OAuth2.0

1. 概念

1.1 Bearer Token

> Bearer Token 是一种 Access Token ;

1.1.1 格式

Bearer XXXXXXXX

其中 XXXXXXXX 的格式 b64token。

2. 主要类

2.1 Authentication

经过 `AuthenticationManager.authenticate(Authentication)` 方法，Authentication就代表认证的主体信息；

一旦请求被认证，Authentication会被保存在SecurityContextHolder管理的线程的SecurityContext中：

> Once the request has been authenticated, the Authentication will usually be stored in a thread-local SecurityContext managed by the SecurityContextHolder by the authentication mechanism which is being used.

也可以不必通过spring-security机制，直接创建一个明确的authentication：

```
SecurityContextHolder.getContext().setAuthentication(anAuthentication);
```

`authentication.authenticated` 属性除非被设置为true，否则，authentication会一直被认证机制拦截；

杂记

- OAuth 2.0 定义Access Token 是 Resource Server 用来认证的唯一方式；

  > RFC 6749 里面只定义抽象的概念，细节如 Access Token 格式、怎么传到 Resource Server ， 以及 Access Token 无效时， Resource Server 怎么处理，都没有定义。所以在 RFC 6750 另外定义了 Bearer Token 的用法。

-