Security et JWT

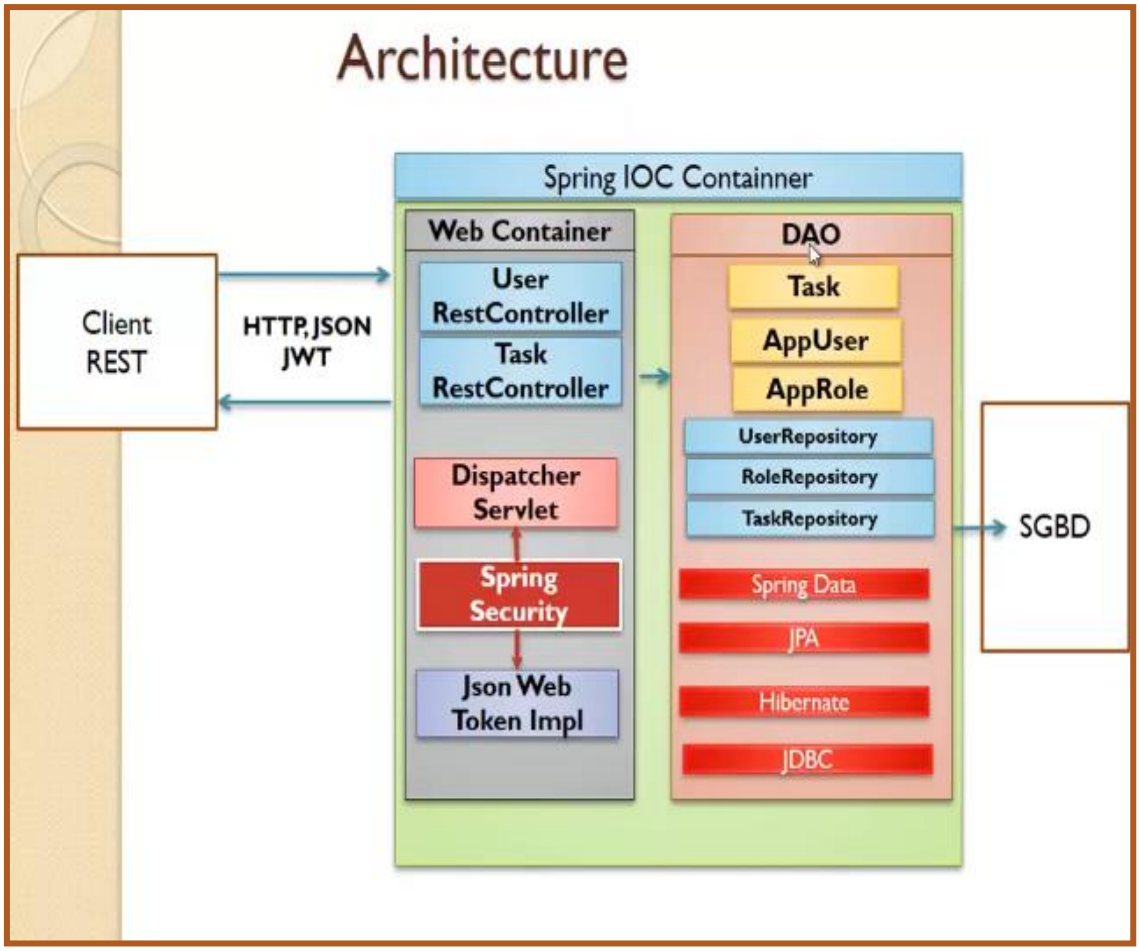
Exigences fonctionnelles :

- L' application doit permettre de
  - Gérer des tâches :
    - Ajouter une tâche, seulement si tu as le rôle ADMIN
    - Tous les utilisateurs (Rôle : ADMIN et USER) peuvent consulter les taches
  - Gérer les utilisateurs
    - Un utilisateur peut s'enregistrer afin de consulter les tâches
    - Lors de son enregistrement, il aura le rôle USER par défaut
  - Gérer les rôles (USER, ADMIN)

Exigences Techniques :

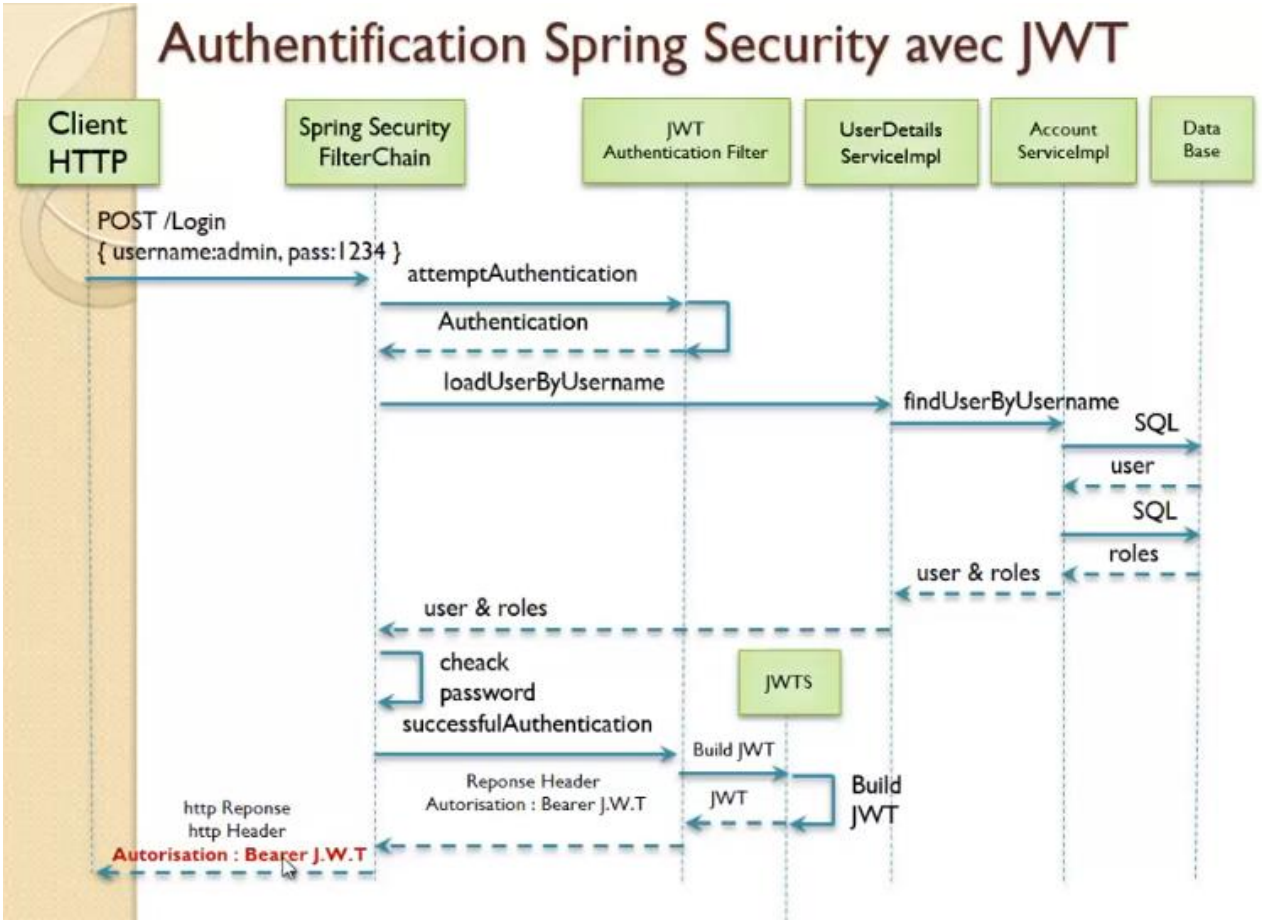
- Les données sont stockées dans une base de données H2
- L'application se compose de quatre couches :
  - La couche DAO qui est basée sur Spring Data, JPA, Hibernate et JDBC.
  - La couche Métier ou Service
  - La couche Web qui est basée sur l'API REST
  - Spring Security en utilisant l'API Json Web Token
- L'accès à l'API REST est sécurité d'une manière Statless, par Spring Security en utilisant Json Web Token.
- Pour la partie front end, on utilise Angular 6

Architecture Technique



Mise en place de deux Filtres

- Un filtre nommé **Authentication Filter** pour l'authentification :



- Un filtre nommé Autorisation Filter qui intervient à chaque demande de ressource nécessitant l'authentification.