它的步骤如下：

（A）用户访问客户端（包含第三方web应用），后者将前者导向认证服务器。

（B）用户选择是否给予客户端授权。（输入账号和密码）

（C）假设用户给予授权，认证服务器将用户导向客户端事先指定的"重定向URI"（redirection URI），同时附上一个授权码。（根据服务提供商的不同，url里面会有账号的唯一id，加密后的请求url地址）

（D）客户端（第三方应用）收到授权码，附上早先的"重定向URI"，向认证服务器申请令牌。这一步是在客户端的后台的服务器上完成的，对用户不可见。

（E）认证服务器核对了授权码和重定向URI，确认无误后，向客户端发送访问令牌（access token）和更新令牌（refresh token）。

下面是上面这些步骤所需要的参数。

A步骤中，客户端申请认证的URI，包含以下参数：

response\_type：表示授权类型，必选项，此处的值固定为"code"

client\_id：表示客户端的ID，必选项

redirect\_uri：表示重定向URI，可选项

scope：表示申请的权限范围，可选项 可以是 username Email等

state：表示客户端的当前状态，可以指定任意值，可选项.认证服务器会原封不动地返回这个值。(如果是你自己实现的oauth2.0服务端，可以不校验这个参数，client端就可以不管这个参数

GET /authorize?response\_type=code

&client\_id=s6BhdRkqt3

&state=xyz

&redirect\_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1

&scope username email

