**OAuth2简介**

OAuth2 协议允许用户让第三方应用访问该用户在某服务的特定私有资源

1. **OAuth2的四个重要角色**

Resource Owner：资源拥有者，即用户；

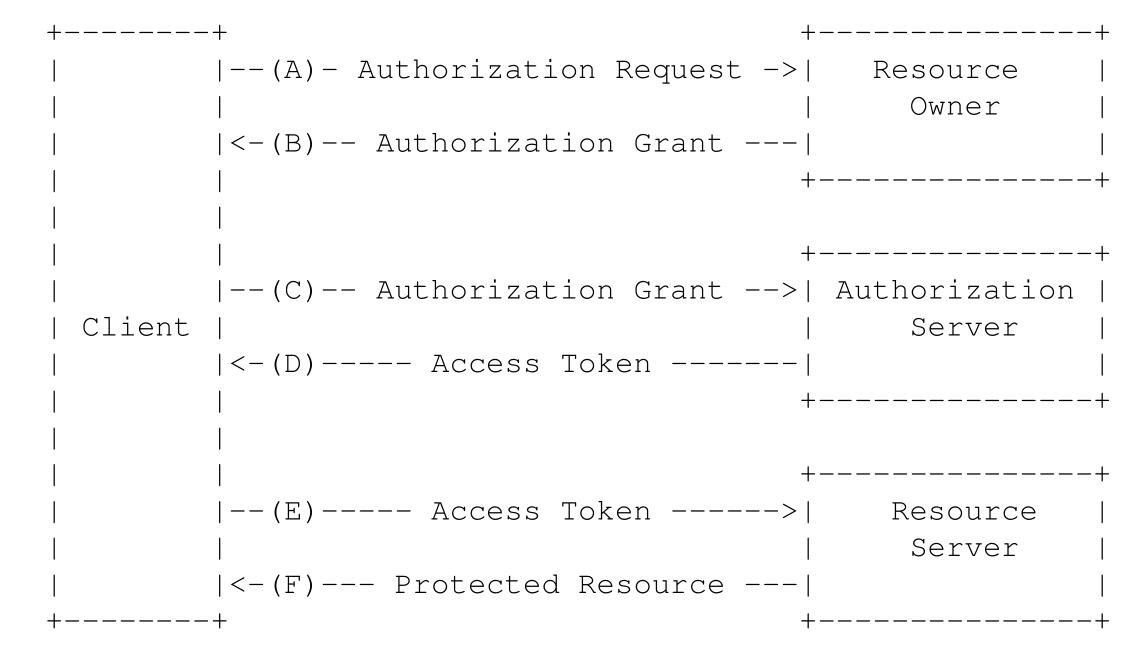
Resource Server：客户端想要访问的服务器；

Client：客户端，客户端是一个站点或者一个APP等；

Authorization Server：授权服务器

其中Authorization server和Resource server可以是独立的服务提供商，也可以是在一起的

**OAuth2的授权流程**



如下描述授权基本流程

（A）用户访问客户端，客户端向授权服务器发起授权请求；

（B）授权服务器接受客户端的授权请求，并返回授权许可给客户端；

（C）客户端使用授权许可向授权服务器发起请求；

（D）授权服务器验证客户端的身份和授权许可，发送访问令牌给客户端；

（E）客户端用访问令牌请求小明存储在资源服务器的资源（如照片等）；

（F）资源服务器根据访问令牌，返回资源信息给客户端。

客户端如何获取访问令牌，衍生出4出授权模式

Authorization Code：授权码；

Implicit：隐式许可；

Resource Owner Password Credentials：资源所有者密码凭据；

Client Credentials ：客户端凭据。

**授权模式**

1. **Authorization Code（授权码）**

授权码具体的流程如下

* 1. 用户使用浏览器访问Client站点，Client将浏览器重定向到Authorization server进行登录授权

1）Client重定向到Authorization server所需要携带的参数如下

response\_type：必选。值固定为“code”。

client\_id：必选。第三方应用的标识ID。

state：推荐。Client提供的一个字符串，服务器会原样返回给Client。

redirect\_uri：必选。授权成功后的重定向地址。

scope：可选。表示授权范围。

2）示例

GET /authorize?response\_type=code&client\_id=1&state=xyz&redirect\_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Foauth2&scope=user,photo HTTP/1.1

Host: server.example.com

* 1. Authorization server引导用户登录，并引导用户授权Client可以访问什么资源
  2. 用户授权后，Authorization server重定向回Client，并携带一个授权码

1）Authorization server会携带如下参数返回Client

code：授权码。

state：步骤1.1中客户端提供的state参数原样返回。

2）示例

HTTP/1.1 302 Found

Location: https://client.example.com/oauth2?code=SplxlOBeZQQYbYS6WxSbIA&state=xyz

* 1. Client拿授权码请求Authorization server获取用户的访问令牌

1. Client需要携带的参数

grant\_type：必选。固定值“authorization\_code”

code : 必选。Authorization Response 中响应的code

redirect\_uri：必选。必须和Authorization Request中提供的redirect\_uri相同

client\_id：必选。必须和Authorization Request中提供的client\_id相同

2）示例

POST /token HTTP/1.1

Host: server.example.com

Content-Type: application/x-www-form-urlencoded

grant\_type=authorization\_code&code=123&client\_id=1&redirect\_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Foauth2

3）示例（提供client id和client 密码）

POST /token HTTP/1.1

Host: server.example.com

Content-Type: application/x-www-form-urlencoded

Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant\_type=authorization\_code&code=SplxlOBeZQQYbYS6WxSbIA

&redirect\_uri=https%3A%2F%2Fclient.example.org%2Fcb

Authorization: Basic 为ClientID和密码的base64加密字符串

格式为 UserName:Passwd

1.5 Authorization server返回访问令牌和可选的刷新令牌以及令牌有效时间等信息给Client

1）Authorization server的信息

access\_token：访问令牌

refresh\_token：刷新令牌

expires\_in：过期时间

1. 示例

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

{

"access\_token":"2YotnFZFEjr1zCsicMWpAA",

"token\_type":"example",

"expires\_in":3600,

"refresh\_token":"tGzv3JOkF0XG5Qx2TlKWIA",

"example\_parameter":"example\_value"

}

1. **Implicit（隐式模式）**

这个是Authorization Code的简化版本。 其中省略掉了颁发授权码的过程，直接返回访问令牌和可选的刷新令牌。其适用于没有Server服务器来接受处理Authorization Code的第三方应用

其步骤就不做详细介绍了

2.1 Client发起授权请求

1）所需参数

response\_type：必选。值固定为“token”

client\_id：必选。第三方应用的标识ID

state：推荐。Client提供的一个字符串，服务器会原样返回给Client

redirect\_uri：可选。授权成功后的重定向地址

scope：可选。表示授权范围

2）示例

GET /authorize?response\_type=token&client\_id=1&state=xyz&redirect\_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Foauth2&scope=user,photo HTTP/1.1

Host: server.example.com

2.2 引导用户登录授权

2.3 授权后返回Client

1）返回信息

access\_token：访问令牌。

refresh\_token：刷新令牌。

expires\_in：过期时间。

2）示例

HTTP/1.1 302 Found

Location: http://client.example.com/oauth2#access\_token=2YotnFZFEjr1zCsicMWpAA&state=xyz&expires\_in=3600

1. **Resource Owner Password Credentials Grant（用户名密码模式）**

这种模式再一步简化，其建立在Client和授权服务器高度信任的基础上

* 1. Client要求用户填写用户名密码
  2. Client使用用户的用户名密码请求授权服务器获取访问令牌

1）请求所需参数

grant\_type：必选。值固定为“password”

username：必选。用户登陆名

passward：必选。用户登陆密码

scope：可选。表示授权范围

2）示例

POST /token HTTP/1.1

Host: server.example.com

Content-Type: application/x-www-form-urlencoded

grant\_type=password&username=blackheart&password=1234

3.3 授权服务返回访问令牌

1. **Client Credentials Grant（客户凭证授予模式）**

这种类型就更简化了，Client直接已自己的名义去访问Resource server的的资源，其不需要用户参与

4.1 客户端请求授权服务器

1）请求参数

grant\_type：必选。值固定为“client\_credentials”

scope：可选。表示授权范围

2）示例

POST /token HTTP/1.1

Host: server.example.com

Content-Type: application/x-www-form-urlencoded

grant\_type=client\_credentials

4.2 授权服务器返回访问令牌

**OAuth2刷新令牌**

Client可以使用刷新令牌在访问令牌过期前重新向授权服务器请求访问令牌

1. **所需参数**

grant\_type：必选。固定值“refresh\_token”。

refresh\_token：必选。客户端得到access\_token的同时拿到的刷新令牌。

1. **返回信息**

access\_token：访问令牌

refresh\_token：刷新令牌

expires\_in：过期时间

1. **示例**

POST /token HTTP/1.1

Host: server.example.com

grant\_type=refresh\_token&refresh\_token=tGzv3JOkF0XG5Qx2TlKWIA

**Token传递方式**

在第三方Client拿到access\_token后，如何发送给Resouce Server

如下主要有三种方式

1. **URI Query Parameter**

这种使用途径应该是最常见的一种方式，非常简单，比如：

GET /resource?access\_token=mF\_9.B5f-4.1JqM HTTP/1.1

Host: server.example.com

1. **Authorization Request Header Field**

使用Http头部Authorization字段：

GET /resource HTTP/1.1  
Host: server.example.com  
Authorization: Bearer mF\_9.B5f-4.1JqM

1. **Form-Encoded Body Parameter**

POST /resource HTTP/1.1  
Host: server.example.com  
Content-Type: application/x-www-form-urlencoded  
  
access\_token=mF\_9.B5f-4.1JqM