oauth2.0授权文档

# 概述

## 功能描述

本文档用于描述oauth2.0对接的流程和协议。

## 名词解释

### Oauth2

OAuth2是一个关于授权（authorization）的开放网络标准，在全世界得到广泛应用，目前的版本是2.0版。Oauth2在"客户端"与"服务提供商"之间，设置了一个授权层（authorization layer）。"客户端"不能直接登录"服务提供商"，只能登录授权层。"客户端"登录授权层所用的令牌（token），与用户的密码不同。用户可以在登录的时候，指定授权层令牌的权限范围和有效期。"客户端"登录授权层以后，"服务提供商"根据令牌的权限范围和有效期，向"客户端"开放用户储存的资料。传统的Oauth授权是指Oauth1，现已过时，升级到Oauth2不再兼容Oauth1。

# 登录方法

## Oauth2

适用于任何合作方经过用户授权后获取服务方用户资源的场景。

注意点：

1、服务器分为两种，即认证服务器和资源服务器，资源服务端需设置不同用户的不同权限以及令牌的有效时间；

2、合作方需要接入，服务方需要向其提供client\_id，redirect\_uri（由合作方指定提供）和其他密码等信息方可接入(需要我方提供)；

3、相似地，合作方在拿到服务方给出的信息后，也要确认正确的信息方可接入到服务方。

Oauth2的使用一般流程如下：

（A）用户打开客户端以后，客户端要求用户给予授权。

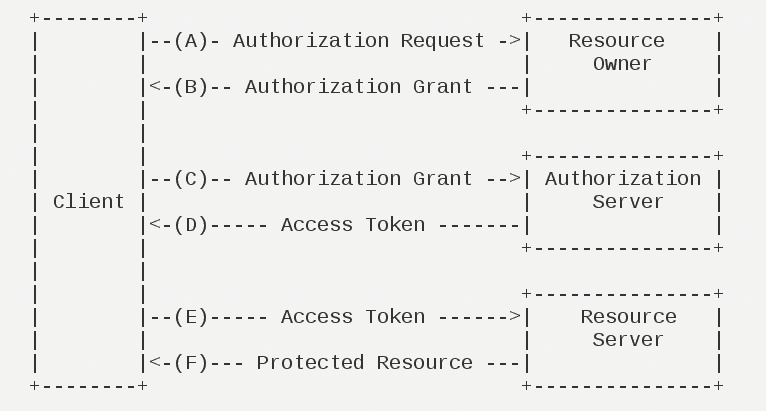
（B）用户同意给予客户端授权。

（C）客户端使用上一步获得的授权，向认证服务器申请令牌。

（D）认证服务器对客户端进行认证以后，确认无误，同意发放令牌。

（E）客户端使用令牌，向资源服务器申请获取资源。

（F）资源服务器确认令牌无误，同意向客户端开放资源。

****

PS：合作方需省申请client\_id和client\_secret，以及适当的配置。

# 接口详细说明

## 授权登录

应用场景: oauth2是一个双方的协议，即双方任何一方作为服务方或合作方都允许，适用于一些合作平台和开放平台。

合作方通过url跳转让用户主动选择授权，授权通过后，让合作方获取服务方的用户资源。

前置条件：serivce帐号已经登录。

现我方作为服务方，合作方作为应用方，则对方需获取我方的信息，然后可以使用我方的账户登录。主要接口有：

1、请求授权接口

|  |  |
| --- | --- |
| **URL：** | http://open.oauth.com/oauth2/authorize.do?client\_id=abc&redirect\_uri=http://oauth.abc.com &client=touch |
| **方法** | GET |
| **功能描述** | 请求授权页面接口，正常情况下返回授权码code |
| **调用源** | 浏览器，由用户选择点击 |
| **正常结果** | 如果用户未登陆或者code生成错误则跳转到“请求授权接口”的页面；如果成功则跳转到redirect\_uri  1.如果未传递参数会跳转到错误页面，并显示信息“对不起，请求参数不能为空”；  2.如果校验参数出错会跳转到错误页面，并显示信息“对不起，该网站尚未开通xx账号登录”；  3.当回调地址的域名与保存的域名不同时，会跳转到错误页面，并显示信息“对不起，你所在的站点在xxx认证失败，请联系xxx”；  4. 请求code但找不到在线用户时，给错误提示“请先授权并登录您的xx账号”；  5.当授权失败时，返回错误信息“授权失败，请重试”；  6.授权成功后会带code重定向到redirect\_uri,例如本例会跳转到：http://oauth.abc.com?code=009424bed669f5bef8c9b718b3033a41  7.其中参数client=touch 是触屏版使用（手机端、客户端等），PC端请勿使用此参数。 |
| **异常结果** | http错误：如500、404、400 |

2、生成token的接口：JSON

|  |  |
| --- | --- |
| **URL：** | http://open.oauth.com/oauth2/token.do?client\_id=1234567&redirect\_uri=http://oauth.abc.com&code=009424bed669f5bef8c9b718b3033a41&client\_secret=efewf3924fee5w.;%27.&grant\_type=authorization\_code |
| **方法** | GET |
| **功能描述** | 使用授权码获取令牌的接口 |
| **调用源** | 服务器自动跳转 |
| **正常结果** | 为请求端发放令牌，令牌有效时间一般为一个月，返回的参数包括令牌id：tokenId和有效日期：expires，各种出错结果如下：  {"message":"参数不对","data":{},"code":"-1","success":0}  {"message":"暂时只支持authorization\_code授权","data":{},"code":"-1","success":0}  {"message":" code失效或者已过期","data":{},"code":"-2","success":0}  {"message":"第三方应用检查不通过","data":{},"code":"-2","success":0}  {"message":"服务器出错，请稍后再试","data":{},"code":"-3","success":0}  成功结果如下：  {"message":"令牌发放成功","data":{"expires":1438832321000,"tokenId":"833c95512f868cd135da253d89bc2dbe"},"code":"1","success":1} |
| **异常结果** | http错误：如500、404、400 |

3、开放信息：JSON

|  |  |
| --- | --- |
| **URL：** | http://open.oauth.cn/oauth2/user/info.do?client\_id=1234567&token=23f8bb6828f8161ef0e0d5f871638a4f |
| **方法** | GET |
| **功能描述** | 使用令牌获取用户信息接口 |
| **调用源** | 服务器自动跳转 |
| **正常结果** | 可能出错的情况如下：  {"message":"参数不对","data":{},"code":"-1","success":0}  {"message":"token不存在或者已经失效","data":{},"code":"-2","success":0}  正常时返回用户信息，包括：用户id：user\_id,用户名：user\_name，性别:sex等信息，如下：  {"message":"获取用户信息成功","data":{"data":{"username":"username","sex":"男"}},"code":"1","success":1} |
| **异常结果** | http错误：如500、404、400 |