品而数据科技有限公司

品而信用支付接口开发包

1.0

2015/09/14

1 文档说明

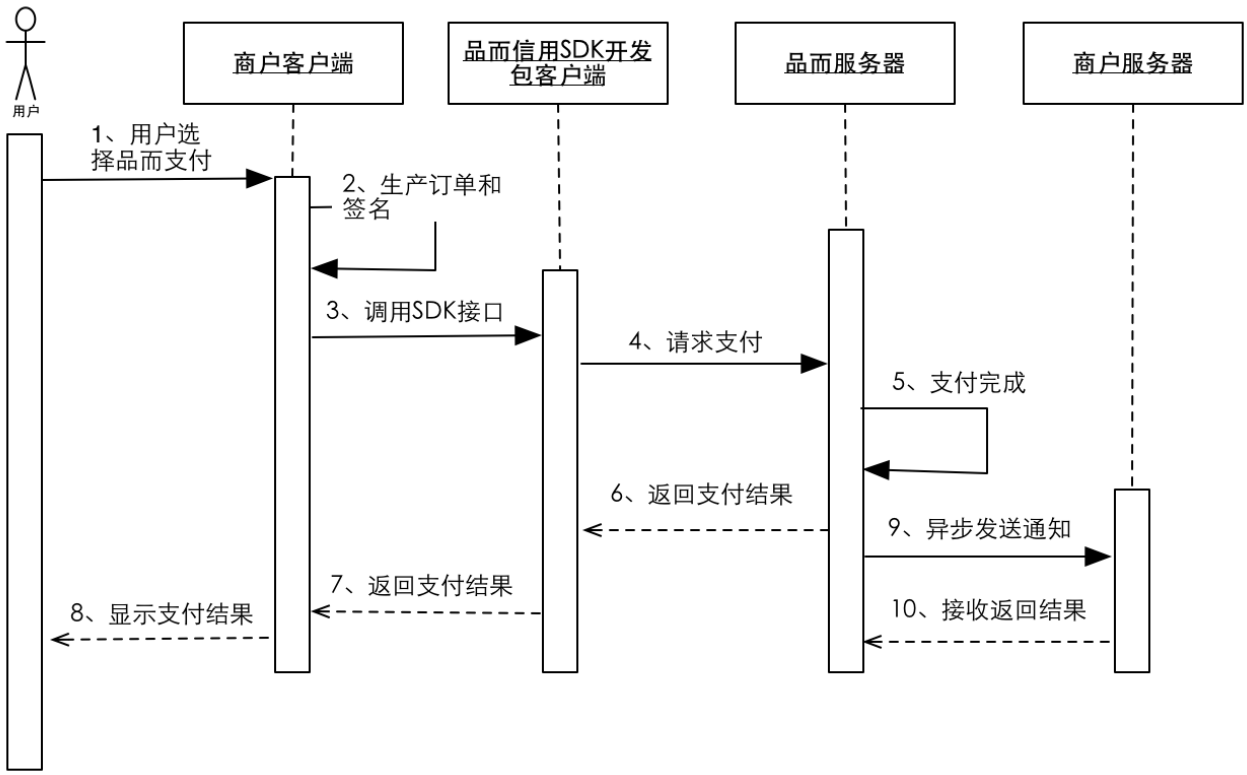
1.1 功能描述

本文主要描述开发包支付接口的使用方法,供合作伙伴的开 发者接入使用。

1.2 阅读对象

本文档面向具有一定 iOS 客户端开发能力,了解 iOS 客户端的开发和管理人员。

2 品而支付数据交互



2.1 品而支付 SDK 支付时序图

2.1 品而支付 SDK 数据交互

1) 用户选择品而支付

用户选择支付时选择用品而支付

2) 商户生产订单和签名

商户客户端根据 SDK 开发包的接口规则，通过程序生成得到签名结果及要传输给品而 SDK 开发包的数据集合。

3) 商户调用 SDK 接口发送请求

商户客户端把构造好的数据集合传给 SDK。

4) SDK 调用品而支付服务

SDK 内部调用品而支付服务器 API 将请求数据发送给品而服务器。

5) 品而支付服务返回支付结果给 SDK

品而支付服务器对请求数据进行安全校验，一系列校验通过之后生产支付结果数据包。

6) SDK 收到支付结果

品而支付服务器将支付结果数据返回给 SDK。

7) SDK 返回支付结果给商户

SDK 收到品而返回数据集合后，将支
付结果返回给商户。
8) 用户显示支付完成

商户处理收到支付完成的信息。

9) 品而服务器发送异步回调给商户服务器

品而服务器在支付完成之后，主动调用商户支付请求时配置的回调 URL，通知商户支付结果。

10) 品而服务器接收商户服务器相应

品而服务器，等待商户服务器返回结果。

2.1 品而支付 SDK 参数

请求参数

字段说明	字段名	是否必须	类型	描述
基本请求参数				
商户号	merchant_id	是	String	商户编号是商户在品而的唯一标识
商户秘钥索引	api_id	是	String	品而分配给商家的秘钥的索引，秘钥在商家和品而签约时由品而分配给商家
字符集	charset	是	String	商户发起交易的参数的编码集
画面回跳地址	return_url	否	String	品而支付完成后，回跳到画面的 URL
签名算法	sign_type	是	String	RSA 或者 MD5，目前只支持 RSA
签名	sign	是	String	加密签名串：除 sign，sign_type 外的所有参数按签名算法生成的签名串，不包含空参数，见安全签名机制
订单信息				
商户端订单号	order_id	是	String	交易订单号
交易金额	amount	是	String	交易金额，精确到小数点后两位
订单详情	order_detail	是	String	订单详情，是一个 JSON 的字符串

返回参数

字段说明	字段名	是否必须	类型	描述
基本参数				
商户端订单号	order_id	是	String	商户端唯一订单号
交易流水号	transaction_id	是	String	品而内部的交易流水号
签名算法	sign_type	是	String	RSA 或者 MD5，目前只支持 RSA
签名	sign	是	String	加密签名串：除 sign 外的所有参数按签名算法生成的签名串，不包含空参数，见安全签名机制，采用 RSA 签名机制

返回参数中包含的字段可由商户配置，在商户和品而签约时确定。

2.2 品而支付 SDK 参数

商户号（merchant_id）

商户秘钥索引（api_id）

字符集（charset）

画面回跳地址（return_url）

签名算法（sign_type）

签名（sign）

商户订单号（order_id，若商家无订单系统，则不需要该参数）

交易金额（amount）

订单详情（order_detail）

3 品而支付异步回调

若商家有自己的订单系统且品而支付成功，品而会异步回调商家的 API，对于该 API 的说明如下：

1、该 API 回调是 POST 方法

2、该 API 的参数商户可定制，默认是订单号（order_id）和交易流水号（transaction_id），通过 HTTP 请求的 BODY 传送。

3、该 API 的响应是 JSON 格式，且含有“code”：“XXX”键值对。若 code 的值是 200.表明商户服务器已正常处理。例如：

```
{
"code": "200"
}
```

4.如果响应不含有“code”或者其值不是 200，品而的服务器会重新回调该 API，最多会重新回调 7 次（间隔分别为：10m，10m，10m，1h，2h，6h，15h）

4 品而支付签名机制

4.1 RSA 安全签名机制说明

在 RSA 签名时，需要私钥和公钥一起参与签名。私钥与公钥皆是客户通过 OPENSSL 来生成得出的。客户把生成出的公钥与品而的技术人员配置好的品而支付的公钥做交换。因此，在签名时，客户要用到的是客户的私钥及品而支付的公钥。

- 请求时签名

商户当拿到请求时的待签名字符串后，把待签名字符串与商户的私钥一同放入 RSA 签名函数中进行签名运算，从而得到签名结果字符串。

- 通知或返回时验证签名

商户当获得到通知或返回时的待签名字符串后，把待签名字符串、品而提供的公钥、品而通知返回参数中的参数 sign 的值三者一同放入 RSA 签名函数中进行非对称的签名运算，来判断签名是否验证通过。

4.2 品而支付具体实施

1.秘钥分发

1）商户和品而签约时，由品而分配给商家一组或者多组秘钥（api_secret_key），每个秘钥都有一个索引（api_id），商户要妥善保存该组秘钥，不能泄露。

2）品而的服务器会生成一组用于签名的 RSA 秘钥，品而将公钥告知商家，自己保存私钥。商家请求品而的支付服务时，要用品而的公钥签名，品而用自己的私钥验签。

3）商户也要生成一组用于签名的 RSA 秘钥，将公钥告知品而，自己保存私钥。待支付成功后，品而会采用该公钥生成签名，商户要用自己的私钥验签，以验证该回调来自品而。

2.生成待签名字符串

1）需要参与签名的参数

a)商家请求品而的签名参数：

商户标识号：merchant_id,

商户秘钥索引：api_id

商户秘钥：api_secret_key

编码字符集：charset

回跳地址：return_url（如果非空），

订单号：order_id(如果非空)，

交易金额：amount（精确到小数点后两位）

b)品而回调商家的签名参数：

订单号：order_id

交易流水号：transaction_id

2)生成待签名字符串

对参与签名的各个参数，参数名按从 a 到 z 的顺序排序，若遇到相同字母，则看第二个字母，以此类推。并以“&”连接生成字符串。对于如下的参数：

"amount":"11.01",

"merchant_id": "MC0000001409",

"order_id":"fsdirwl24932130fs",

"api_id":"1819957c-1a3f-11e5-ba25-3a22fd90d682",

"charset":"UTF-8",

"return_url":"/checkout/orderList",

生成的待签名字符串为：

amount=11.01&api_id=1819957c-1a3f-11e5-ba25-3a22fd90d682&api_secret_key=mk-prod-18199475-1a3f-11e5-ba25-3a22fd90d682&charset=UTF-8&merchant_id=MC0000001409&order_id=fsdirwl24932130fs&return_url=/checkout/orderList

备注：对应于该 api_id 的秘钥为：（mk-prod-18199475-1a3f-11e5-ba25-3a22fd90d682）

3.签名生成或者验签

对于上述生成的签名字符串做 RSA 签名或者验签