
Curso Spring Boot

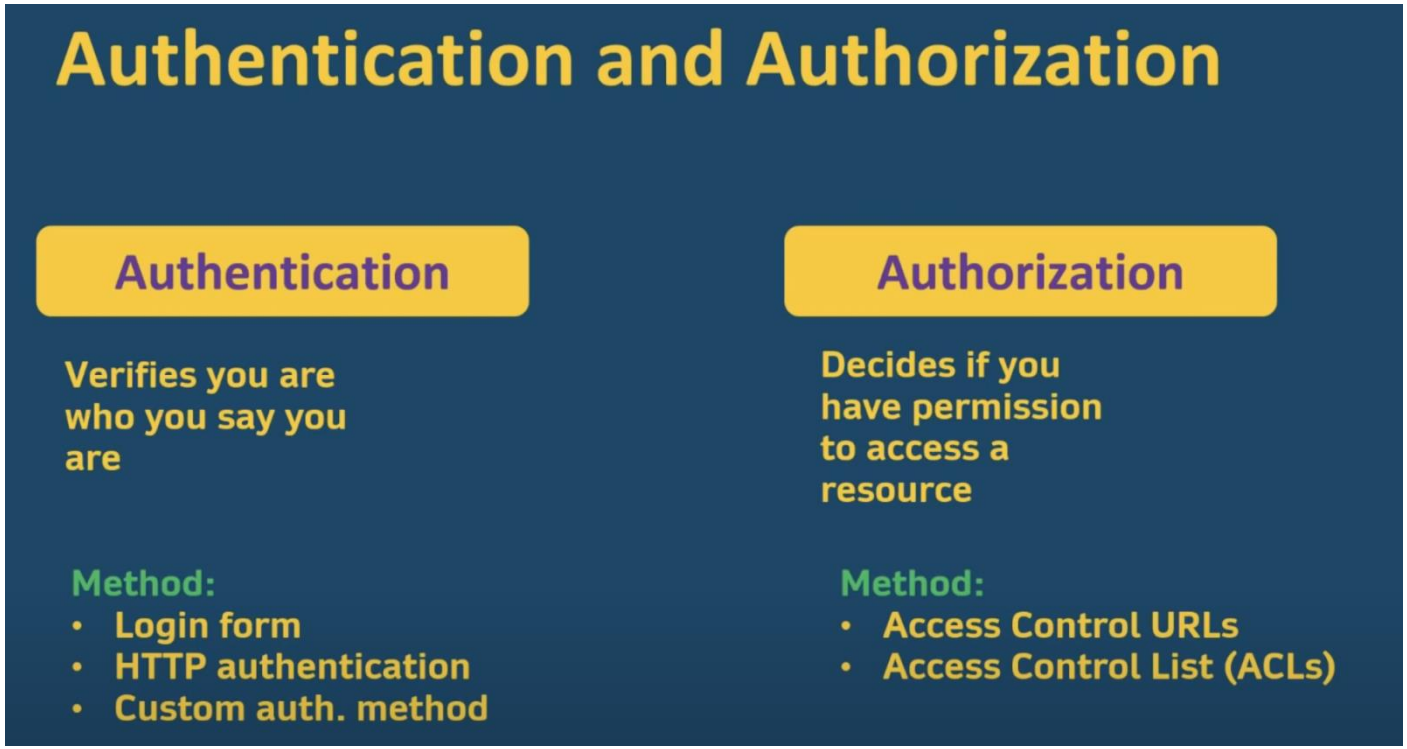
JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

JWT


Security with JSON Web Token
Client
POST/login, username/password
Application
Client
Json Web Token (JWT)
Application
Client(JWT)
GET /users, JWT
Application

Authentication and Authorization



OAuth2

- OAuth 2 es un framework de autorización, que permite a las aplicaciones obtener acceso (limitado) a las cuentas de usuario de determinados servicios, como Facebook, GitHub, Twitter, Steam, BitBucket, LinkedIn y muchos más.

- Consiste en delegar la autenticación de usuario al servicio que gestiona las cuentas, de modo que sea éste quien otorgue el acceso para las aplicaciones de terceros.

- OAuth 2 provee un flujo de autorización para aplicaciones web, aplicaciones móviles e incluso programas de escritorio.

OAuth2

- **Client**.- Es la **aplicación cliente** que quiere acceder a la cuenta de un usuario, en un servicio determinado. A fin de conseguir ello, debe contar con una autorización del usuario, y esta autorización se debe validar (a través de la API del servicio).

- **Resource Owner**.- El "dueño del recurso" es el usuario que autoriza a una aplicación, para que pueda acceder a su cuenta. El acceso está limitado en función del "scope" que concede el usuario durante la autorización.

- **Resource & Authorization Server**.- Resource server es el servidor que almacena las cuentas de usuarios, y authorization server es el servidor que verifica la identidad de los usuarios y emite access tokens a la aplicación cliente.

OAuth2

1. La aplicación cliente solicita una autorización para acceder a los recursos de un usuario, en un servicio determinado.

2. Si el usuario autoriza esta solicitud, la aplicación recibe una authorization grant (concesión de autorización).

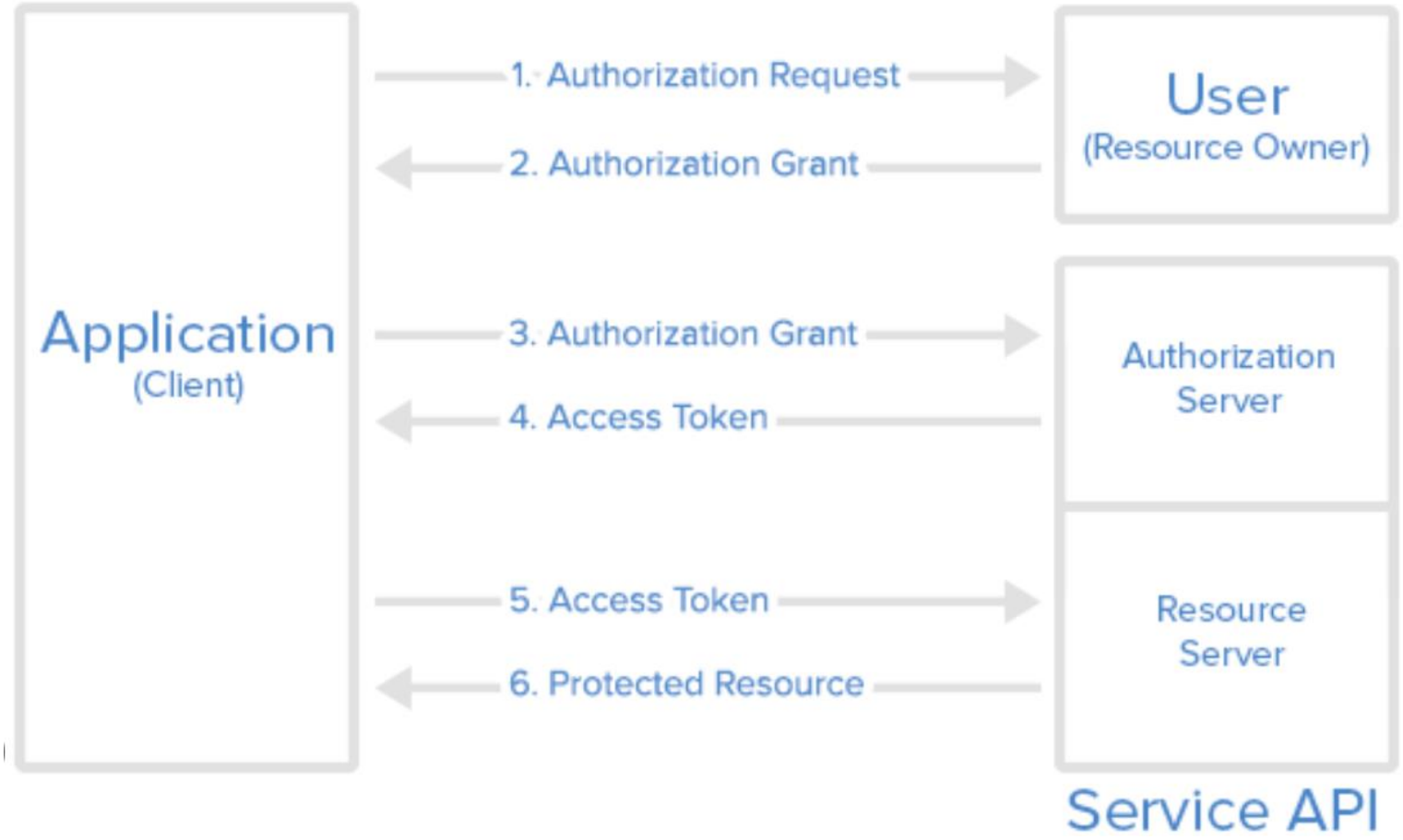
3. La aplicación cliente solicita un access token al authorization server, demostrando que es un cliente válido, y el permiso concedido anteriormente.

4. Si la identidad de la aplicación cliente se valida adecuadamente por el servicio, y la concesión de autorización es válida, el authorization server emite un access token a la aplicación cliente. Con esto la autorización se ha completado.

5. La aplicación cliente puede presentar el access token recibido en el paso anterior, y "solicitar un recurso" al resource server.

6. Si el access token es válido, el resource server hace entrega del recurso a la aplicación.

OAuth2


Application
(Client)
1. Authorization Request
2. Authorization Grant
3. Authorization Grant
4. Access Token
5. Access Token
6. Protected Resource
User
(Resource Owner)
Authorization
Server
Resource
Server
Service API