

# Spring Authorization Server入门 (一) 初识SpringAuthorizationServer和OAuth2.1协议

叹雪飞花 2023-06-02 👁 3,259 ⌚ 阅读6分钟

关注

## 什么是OAuth2.1?

经过近些年网络设备的不断发展，之前的oauth2.0发布的授权协议标准已经远远不能满足现在的场景和需求，根据其安全最佳实践，在oauth2.0的基础上移除了一些不安全的授权方式，并且对扩展协议进行整合。该协议定义了一系列关于授权的开放网络标准，允许用户授权第三方应用访问他们存储在另外的服务提供者上的信息。现在各三方平台提供的授权登录基本都是基于oauth协议的，例如微信、QQ、GitHub和Gitee等平台提供的授权登录。而Spring Security的团队也在社区的推动下推出了基于oauth2.1协议的授权框架：Spring Authorization Server。

## 什么是Spring Authorization Server?

Spring authorization server是由社区推动的一个项目，在Spring security团队的领导下基于Nimbus库重头编写，其目的主要是为Spring社区提供OAuth 2.0 授权服务器支持，替代已被废弃的Spring Security OAuth框架。Spring authorization server提供了OAuth 2.1和OpenID Connect 1.0规范以及其他相关规范的实现。

## Spring Authorization Server根据oauth2.1规范实现的特性列表

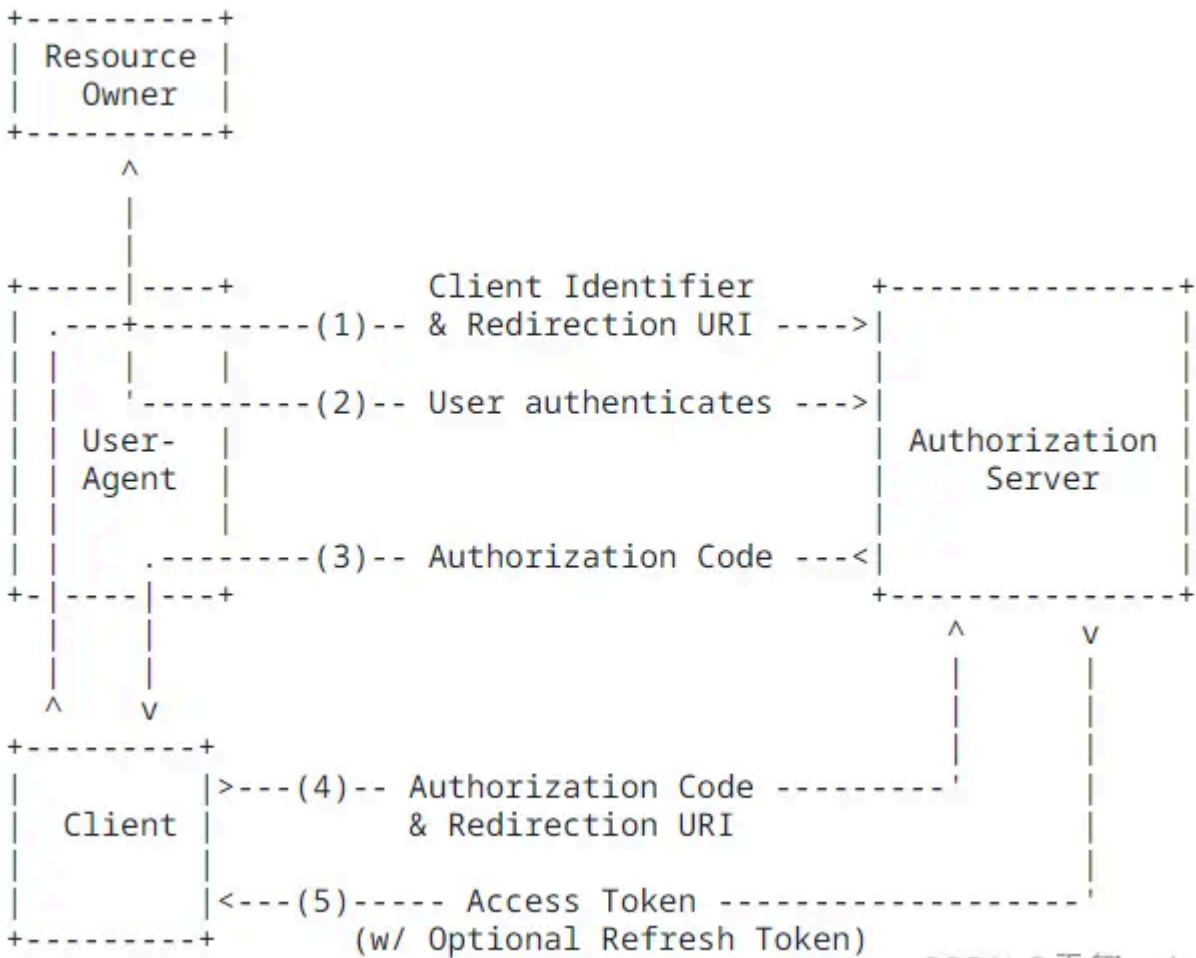
在列出特性时也会根据特性说明该特性对应的oauth2.1规范。

角色解释(摘抄自oauth2.1规范文档 [Roles](#))

1. Resource Owner：资源拥有者；能够授予对受保护资源的访问权限的实体，通常指的是终端用户。
2. Client：客户端；代表资源所有者发出受保护资源请求并获得其授权的应用程序。
3. Authorization Server：认证服务器；服务器在成功对资源所有者进行身份验证并获得授权后向客户端发出访问令牌。
4. Resource Server：资源服务器；托管受保护资源的服务器，能够使用访问令牌接受和响应受保护的资源请求。

• 授权码模式

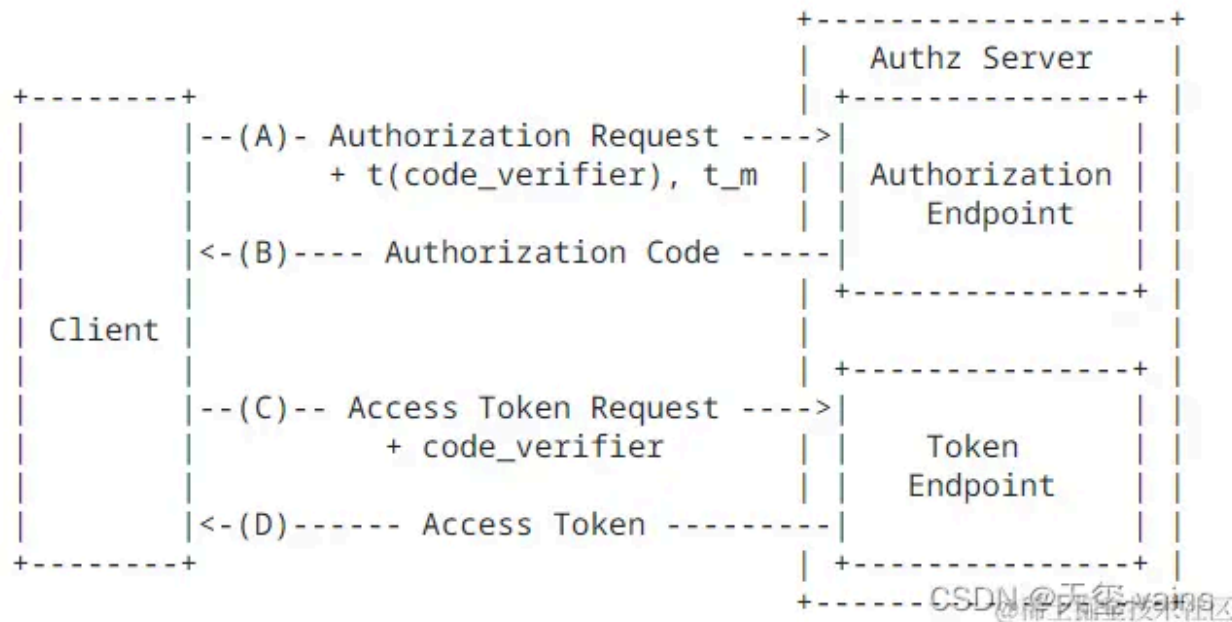
授权码模式（Authorization Code Grant）是功能最完整、流程最严密的授权模式。它的特点就是通过客户端的后台服务器，与"服务提供商"的认证服务器进行互动；流程如下



CSDN @ 天泽-vains

## 授权码扩展流程PKCE(Proof Key for Code Exchange)

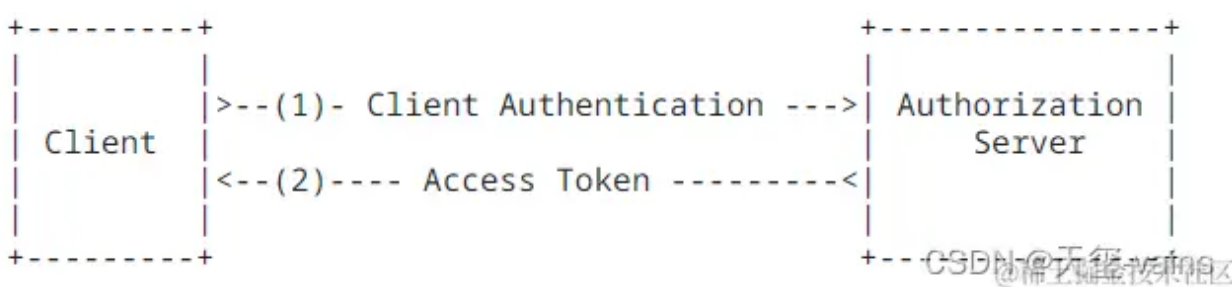
使用授权码授予的OAuth 2.0公共客户端是易受授权码拦截攻击。该流程可以减轻攻击，通过使用代码交换证明密钥来抵御威胁。客户端生成code\_verifier和code\_challenge跟认证服务器进行交互，以生成的随机认证码进行身份认证。



更详细内容请查看规范中关于PKCE的介绍. [rfc7636](#)

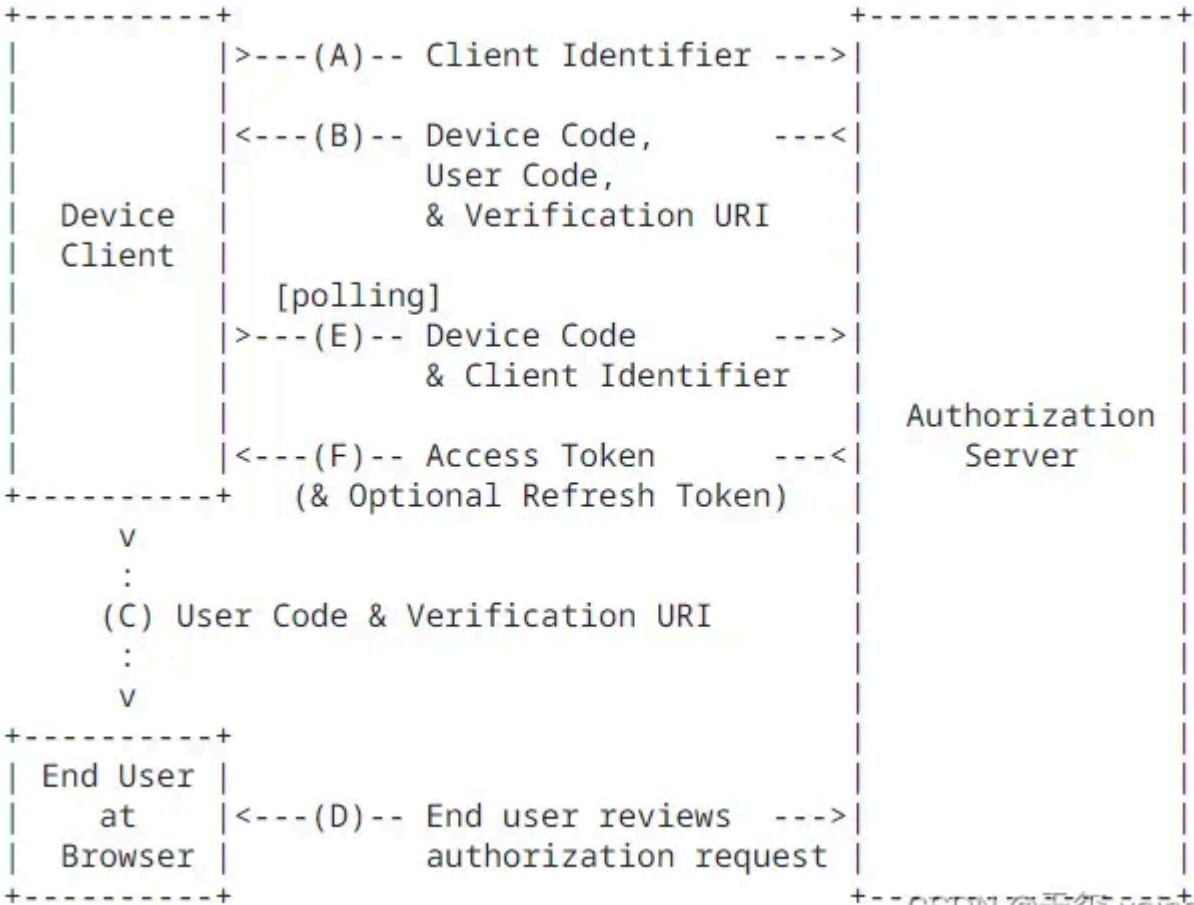
### • 客户端模式

客户端模式 (Client Credentials Grant) 指客户端以自己的名义，而不是以用户的名义，向"服务提供商"进行认证。严格地说，客户端模式并不属于OAuth框架所要解决的问题。在这种模式中，用户直接向客户端注册，客户端以自己的名义要求"服务提供商"提供服务，其实不存在授权问题；流程如下



更详细内容请查看规范中关于客户端模式的介绍.[4.2. Client Credentials Grant](#)

设备授权码模式（Device Authorization Grant）主要会出现在凭证式授权类型中，为设备代码，设备流中无浏览器或输入受限的设备提供的一种认证方式，设备会让用户在另一台设备上的浏览器中访问一个网页，以进行登录。用户登录后，设备可以获取所需的访问令牌和刷新令牌；流程如下



更详细内容请查看规范中关于设备授权码模式的介绍[rfc8628](#)

• 刷新access token

刷新令牌在获取access token时会同步获取刷新令牌(Refresh token)，如果用户访问的时候，客户端的"访问令牌"已经过期，则需要使用"更新令牌(Refresh token)"申请一个新的访问令牌。

**注意：**oauth2.1移除了隐式授权模式(Implicit grant)和密码模式(Resource Owner Password Credentials Grant)。详见oauth2.1规范中提到的“[与oauth2.0的区别](#)”和oauth2.0规范中对于“[密码模式](#)”的描述：*The resource owner password credentials grant MUST NOT be used.*

- 令牌生成器

框架提供了令牌生成器（`OAuth2TokenGenerator`），负责从提供的 `OAuth2TokenContext` 中根据 `TokenType` 类型生成对应的 `OAuth2Token`，`tokenGenerator` 很灵活，它可以支持 `access_token` 和 `refresh_token` 的任何自定义令牌格式。

- JWT [RFC 7519](#)

- JWS [RFC 7515](#)

## 客户端认证方式

### client\_secret\_basic

客户端将 `clientId` 和 `clientSecret` 通过 ‘:’ 号拼接，并使用 Base64 进行编码得到一个字符串。将此编码字符串放到请求头(Authorization)去发送请求。授权服务器通过获取请求头中的 `clientId` 和 `clientSecret` 对客户端进行认证。

### client\_secret\_post

客户端将 `clientId` 和 `clientSecret` 放到请求体(表单)去发送请求。授权服务器获取请求参数中的 `clientId` 和 `clientSecret` 对客户端进行认证。

### client\_secret\_jwt

`client_secret_jwt` 方式就是利用 JWT 进行认证。请求方和授权服务器，两者都知道客户端的 `client_secret`，通过相同的 HMAC 算法（对称签名算法）去加签和验签 JWT，可以达到客户端认证的目的。请求方通过 HMAC 算法，以 `client_secret` 作为密钥，将客户端信息加签生成 JWT；授权服务器使用相同的 HMAC 算法和 `client_secret`，对请求方的 JWT 进行验签以认证客户端。

### private\_key\_jwt

到客户端认证的目的。请求方维护了一对公私钥，通过 RSA算法，使用私钥将客户端信息加签生成 JWT；另外还通过接口暴露公钥给授权服务器；授权服务器使用请求方的公钥对请求方的 JWT进行验签以认证客户端。

## none (public clients)

当客户端是公共客户端时认证服务器不会对客户端进行验证，PKCE(Proof Key for Code Exchange)流程要求客户端为公共客户端。

## 认证服务器端点

包含OAuth2.1和Open Connect 1.0相关端点，详见官网对于端点的介绍文档

## 总结

本篇文章只是一个引子，很多地方说的很简单，大概了解了一些关于spring Authorization Server和oauth协议的相关内容，如果对某个点感兴趣可以针对性的去读一些相关的文章。

标签：Java

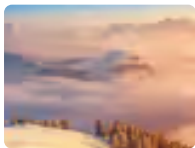
话题：我的技术写作成长之路

### 本文收录于以下专栏

◀

1 / 2

▶



Spring Authorization Server

Spring Authorization Server系列文章

176 订阅 · 25 篇文章

专栏目录

订阅

下一篇

Spring Authorization Server入门 (二) Spr...

### 评论 2



最热 最新

\_托尔的尾巴

插嘴一句， OAuth 2.0 的诞生源于传统的用户名和密码登录方式在不受信任的网站（容易明文保存用户账号密码的小网站）上会出现安全问题（说白了就是容易出现撞库问题），它的机制相当于你在不受信任的网站登录时候，使用受信任的网站的信息。举个例子，你在第三方博客登录（小网站）使用QQ（大公司，安全）登录。但Oauth2更偏向于授权，实际上如果你不勾选授权，他是无法访问到你的个人信息（头像那些），这也是为什么很多时候授权勾选个人信息的框是灰色，默认选中的原因。后续作者其他...

展开

6月前


 2

 1

...

叹雪飞花 作者：非常感谢您的补充！

6月前

 点赞

 回复

...

目录

收起 ^

什么是OAuth2.1?

什么是Spring Authorization Server?

Spring Authorization Server根据oauth2.1规范实现的特性列表

认证功能列表

授权码模式

客户端模式

设备授权码模式

刷新access token

Token生成

客户端认证方式

client\_secret\_basic

client\_secret\_post

client\_secret\_jwt

认证服务器端点

总结

相关推荐

- Spring Authorization Server入门 (三) 集成流程说明、细节补充和多种方式获取token测试  
3.2k阅读 · 7点赞
- Spring Authorization Server入门 (四) 自定义设备码授权  
2.0k阅读 · 4点赞
- Spring Authorization Server入门 (二) Spring Boot整合Spring Authorization Server  
6.5k阅读 · 31点赞
- Spring Authorization Server入门 (八) Spring Boot引入Security OAuth2 Client对接认证服务  
2.7k阅读 · 13点赞
- Spring Authorization Server入门 (十七) Vue项目使用授权码模式对接认证服务  
734阅读 · 9点赞

精选内容

- python 闭包在实际项目中的一些实现方式  
shengjk1 · 228阅读 · 2点赞
- Java和Rust之间的JSON序列化互转解决方案  
蚂蚁背大象 · 286阅读 · 0点赞
- kubectx 和 kubens工具  
运维开发笔记 · 207阅读 · 0点赞
- TikTok 被围剿："言论自由"的水下世界  
官水三叶的刷题... · 905阅读 · 6点赞
- 10 个解放双手的 IDEA插件，少些冤枉代码（第三弹）  
程序员小富 · 295阅读 · 2点赞

为你推荐

Spring Authorization Server入门 (二) Spring Boot整合Spring Authorization Server



Spring Authorization Server入门 (十二) 实现授权时候使用前后端分离的登录页面

叹雪飞花

8月前

 4.6k

 24

 65

后端

Spring ...

Spring

Spring Authorization Server入门 (十) 添加短信验证码方式登录

叹雪飞花

8月前

 3.3k

 20

 9


Spring

Spring ...

Spring Authorization Server入门 (八) Spring Boot引入Security OAuth2 Client对接认...

叹雪飞花

9月前

 2.7k

 13

 43

Spring ...

Spring

Spring Authorization Server入门 (十六) Spring Cloud Gateway对接认证服务

叹雪飞花

6月前

 2.5k

 17

 44

Spring ...

Spring ...

安全

Spring Authorization Server入门 (十三) 实现联合身份认证, 集成Github与Gitee的OAu...

叹雪飞花

7月前

 2.2k

 13

 51

Spring


Spring ...

安全

Spring Authorization Server入门 (十一) 自定义grant\_type(短信认证登录)获取token

叹雪飞花

8月前

 2.4k

 15

 39

Spring

Spring ...

安全

Spring Authorization Server入门 (七) 登录添加图形验证码

叹雪飞花

9月前

 2.8k

 18

 2

Spring ...

SpringBoot3.x最简集成SpringDoc-OpenApi

叹雪飞花

3月前

 2.2k

 16

 评论

后端

Spring ...


Java

Spring Authorization Server入门 (九) Spring Boot引入Resource Server对接认证服务

叹雪飞花

9月前

 1.8k

 13

 8

Spring

Spring ...

Spring Authorization Server优化篇: 添加Redis缓存支持和统一响应类

叹雪飞花

8月前

 1.7k

 6

 12

Spring

Spring ...

安全

Spring Authorization Server入门 (十五) 分离授权确认与设备码校验页面

叹雪飞花

7月前

 1.5k

 14

 8

Spring ...

Spring

Vue.js

Spring Authorization Server入门 (十九) 基于Redis的Token、客户端信息和授权确认信...

叹雪飞花

4月前

 1.2k

 8

 19

Spring ...

后端

Redis

Spring Authorization Server入门 (二十) 实现二维码扫码登录

叹雪飞花

1月前

 825

 16

 6

Spring ...

Spring

Java

