FORMADORES { IT }

Curso Spring Boot

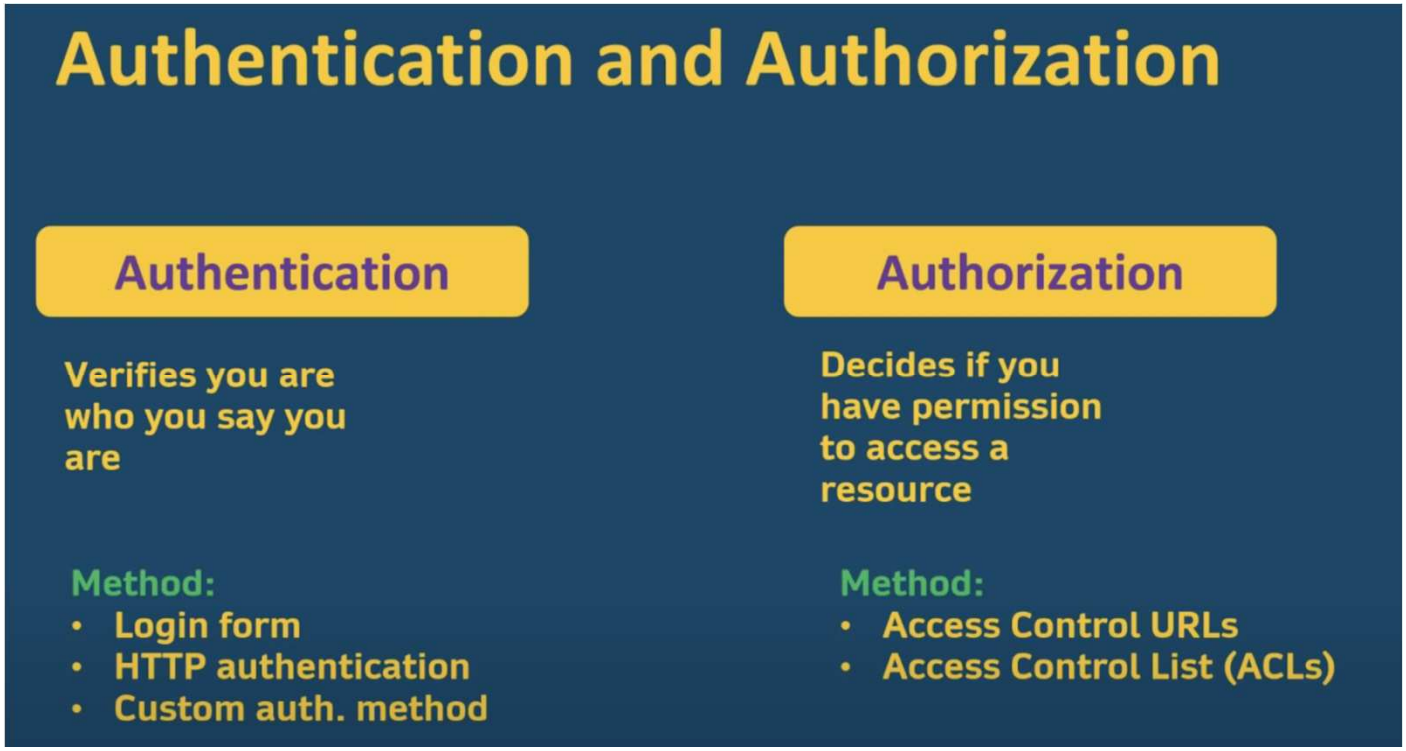
JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

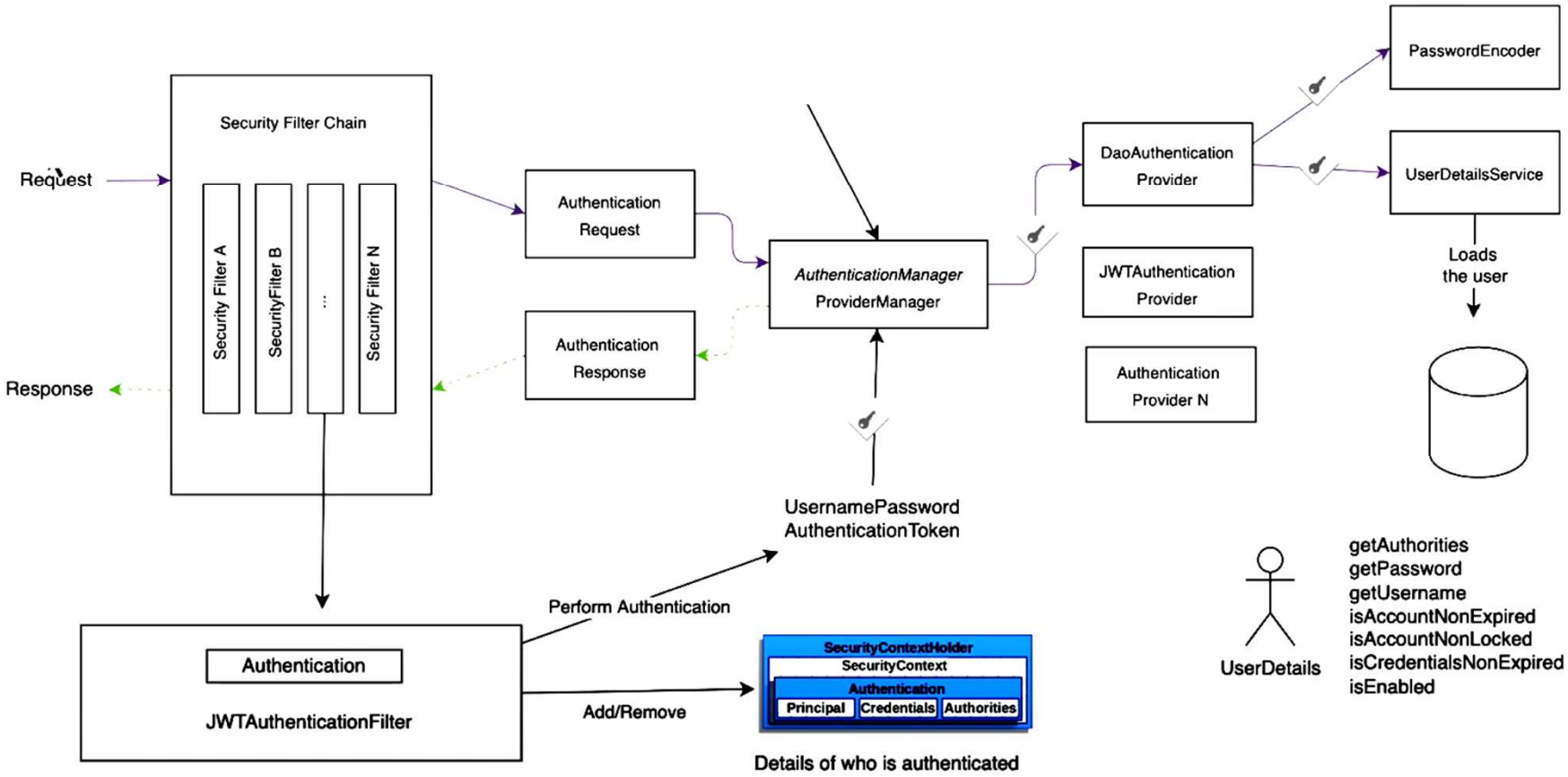
JWT


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

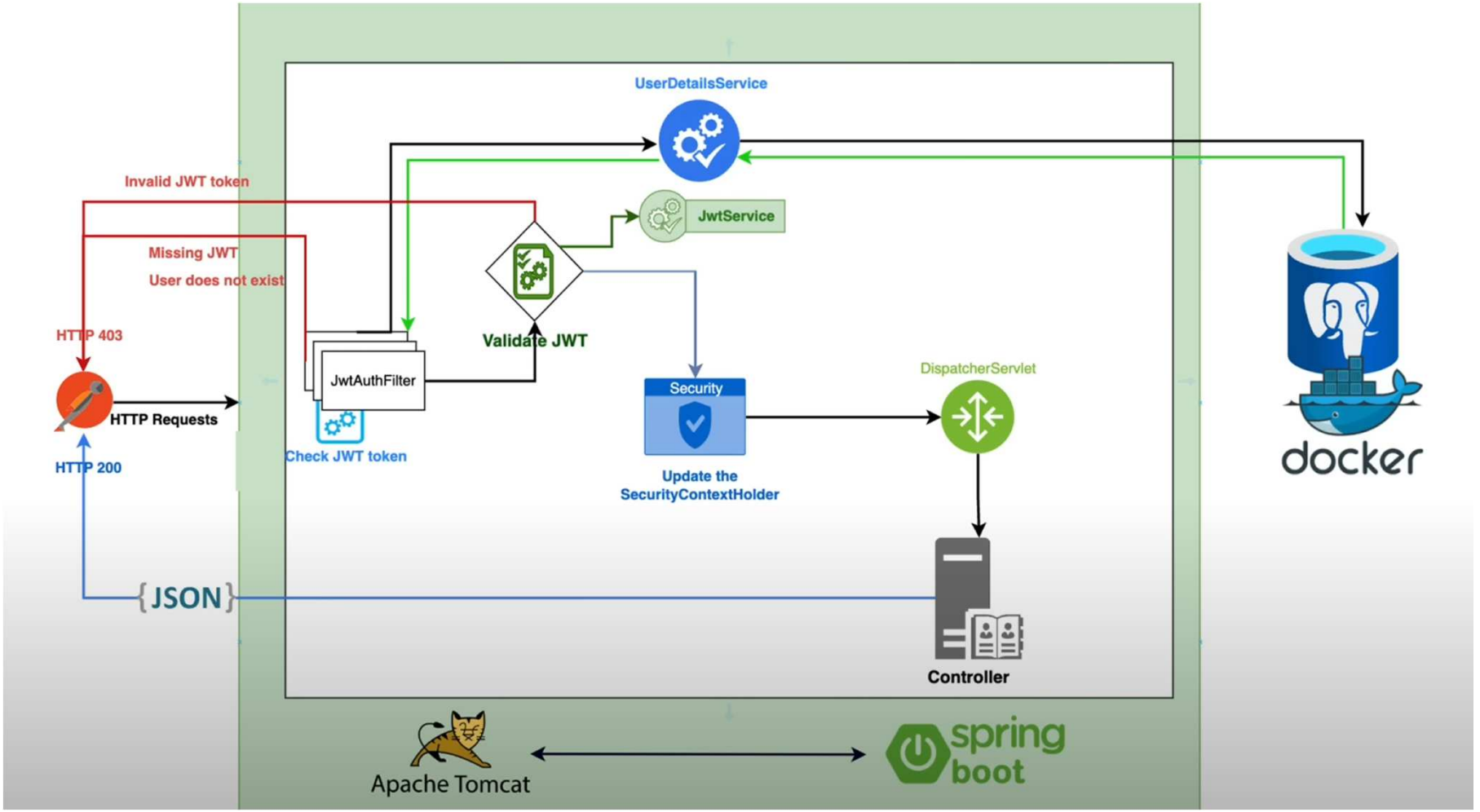
Authentication and Authorization



Arquitectura



Arquitectura



Roles presentes en OAuth

En el protocolo que define OAuth podemos identificar 4 roles.

- Client
- Resource Owner
- Resource Server
- Authorization Server

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.

FORMADORES { IT }

OAuth2