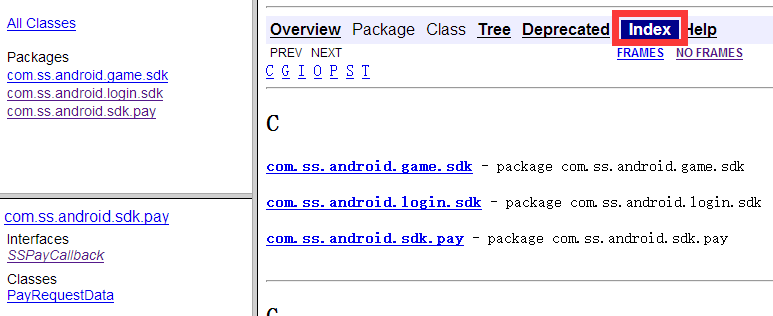
1. 打开index.html，然后选择index，即可看到接口说明：



1. 支付SDK合作文档

A）版本

| **更新日期** | **版本** | **变更** | **是否需要紧急升级** |
| --- | --- | --- | --- |
| 20150403 | 1.0 | 第一版文档 |  |
| 20150527 | 2.0 | 1. 增加银联支付  2. 增加联系电话  3. 修复安全问题及其他bug | 需要 |

# B)名词解析

## 1. 签名

目的：数据防伪

方式：分为对称签名和非对称签名。

## 2. 同步通知

客户端调用支付SDK的接口，SDK经过一系列支付流程，从调用函数返回，唤醒调用支付的app，继续走之后的流程。

## 3. 异步通知

客户端调用支付SDK的接口，SDK经过一系列支付流程，完成支付后，由相应的支付服务器对设定好的notify\_url发通知。

## 4. 常用参数

| **名称** | **含义** | **别名** | **备注** |
| --- | --- | --- | --- |
| client\_id | 合作方ID或APPID | client\_key; app\_id |  |
| client\_secret | 合作方密钥 | app\_secret |  |
| pay\_key | 支付MD5签名密钥 |  | 由client\_id和client\_secret生成 |
| open\_id | 授权给某个合作方/APP的头条用户的ID |  | 同一个用户，对不同合作方/不同APP生成的open\_id都不一样 |

# C) SDK使用流程

主要流程如下：

1. 用户在第三方应用内下单，第三方应用请求第三方应用服务端；
2. 第三方应用服务端生成商品订单，并返回支付相关参数给第三方应用；
3. 第三方应用使用支付相关参数，调用头条支付SDK；
4. 用户使用头条支付SDK完成支付；
5. 头条支付SDK异步通知第三方应用服务器支付结果；
6. 第三方应用服务器校验通知结果，并发放商品到应用。

# D)支付SDK唤醒

TODO 增加SDK文档

# E) 支付异步通知接口

头条整合微信/支付宝的异步通知，合并成同构的异步通知转发给业务方。业务方需要为头条提供一个处理异步通知的url。在校验过参数后并处理完关键逻辑后，返回success。在通知失败时会重试通知，策略和支付宝/微信类似。

为了保证异步通知数据安全，请务必做以下两件事情：

1. 校验头条签名。
2. 校验支付金额是否和订单金额一致。

头条请求改接参数都以POST方式传递，参数列表如下：

| **域** | **含义** | **说明** | **类型** | **是否可空** |
| --- | --- | --- | --- | --- |
| notify\_id | 通知ID |  |  | 否 |
| notify\_type | 通知类型 | 支付异步通知：trade\_status\_sync |  | 否 |
| notify\_time | 通知时间 | 格式为【yyyy-MM-dd HH:mm:ss】 |  | 否 |
| trade\_status | 支付订单状态 |  |  | 否 |
| way | 支付类型 |  |  | 否 |
| client\_id | client\_id |  |  | 否 |
| out\_trade\_no | 商品订单号 |  |  | 否 |
| trade\_no | 支付流水号 | 支付宝对应trade\_no  微信对应transaction\_id |  | 是 |
| pay\_time | 支付时间 | 格式为【yyyy-MM-dd HH:mm:ss】 |  | 是 |
| total\_fee | 总费用 | 单位为分 | int | 是 |
| buyer\_id | 购买者 | 支付宝对应buyer\_email  微信对应open\_id | string |  |
| tt\_sign | 头条签名 |  |  | 否 |
| tt\_sign\_type | 头条签名类型 | 暂只支持RSA签名 |  | 否 |

# F) 用户验证接口

### url

<https://open.snssdk.com/partner_sdk/check_user/>

请求参数

| **name** | **类型** | **说明** |
| --- | --- | --- |
| client\_key | string | 合作方client\_key(client\_id) |
| uid | int | 要校验的用户id |
| access\_token | string | 要校验的access\_token |

接口返回

|  |  |  |
| --- | --- | --- |
| message | string | 成功返回success，非法返回error |
| data | dict | 成功   | **name** | **类型** | **说明** | | --- | --- | --- | | result | int | 验证通过返回1，异常返回0 |   失败   | **name** | **类型** | **说明** | | --- | --- | --- | | error\_code | int | 错误码 | | description | string | 错误描述 | |
| **name** | **类型** | **说明** |

正确请求

|  |
| --- |
| {      message: "success",      data:          {              verify\_result: 1          }  }  {      message: "success",      data:          {              verify\_result: 0          }  } |

错误请求

|  |
| --- |
| message: "error",  data: {      error\_code: 1,      description: "会话过期，请重新登录"  } |

# G) 支付订单状态（trade\_status）

| **状态** | **值** | **说明** | **备注** |
| --- | --- | --- | --- |
| 交易成功 | 0 | 交易成功，可以做退款操作 | 对应微信的trade\_status=0  对应支付宝的TRADE\_SUCCESS |
| 等待支付 | 1 |  | 微信无此状态  对应支付宝的WAIT\_BUYER\_PAY |
| 交易关闭 | 2 | 交易支付超时关闭  交易退款成功后关闭 | 微信无此状态  对应支付宝的TRADE\_CLOSED |
| 交易结束 | 3 | 交易成功，并且不可退款 | 微信无此状态  对应支付宝的TRADE\_FINISH  【备注1】 |
| 未知状态 | 99 | 发现有这种状态，是未处理的，请通知头条工程师 |  |

备注1：

同一个订单可能通知多次，应用服务器需要记录防止重复处理。

# H) 支付方式（way）

| **方式** | **值** | **使用场景** | **说明** |
| --- | --- | --- | --- |
| 微信 | 1 | 微信app支付 |  |
| 支付宝 | 2 | 支付宝快捷支付 |  |
| 银联 | 4 | 银联支付 |  |
| 充值卡 | 5 | 高阳充值卡 |  |

# I) 支付签名方式

### 待签名数据集

待签名数据集是一个键值对集合

### 待签名字符串生成方式

由待签名数据集的键值对，按照key=value的形式拼接，然后按照字母序排序成一个字符串数组，用字符'&'来连接这个数组，得到的字符串作为待签名字符串。其中value不需要做url\_encode转换。

### MD5签名方式

签名方式：在待签名数据集生成签名串后，加上'&key=pay\_key'，构成最后待签名字符串，对此字符串做md5摘要，得到的结果转成字母小写格式后就是签名结果。其中pay\_key由client\_id和client\_secret两者生成。生成算法：pay\_key=md5(client\_id#client\_secret)。

验签方式：同签名方式，得到验证签名结果，对比是否和原始签名结果一致。

### RSA签名方式

签名方式：得到待签名字符串后，用私钥签名，得到的结果就是签名结果。

验签方式：得到待签名字符串后，用公钥验证给出的签名是否正确。

### 签名使用情况

| **应用场景** | **签名方** | **验证方** | **签名方式** | **待签名数据集** | **验证结果** | **签名数据** | **验签数据** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| notify通知防伪 | 头条 | 第三方 | RSA | notify通知中POST的参数中，除了tt\_sign和tt\_sign\_type之外的所有参数 | tt\_sign | 头条支付私钥 | 头条支付公钥 |

### 头条支付公钥

#### PEM格式

-----BEGIN PUBLIC KEY-----  
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOZZ7iAkS3oN970+yDONe5TPhP  
rLHoNOZOjJjackEtgbptdy4PYGBGdeAUAz75TO7YUGESCM+JbyOz1YzkMfKl2HwY  
doePEe8qzfk5CPq6VAhYJjDFA/M+BAZ6gppWTjKnwMcHVK4l2qiepKmsw6bwf/kk  
LTV9l13r6Iq5U+vrmwIDAQAB  
-----END PUBLIC KEY-----

#### DER格式

MIICWDCCAcGgAwIBAgIJAMN5U/9tdXkqMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNVBAYTAkFVMRMw  
EQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwHhcN  
MTQxMDExMDQwMzU3WhcNMTQxMTEwMDQwMzU3WjBFMQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29t  
ZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEB  
AQUAA4GNADCBiQKBgQDOZZ7iAkS3oN970+yDONe5TPhPrLHoNOZOjJjackEtgbptdy4PYGBGdeAU  
Az75TO7YUGESCM+JbyOz1YzkMfKl2HwYdoePEe8qzfk5CPq6VAhYJjDFA/M+BAZ6gppWTjKnwMcH  
VK4l2qiepKmsw6bwf/kkLTV9l13r6Iq5U+vrmwIDAQABo1AwTjAdBgNVHQ4EFgQUF18veywud+8P  
0TiaRqHFMJsVAZ4wHwYDVR0jBBgwFoAUF18veywud+8P0TiaRqHFMJsVAZ4wDAYDVR0TBAUwAwEB  
/zANBgkqhkiG9w0BAQUFAAOBgQBMHZrUO0FSHxIe/W1D+uRFreYvDONd0TRr6EEhFAPlNFuUapJo  
T+iYMCrHG5mhlgCk3uUl+mTRdxHXVuIIyL6N2a0IGDYwQN7FD3oh8T0We5gMAE26Ns1d52rNOc6M  
oUn/DY74Eji/LMZpLZQSfZope/6hHHfYoCc/fva74bUGjw==

# [SDK接入FAQ](https://wiki.bytedance.com/pages/viewpage.action?pageId=28508821)

Q：申请接入通过后需要从头条获取那些参数来集成SDK？  
A：client\_key，client\_secret（请联系头条游戏运营获取），pay\_key（合作方自己生成）

Q：是否需要为每一款应用配置不同的client\_key，client\_secret？  
A：是的。

Q：如何生成pay\_key？  
A：pay\_key由client\_id和client\_secret两者生成。生成算法：pay\_key=md5(client\_id#client\_secret)。

Q：接入需要准备什么参数？  
A：准备一个异步通知地址，并告知头条。

Q：RSA验签用哪种？  
A：RSA签名是对数据做sha1后再做rsa签名。Java中对应是SHA1WithRSA。

Q：头条内否保证异步通知的金额准确？  
A：可以保证异步通知的金额与用户实际支付的金额一致，但不保证通知金额和订单期望支付金额一致，所以合作方需要对这两者做校验。

Q：可以退款吗？  
A：SDK支付目前不支持退款操作。

Q：收到什么样的异步通知可以发货？  
A：trade\_status为0或3时表示支付成功，可以发货。但要主要避免重复发货。

Q：需要有私钥吗？  
A：现在合作方服务端不需要签名，所以不需要私钥。

Q：是否支持微信支付？  
A：sdk机制上支持，但需要为每一款应用申请微信支付权限。

Q：登录回调在哪？  
A：在SsGameApi中有一个onActivityResult，放到Activity。在onActivityResult中，会返回一个AccessToken和userId。

Q：登录接口有显式调用方式吗？  
A：登陆的Api是这个：tryLogin(Activity act, int requestCode, StatusCallback statusCallback)

Q：如何实现游戏时长统计？  
A：有两个API, 来记录应用开启时长，SsGameApi.onResume和SsGameApi.onPause，合作方需要主动调用。

Q：包名有特殊要求么？横竖屏，切换有相关接口吗？  
A：没有要求，横竖屏没有相关接口，接入只要引用libs 工程就行了。

Q：sdk初始化后会自动调用登录吗？  
A：登陆过会记录AccessToken，在有效期内可以认为登陆了，可以通过isLogin来判断。

Q：如何判断用户验证成功了？  
A：可以这样判断：  
if response.get('ret', 0) != 0:  
    handle\_error()  
else:  
    handle\_success()

Q：有更多问题想咨询头条研发？  
A：请加QQ群：416571440，负责SDK对接的研发会在群里解答。