**基于OAuth2.0的登录验证授权方式介绍**

* [前言](http://open.taobao.com/doc/detail.htm?id=118#s0)
* [名词解释](http://open.taobao.com/doc/detail.htm?id=118#s1)
* [Server-side flow](http://open.taobao.com/doc/detail.htm?id=118#s2)
* [Client-side flow](http://open.taobao.com/doc/detail.htm?id=118#s3)
* [Native Application](http://open.taobao.com/doc/detail.htm?id=118#s4)
* [Refreshing an Access Token](http://open.taobao.com/doc/detail.htm?id=118#s5)
* [登录帐号退出流程](http://open.taobao.com/doc/detail.htm?id=118#s6)
* [DEMO](http://open.taobao.com/doc/detail.htm?id=118#s7)
* [附录](http://open.taobao.com/doc/detail.htm?id=118#s8)
* [错误码排查](http://open.taobao.com/doc/detail.htm?id=118#s9)

**前言**

       如果您的网站和淘宝对接后，需要获取一些与用户紧密相关的信息（如用户偏好、收藏夹、购物车信息等），为保证用户数据的安全性与隐私性，您的网站需要取得用户的同意，即引导用户去授权。在这种情况下，您的网站需要使用“用户使用淘宝帐号登录并授权”流程。

       淘宝的Taobao ID（淘帐号）产品，采用国际通用的OAuth2.0标准协议，作为用户身份验证与授权协议，支持网站、手机客户端、桌面客户端。若要了解更多关于 OAuth2.0 的技术说明文档，可参看官方网站(http://oauth.net/2/) 。目前淘宝OAuth2.0服务支持采用以下4种获取Access Token（授权令牌）的方式：

* Server-side flow 此流程要求ISV应用有Web Server应用，能够保存应用本身的密钥以及状态，可以通过https直接访问淘宝的授权服务器。
* Client-side flow 此流程适用于没有独立服务器的应用，但是能够借助浏览器或者JS脚本访问授权服务器。
* Native Application 此流程适合客户端应用，同时应用无法与浏览器交互，但是可以外调用浏览器。
* Refreshing an Access Token 用户如果在获取访问令牌时，同时获取到了刷新令牌，当访问令牌过期时，用户可以用刷新令牌刷新，从而延长访问令牌的时间。

**名词解释**

**1. redirect\_uri及callback定义规则**

redirect\_uri指的是应用发起请求是，所传的回调地址参数。

callback指的是应用注册时，填写的回调地址链接。

相关的规则是：

（1）对于Server-side flow，redirect\_uri是必选参数，并且要求redirect\_uri与callback的顶级域名一致。

（2）对于Client-side flow，redirect\_uri是可选参数，如果传了redirect\_uri，则相应的中间参数会返回到redirect\_uri，并且要求 redirect\_ur与callback的顶级域名一致，如果没有传redirect\_uri，则不做校验，返回相应的中间参数到淘宝默认授权返回页 面。

（3）在不可预知错误的情况下，返回到默认错误页面。

**2. scope定义规则**

scope指的是应用发起请求时，所请求的API调用权限范围。

scope参数为以下可选值：

item,promotion, usergrade。

应用发起请求时，多个scope值要求用逗号分隔。其中item,promotion, usergrade为高危授权。

**3. View参数为以下可选值：**

web,tmall,wap。

其中：

Web对应普通的PC端（淘宝logo）浏览器页面样式。

Tmall对应天猫的浏览器页面样式。Web对应普通的PC端（淘宝logo）浏览器页面样式。

Wap对应无线端的浏览器页面样式。

**4.Access Token**

Access Token即用户授权后颁发的[session key](http://open.taobao.com/doc/detail.htm?id=162)

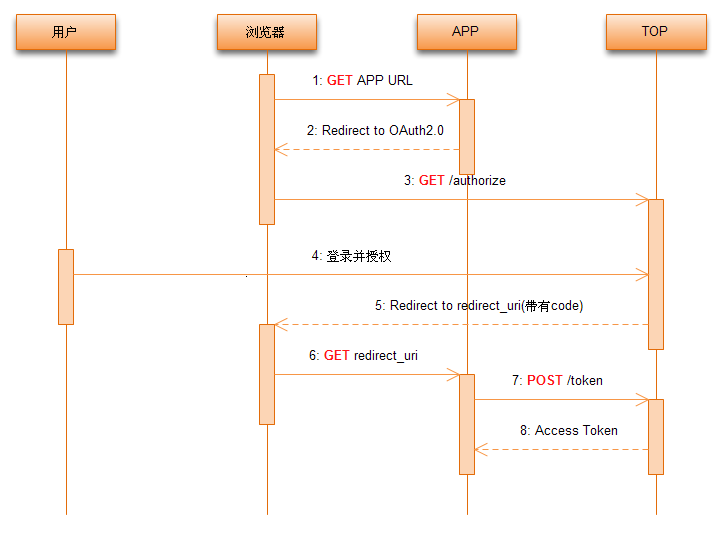
**5.使用淘宝帐号登录（不授权）**

[详细文档](http://open.taobao.com/doc/detail.htm?spm=0.0.0.22.dudlU2&id=974)

**Server-side flow**

此流程需要您有自己的web服务器,能够保存应用本身的密钥以及状态，可以通过https直接访问淘宝的授权服务器。

授权过程分为两个步骤：



(1) 通过用户授权获取授权码Code； （获取授权码 :<https://oauth.taobao.com/authorize> ）

(2) 用上一步获取的Code和应用密钥（AppSecret）通过Https Post方式换取Token。 （获取访问令牌： <https://oauth.taobao.com/token> ）

沙箱环境 访问 https://oauth.tbsandbox.com/authorize

**1. 参数说明**

**1.1 获取授权码参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名字 | 参数选项 | 参数值 | 参数释义 |
| client\_id | 必选 |  | 等同与appkey |
| response\_type | 必选 | code |  |
| redirect\_uri | 必选 |  | 参见redirect\_uri的定义 |
| scope | 可选 |  | 参见scope的定义 |
| state | 可选 |  | 维持应用的状态，传入值与返回值保持一致。 |
| view | 可选 | 默认为web |  |

**1.2 返回值说明**

|  |  |  |
| --- | --- | --- |
| 参数名字 | 参数选项 | 参数释义 |
| code | 正常结果 | 授权码 |
| error | 异常时返回 | 错误码 |
| error\_description | 异常时返回 | 错误描述 |

**2.1 获取访问令牌参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名字 | 参数选项 | 参数值 | 参数释义 |
| client\_id | 必选 |  | appkey的值 |
| client\_secret | 必选 |  | appsecret |
| grant\_type | 必选 | authorization\_code |  |
| code | 必选 |  | 授权码 |
| redirect\_uri | 必选 |  | 参见redirect\_uri的定义 |
| scope | 可选 |  | 参见scope的定义 |
| state | 可选 |  | 维持应用的状态，传入值与返回值保持一致。 |
| view | 可选 | 默认为web |  |

注：服务平台上的“立即使用”链接点击以后会传递一些信息给应用，这些参数会使用state参数传递。

参数形式如下：state=versionNo:1;itemCode:xxxxx

**2.2 获取访问令牌的返回值以json格式返回**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | 类型 | 选项 | 示例 | 说明 |
| access\_token | string | 必选 | 2YotnFZFEjr1zCsicMWpAA | Access token |
| token\_type | string | 必选 | Bearer | Access token的类型目前只支持bearer |
| expires\_in | number | 必选 | 10（表示10秒后过期） | Access token过期时间 |
| refresh\_token | string | 可选 | 2YotnFZFEjr1zCsicMWpAA | Refresh token |
| re\_expires\_in | number | 可选 | 10（表示10秒后过期） | Refresh token过期时间 |
| r1\_expires\_in | number | 必选 | 10（表示10秒后过期） | r1级别API或字段的访问过期时间 |
| r2\_expires\_in | number | 必选 | 10（表示10秒后过期） | r2级别API或字段的访问过期时间 |
| w1\_expires\_in | number | 必选 | 10（表示10秒后过期） | w1级别API或字段的访问过期时间 |
| w2\_expires\_in | number | 必选 | 10（表示10秒后过期） | w2级别API或字段的访问过期时间 |
| taobao\_user\_nick | string | 必选 | 淘宝测试test | 淘宝账号 |
| taobao\_user\_id | string | 必选 | 706388888 | 淘宝帐号对应id |
| sub\_taobao\_user\_id | string | 可选 | 2343535 | 淘宝子账号 |
| sub\_taobao\_user\_nick | string | 可选 | 淘宝测试test:123 | 淘宝子账号对应id |

**3.应用示例**

**3.1请求授权用户登录**

<https://oauth.taobao.com/authorize?response_type=code&client_id=12304977&redirect_uri=http://www.oauth.net/2/&state=1212&scope=item&view=web>



**3.2 请求授权用户授权（用户登录后）**

****

**3.3 获取授权码**

出现授权页面后，用户可以选择“授权“ 或 ”取消“。

若用户选择“取消“，则页面跳转至应用的回调地址，同时返回如下错误信息：

error=access\_denied

error\_description=authorize%20reject

http://img01.taobaocdn.com/top/i1/T15tKPXopgXXb1upjX.jpg

若用户选择“授权“，则页面跳转至应用的回调地址，同时返回授权码code以及state参数。

http://img01.taobaocdn.com/top/i1/T1cUKOXmJsXXb1upjX.jpg

**3.4 获取访问令牌**

如果你对 linux 比较熟悉，可以利用 curl 命令体验一下如何获取访问令牌。**注意替换一下** **"code="后面的授权码,其他参数也根据实际情况进行替换。**

curl -i -d "code=xMuBtklMeuxr0AujfjOZ3lht1&grant\_type=authorization\_code&client\_id=12304977&client\_secret=9288fb99669a14b6a9bf28e49b270f98&redirect\_uri=http://www.oauth.net/2/ " https://oauth.taobao.com/token

对于应用程序，可以参考如下代码获取访问令牌：

Map<String, String> param = new HashMap<String, String>();

param.put(“grant\_type”, "authorization\_code");

param.put(“code”, 授权码);

param.put(“client\_id”, appKey);

param.put(“client\_secret”, appSecret);

param.put(“redirect\_uri”, redirect\_uri);

param.put(“scope”, “item”);

param.put(“view”, “web”);

param.put(“state”, state);

String responseJson=WebUtils.doPost(tbPostSessionUrl, param, 3000, 3000);

然后把responseJson 转化为对象，或者直接从里面提取：access\_token字段。

返回结果内容示例：

|  |
| --- |
| {    "w2\_expires\_in": 0,    "taobao\_user\_id": "263685215",    "taobao\_user\_nick": "%E5%95%86%E5%AE%B6%E6%B5%8B%E8%AF%95%E5%B8%90%E5%8F%B752",    "w1\_expires\_in": 1800,    "re\_expires\_in": 0,    "r2\_expires\_in": 0,    "expires\_in": 86400,    "token\_type": "Bearer",    "refresh\_token": "6200e1909ca29b04685c49d67f5ZZ3675347c0c6d5abccd263685215",    "access\_token": "6200819d9366af1383023a19907ZZf9048e4c14fd56333b263685215",    "r1\_expires\_in": 1800  } |

此种方式获得的access tokn可以通过https协议免签名调用API: <http://open.taobao.com/doc/detail.htm?id=994> (推荐采用此方式）

引用：http://open.taobao.com/doc/detail.htm?id=118#s2