

# Rapport de projet de JEE

par Jordan Baudin, Corentin Le Guen et Geoffrey Spaur

28 janvier 2018

---

## Contents

<b>1</b>	<b>Présentation</b>	<b>3</b>
<b>2</b>	<b>Implémentation de l'authentification</b>	<b>4</b>
<b>3</b>	<b>Implémentation du Front</b>	<b>5</b>

## 1 Présentation

Ce rapport a pour but d'apporter des réponses concernant le déroulement du projet, ainsi que sur le résultat final et nos apprentissages tout au long du projet.

## 2 Implémentation de l'authentification

### Le guide Spring

Tout d'abord, il semblait plus faisable et raisonnable d'utiliser le guide Spring sur l'authentification pour écrire sur le sujet, mais le guide a montré uniquement de simples exemples, mais aucune véritable indication de systèmes fonctionnelles, avec enregistrement d'utilisateur et connexion, sans jamais montrer de gestion de session/token. Uniquement un utilisateur rentré en dur dans le code avec un rôle.

### Notre Implémentation

Le choix a donc été de gérer les utilisateurs, rôles et tokens nous-mêmes. On ajoute donc un utilisateur lors d'une requête d'enregistrement (ou d'ajout par un administrateur, voir paragraphe sur la partie Administration), on vérifie si l'email est au bon format, si le mot de passe l'est aussi (a minima 8 caractères, une lettre minuscule, une lettre majuscule et un chiffre). Ensuite, on l'enregistre avec le rôle "USER".

Lorsqu'une personne a un compte, il peut se connecter, il recevra alors un ID token, qu'il devra donner pour chacune des requêtes qu'il fera, pour vérifier qu'il est effectivement enregistré et connecté. Lorsque le cas est échéant, on vérifiera qu'il a le rôle nécessaire pour la requête faite.

Pour modifier le rôle d'un utilisateur, il sera nécessaire de passer par l'Administration, donc seul un "ADMIN" pourra modifier ce rôle.

La gestion du token se fait dans un module statique qui stocke les tokens valables en cours, si jamais le serveur tombe, tous les tokens deviennent caduques, afin d'éviter une attaque de vol de token. Le but ici est de privilégier la re-connexion de l'utilisateur à un token qui serait valable pendant 10 ans. On invalide le token lors d'une déconnexion.

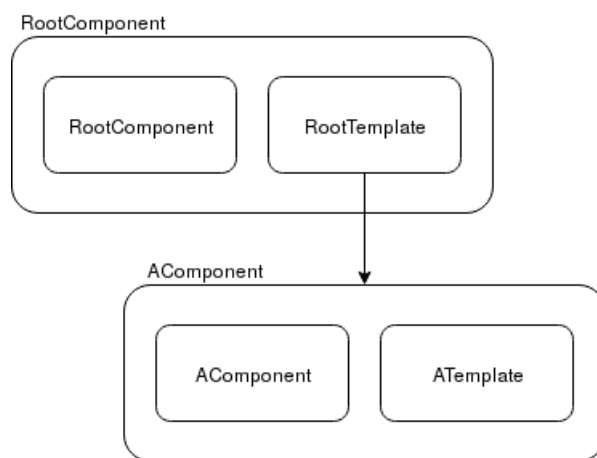
### 3 Implémentation du Front

#### Choix de la technologie

Nous avons choisi d'utiliser Angular4. Nous avons exclu Vue.js du choix des technologies car ce dernier est orienté MVVM (Modèle - Vue - Vue - Modèle), ce qui nous paraissait inapproprié au projet demandé. De plus le framework Angular4 est recommandé dans le travail en groupe car c'est un framework orienté objet.

#### Architecture en composant

Le framework Angular4 permet d'assembler un ensemble de composants entre eux. Ce framework permet de développer une application: *single page application*. Chaque composant Angular4 est composé de plusieurs fichiers permettant en architecture MVC:



Nous avons donc décomposé notre application avec ces composants:

