小葱支付回调文档

对外接口文档(v1.1)

目　录

1. 概述 - 1 -
1.1. 文档目的 - 1 -
1.2. 适用范围 - 1 -
2. 应用内支付的数据交互流程 - 1 -
3. 开发指南 - 2 -
3.1. 前期准备 - 2 -
3.1.1. 签名字符串拼接方法 - 2 -
3.2. 服务器交互 - 3 -
3.2.1. 服务器通知（异步方式） - 3 -
3.2.2. 服务器端订单查询 - 3 -
3.3. 签名及验签 - 4 -
3.4. RSA 密钥文件生成 - 4 -
3.4.1. 生成工具 - 4 -
3.4.2. 生成密钥文件 - 4 -
4. 附录 - 5 -
4.1. 服务器返回状态码 - 5 -
4.2. RSA 密钥生成工具 - 5 -
4.3. 服务端 demo - 5 -
4.4. 客户端 demo - 6 -

1. 概述

小葱应用内支付主要是为合作伙伴提供可通过小葱游戏平台完成应用内支付的功能

1.1. 文档目的

本文档主要为小葱的合作伙伴提供以接口方式接入小葱的应用内支付系统，完成应用内支付功能的操作指南

1.2. 适用范围

本文档适用所有需要接入应用内支付功能的合作商和开发人员

2. 应用内支付的数据交互流程

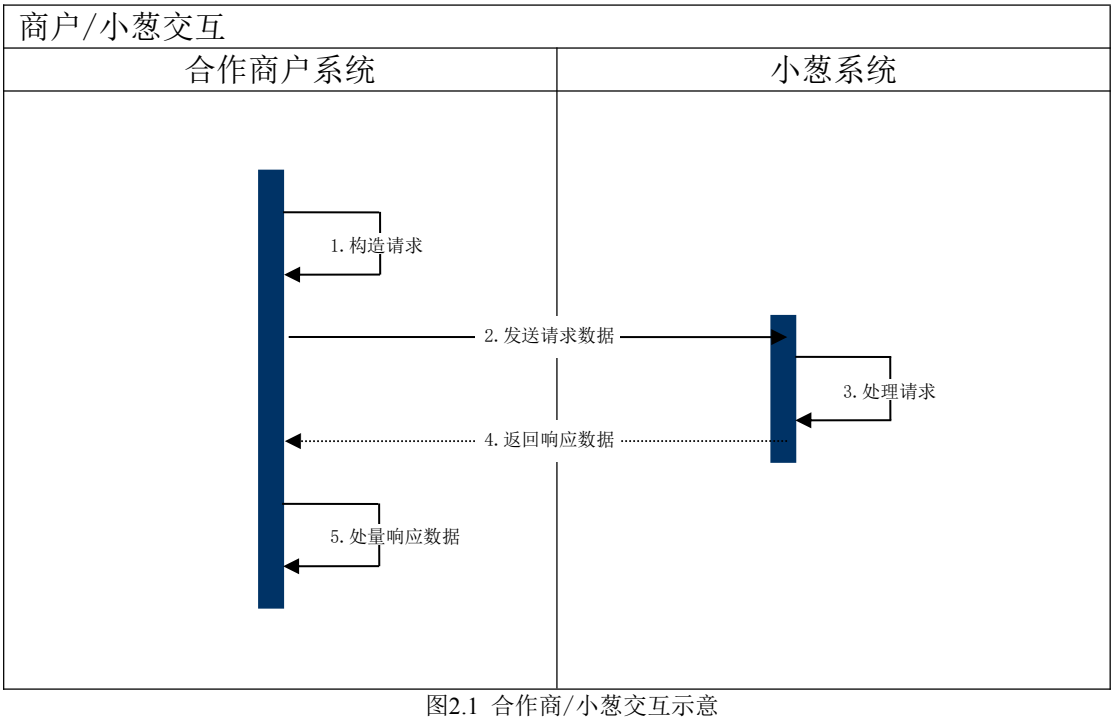

图2.1 合作商/小葱交互示意

(1) 构造请求数据

开发者根据小葱提供的接口规则，通过程序生成得到签名结果及要传输给小葱的参数集合。

(2) 发送请求数据

把构造完成的参数，通过 POST 方式提交给小葱查询接口。
(3) 小葱对请求数据进行处理
小葱平台得到参数后，会先进行签名等验证，验证通过后便会处理这次发送过来的数据请求。
(4) 小葱平台会把处理完成的结果数据以字符串方式返回给开发者。
(5) 开发者利用编程方法来模拟 http 请求并解析返回数据，对返回数据进行验签，再结合自身系统的业务逻辑进行数据处理。

3. 开发指南

3.1. 前期准备

表 3.1 接入前需要准备参数一览

参数名	描述	必须	说明
orderNo	订单号	是	12 到 20 位数字或字母组成，建议 16 位数字
pkgName	应用包名	是	如：tv.xiaocong.launcher
amount	金额	是	单位：分
partnerId	合作商标识	是	合作商在小葱的 ID 号
sign	签名	是	参见签名算法
signType	签名方式	是	MD5,RSA
goodsDes	商品描述	是	请求参数集合
mark	备注	否	第三方临时信息，原样返回
notifyUrl	回调地址	是	异步结果通知地址

接入前合作商请按需要跟我司获取相关商户信息，如果选择 RSA 签名方式，一并将 RSA 公钥告知我司，我司会为合作商提供特定商户标识。已完成商户可略过。

3.1.1. 签名字符串拼接方法

签名串格式为 partnerId&pkgName&amount&orderNo，其中：partnerId 为合作商 ID；pkgName 为当前应用包名；amount 为金额；orderNo 为订单号，字符串示例：100001&tv.xiaocong.launcher&10&2013041510251288。顺序为固定顺序。生成该字符串后再调用相应的签名工具签名，详见章节 3.5

3.2. 服务器交互

3.2.1. 服务器通知（异步方式）

在进行完章节 3.2.1 2）部分请求以后，系统对合作商户的请求数据处理完成后，会将处理的结果数据通过服务器主动通知的方式通知给商户网站。异步通知的参数如下表所示

表 3.3 异步通知参数

参数名	描述	必须	说明
orderNo	订单号	是	12 到 20 位数字或字母组成，建议 16 位数字
amount	金额	是	单位：分
account	小葱号	是	小葱平台账号
sign	签名	是	参见签名算法
notifyTime	回调时间	是	Long 类时间值
goodsDes	商品描述	是	子弹 500 发
status	订单支付状态	是	1：成功；2：失败
mark			
signType	签名方式	否	签名方式(MD5 或 RSA)

1） 异步通知示例

```
http://notify.java.jpxx.org/notify.jsp?
orderNo=2013041510251288&amount=10&account=13218181&notifyTime
=12365212352&goodsDes=子弹 500 发
&status=1&sign=ZPZULntRpJwFmGNIVKwjLEF2Tze7bqs60rxQ22CqT5J1UlvGo575QK
9z/+p+7E9cOoRoWzqR6xHZ6WVv3dloyGKDRObtvrdq
PgUAoeaX/YOWzTh00vwcQ+HBtXE+vPTfAqjCTxiiSJEOY7ATCF1q7iP3sfQxhS0nDUug1
LP3OLk&mark=testcontent
```

2） 合作商户返回结果

商户直接将处理后的返回信息输出到页面上。输出信息为成功：success，失败：fail，签名失败：sign_fail。

3.2.2. 服务器端订单查询

1） 请求格式

```
http://data.xiaocong.tv/queryOrderInfo.action?orderNo=2013041510251288
```

2） 请求参数说明

表 3.4 服务器订单查询参数

参数名	描述	必须	说明
orderNo	订单号	是	12 到 20 位数字或字母组成，建议 16 位数字

3） 返回结果说明

返回结果字符串格式：status~message~，status 代表订单状态，0 未支付，1 成功，2 失败。message 是相应的提示信息。

3.3. 签名及验签

根据选择的签名方式，使用 client-xiaocong-1.0.0-sources.jar 提供的方法完成签名及验签处理。RSA 密钥生成详见章节 3.5

3.4. RSA 密钥文件生成

3.4.1. 生成工具

下载并解压 openssl-0.9.8k_WIN32(RSA 密钥生成工具).zip 工具。章节 4.2 附件

3.4.2. 生成密钥文件

1） 生成 RSA 私钥 PIM 文件

假设您解压后的目录在 C:\xiaocong 目录下，命令行执行“openssl genrsa -out rsa_private_key.pem 1024”命令生成 rsa_private_key.pem 文件，该文件会生成在 C:\xiaocong\bin 文件夹下。

```
C:\xiaocong\bin>openssl genrsa -out rsa_private_key.pem 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.........................++++++
....++++++
e is 65537 (0x10001)
```

图 3.2 生成私钥

2） 生成公钥

继续在命令行执行“openssl rsa –in rsa_private_key.pem –pubout –out rsa_public_key.pem”命令生成 rsa_public_key.pem 文件，该文件会生成在 C:\xiaocong\bin 文件夹下。

```
C:\xiaocong\bin>openssl rsa -in rsa_private_key.pem -pubout -out rsa_public_key.
pem
writing RSA key

C:\xiaocong\bin>
```

图 3.3 生成公钥

3） 将 RSA 私钥转换为 PKCS8 格式

命令行执行“openssl pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outform PEM -nocrypt”命令得到下图的私钥，并 copy 出来保存好。

上面（2）和（3）生成的公钥和私钥是商户自己的公钥和私钥。将换成 PKCS8 格式 pem 或 txt 文件发给我司

```
C:\xiaocong\bin>openssl pkcs8 -topk8 -inform PEM -in rsa_private_key.pem -outfor
m PEM -nocrypt -out rsa_private_key_pkcs8.pem

C:\xiaocong\bin>
```

图 3.4 私钥转换格式

4. 附录

4.1. 服务器返回状态码

表 4.1 服务器返回状态码

状态码	信息	说明
200	OK	成功
400	BAD_REQUEST	请求参数错
500	SERVER_ERROR	服务器错误
509	ORDER_NOT_EXISTS	订单不存在
510	ORDER_CREATE_ERROR	订单创建失败
511	ORDER_STATUS_INVALID	订单未支付
512	ORDER_STATUS_PAY_FAILED	订单支付失败
513	ORDER_SIGN_FAILED	订单签名失败
601	USER_BALANCE_INSUFFICIENT	余额不足

4.2. RSA 密钥生成工具

openssl-0.9.8k_WIN32(RSA密钥生成工具).rar

4.3. 服务端 demo

服务端demo.rar

4.4. 客户端 demo

客户端demo.rar