**签名，详见 RSA 签名校验算法**

商户端异步响应：返回字符串 SUCCESS

3.3 支付查询

请求

生产地址	https://接口域名/pay/query				
接口技术	HTTP/HTTPS				
传输格式	HTTP POST JSON				
名 称	**字段名称**	**数据类型**	**必填**	**示例值**	**字段描述**
商户号	mch_id	String(32)	是	1234567890	平台分配的商户号
随机字符串	nonce	String(32)	是	7VS264I5K8502SI8ZNMTM6LTKCH16CQ2	随机字符串，不长于 32 位
商户订单号	out_trade_no	String(32)	二选一	20150806125346	商户系统内部的订单号，32 个字符内
平台交易单号	platform_trade_no	String(32)			平台交易单号()
签名类型	sign_type	String(32)	否	MD5	签名类型，目前支持 MD5，默认为 MD5
签名信息	sign	String(	是		**签名，详见 RSA 签名校验算法**

响应

接口技术	HTTP/HTTPS				
格式	JSON				
名 称	**字段名称**	**数据类型**	**必填**	**示例值**	**字段描述**
业务结果	result_code	String(16)	是	SUCCESS	SUCCESS/FAIL
商户号	mch_id	String(32)	是	1234567890	平台分配的商户号
交易类型	trade_type	String(10)	是	ALIH5	详见附录支付类型
随机字符串	nonce	String(32)	是	7VS264I5K8502SI8ZNMTM6LTKCH16CQ2	随机字符串，不长于 32 位
时间戳	timestamp	String(32)	是	1524822584	UNIX 时间戳
商户订单号	out_trade_no	String(32)	是	20150806125346	商户系统内部的订单号，32 个字符内
总金额	total_fee	Int	是	8	订单总金额，单位为分
交易流水号	trade_no	String(32)	是		交易流水号
平台交易单号	platform_trade_no	String(32)	是		平台交易单号
支付时间	pay_time	String(14)	是		订单支付时间，格式为 yyyyMMddHHmmss，如 2009 年 12 月 25 日 9 点 10 分 10 秒表示为 20091225091010。
签名信息	sign	String(32)	是	D0F7DBB5574FB2C64AE5ABCA66950A3D	**签名，详见 RSA 签名生成算法**

附录

支持支付类型

GATEWAY 网关支付

QUICK 快捷支付

ALISCAN 支付宝扫码支付

ALIH5 支付宝 H5 支付

QQSCAN QQ 扫码支付

WXSCAN 微信扫码支付

ALIH5 支付宝 H5 支付

QQH5 QQH5 支付

UPSCAN 银联扫码支付