## 第三方用户登录技术需求

## 一．授权登录：

采用auth2.0协议方式，有服务端，客户端

1. 获得授权码（access tokey）

服务端发放一个加密密钥，客户端在每次请求时带入此密钥

1. 跳转到第三方登录（已经登录，到确认授权页）

即在客户端放一个登录按钮，点此按钮进入到服务端，获取Authorization Code，成功通过，显示登录界面，用户输入帐号，密码等登录；

如果用户已经有登录状态，会弹出提示一个确认页。如果还没有登录，会弹出登录页

1. 登录成功，确认授权

成功登录后，弹出授权框引导用户授权（仅在第一次成功登录，以及第一次访问某个未授权的OpenAPI时会出现授权页）；

如果用户点击“跳过”，则跳转到回调地址，返回帐号、性别和邮箱(要求是已验证的邮箱，未验证的不予获取)。

如果用户点击“确认”授权，则成功跳转到指定的redirect\_uri，并跟上Authorization Code（**此code会在10分钟内过期**）。

回调地址通常是客户端的用户中心页

1. 取得第三方授权信息

通过Authorization Code获取Access Token

获取到的access token具有3个月有效期，用户再次登录时自动刷新。

客户端将存储access token信息，以便后续调用OpenAPI访问和修改用户信息时使用

1. 设置用户信息保存（绑定，已经存在不绑定，注册，登录）

使用Access Token来获取用户的OpenID

使用Access Token以及OpenID来获取用户数据

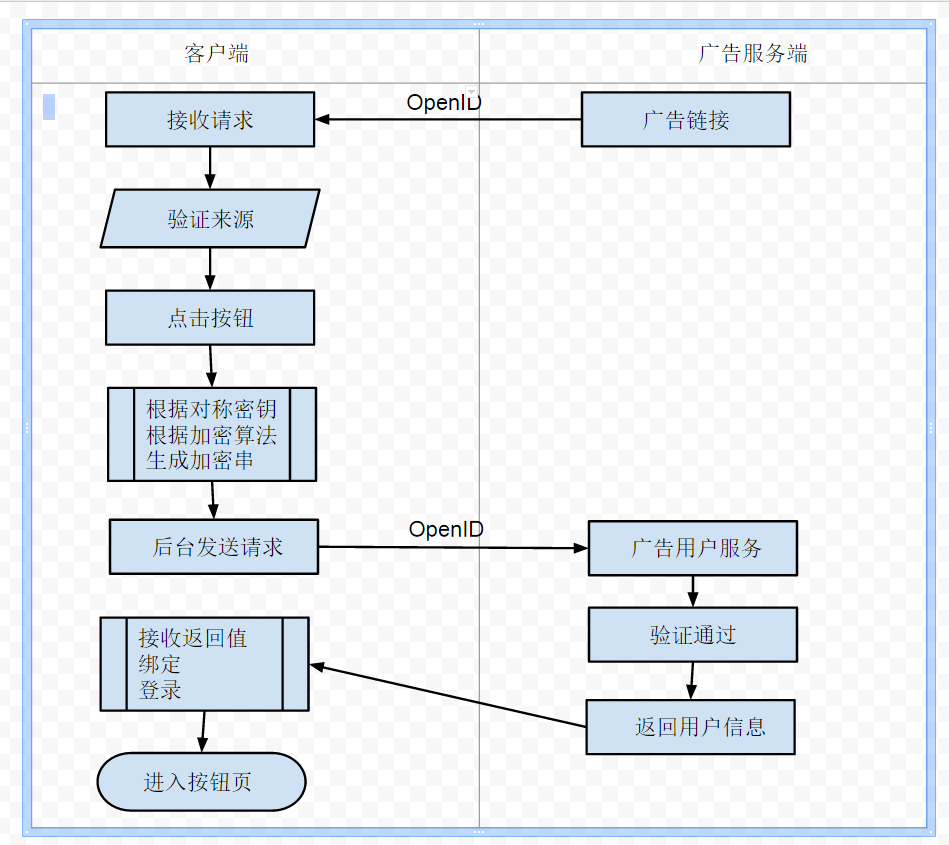
建议网站在用户登录后，即调用get\_user\_info接口，获得该用户的帐号并显示在网站上，使用户体验统一。

## 二．静默登录：

即对称密钥授权方式

服务器绑定

流程如下：



1. 广告链接，前提条件是第三方已登录过来，取得登录用户openID（或者其它能用来识别用户的标识），登录来源（即当前网址）
2. 接收链接

验证来源合法性；

接收openID 并存储在会话中，用以识别广告链接用户

1. 点击某个按钮触发

后台用对称密钥，加密算法，生成加密串 + openID，并在后台发回请求给广告用户服务

1. 广告用户服务接收请求

验证合法性

1. 验证成功

返回帐号、性别和邮箱(要求是已验证的邮箱，未验证的不予获取)；

绑定，注册；

1. 登录

登录成功，更改会话状态

1. 进入系统