# OAuth2.0认证授权技术

## 认证授权过程

在认证和授权的过程中涉及的三方包括：

1、**服务提供方**，用户使用服务提供[方来](http://baike.baidu.com/view/5440797.htm)存储受保护的资源，如照片，视频，联系人列表。

**2、用户**，存放在服务提供方的受保护的资源的拥有者。

**3、客户端**，要访问服务提供方资源的[第三方应用](http://baike.baidu.com/view/5083751.htm)，通常是网站，如提供照片打印服务的网站。在认证过程之前，客户端要向服务提供者申请客户端标识。

使用OAuth进行认证和授权的过程如下所示:

用户想操作存放在服务提供方的资源。

用户登录客户端向服务提供方请求一个临时令牌。

服务提供方验证客户端的身份后，授予一个临时令牌。

客户端获得临时令牌后，将用户引导至服务提供方的授权页面请求用户授权。在这个过程中将临时令牌和客户端的回调连接发送给服务提供方。

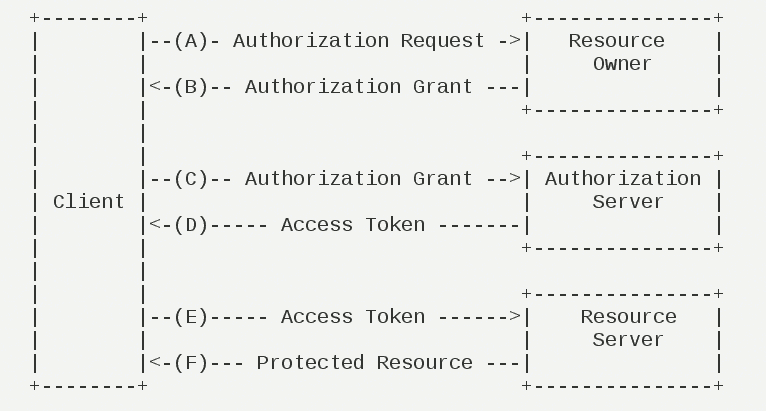
用户在服务提供方的网页上输入用户名和密码，然后授权该客户端访问所请求的资源。

授权成功后，服务提供方引导用户返回客户端的网页。

客户端根据临时令牌从服务提供方那里获取访问令牌。

服务提供方根据临时令牌和用户的授权情况授予客户端访问令牌。

客户端使用获取的访问令牌访问存放在服务提供方上的受保护的资源。



## 技术优点

在使用中，OAuth不会使第三方网站或应用接触到用户的帐号信息(如用户名与密码)，授权后的http通信中也不再传输用户信息而是以数字签名和访问令牌(AccessToken)取代，即使截到数据包，也无法还原出用户的登录信息。这是OAuth最大的优点，也是它得以逐渐成为现在通用的授权标准的原因。

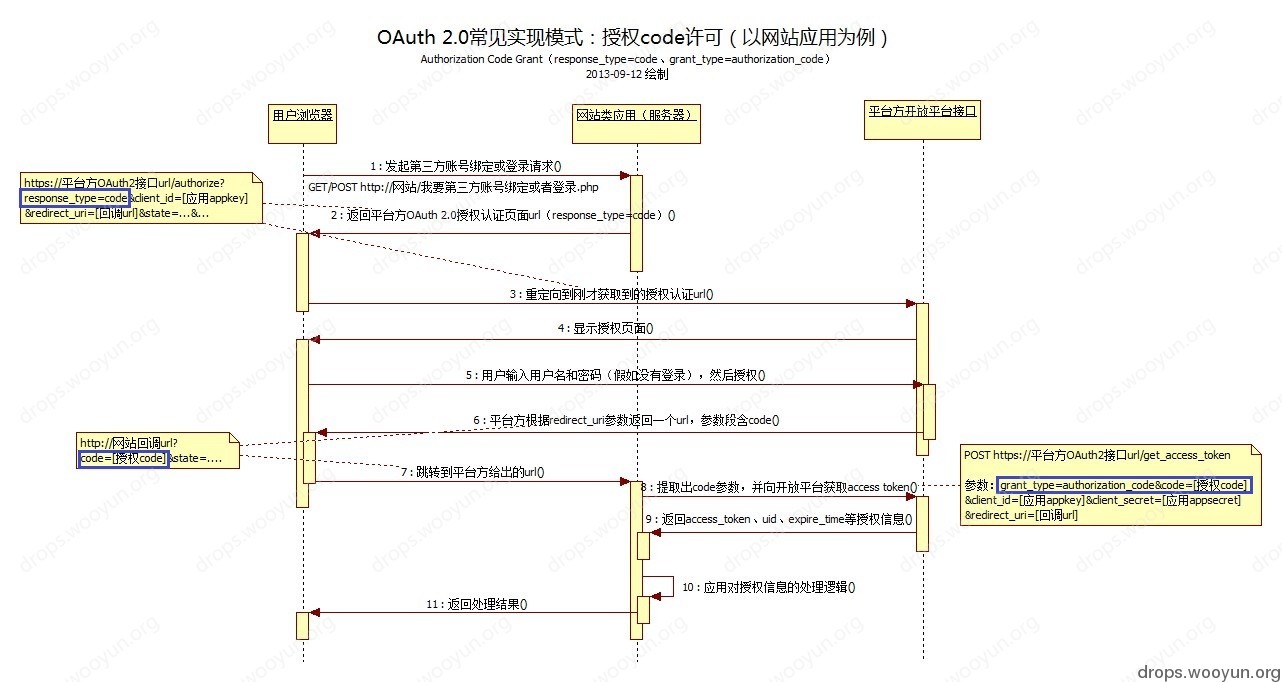
# 统一认证平台实现

## 用户注册

统一认证平台开放用户注册界面（基于html5），可自动适配大小不同屏幕，可直接在页面进行用户注册，用户数据直接存储到统一认证平台。

统一认证平台开放restful接口供其他系统或者第三方应用调用。

## 用户登录



## 权限控制

用户通过统一认证平台登录且完成授权后，用户授权信息记录到认证平台开放授权数据库（可与用户数据库分离）,第三方应用进行系统资源访问时需携带统一认证平台发放的access\_token，系统资源服务器首先进行access\_token对应权限认证，若成功可成功访问系统资源(web页面，restful接口或其他),若失败则访问失败。

## 数据库设计

