Application d'authentification

Application composée de deux services communiquant par protocole REST, développé en Java EE.

Ce projet à été développé au cours d'un Projet Personnel Encadré (PPE), l'application est composée de deux services, l'un permettant à l'utilisateur d'intéragir (l'Interface Homme-Machine, IHM), l'autre permettant de traiter les informations reçus de l'utilisateur, de réaliser un traitement avec les données persistantes dans la base de données et de renvoyer un message (l'authentificateur). L'application utilise une architecture client-serveur.

Le projet à été réalisé avec deux autres projets annexes, à savoir une application de journalisation et une application d'enregistrement d'utilisateurs, les trois applications sont complémentaires et permettent de répondre au contexte du projet global (Cf. contexte PPE-2016/2017).

La conception en « services » permet d'une part de répartir la charge de traitement sur les serveurs, ainsi séparer la saisie sur le formulaire, du traitement lié aux données. D'autre part, cette conception permet d'ajouter une barrière de sécurité, la base de données n'étant pas directement au contact de l'utilisateur, elle l'est au travers du service d'authentification.

Le Client – l'Interface Homme-Machine

L'interface permet à l'utilisateur de saisir un identifiant ainsi qu'un mot de passe et de valider l'envoi du formulaire. Cette application est développé en JAVA à l'aide du framework JSF (Java Server Faces). Ce Framework, permet de faire correspondre les différents champs de formulaire à une classe JAVA, et d'utiliser les boutons de soumission de formulaire pour exécuter des méthodes de classes, il permet également d'afficher les informations contenues dans la base de données sur une page web.

A ce formulaire s'ajoute un comportement AJAX, ce comportement permet d'afficher un message sous le bouton de soumission sans rafraîchissement de la page, son contenu est variable, il dépend du message que renvoi le serveur d'authentification, le message varie donc en fonction des échanges entre l'application cliente (l'IHM), et l'application serveur (l'authentificateur).

Lorsque l'utilisateur soumet le formulaire, l'échange de données entre le client et le serveur s'effectue par protocole RESTFUL.

Le Serveur – l'authentificateur

L'authentificteur est un service permettant de contrôler les informations d'authentifications fournis par des utilisateurs depuis une interface web. L'application reçoit les données par requête HTTP de type POST, utilise les données issus des attributs « login » et « password » et test l'existance de l'utilisateur.

Dans le cas ou l'utilisateur saisi n'existe pas, l'authentificateur renvoi une message d'erreur indiquant que l'utilisateur n'existe pas, dans le cas où ce dernier existe, si le mot de passe est erroné, l'authentificateur renvoi un message indiquant un mauvais mot de passe, sinon, il renvoi un message composé du nom et prénom de l'utiliateur et de son rôle (CF: contexte du PPE).

L'authentificateur utilise le framework JPA (Java Persistence API) pour la persistance des données. Ces dernières sont stockés sur une base de donnée relationnelle Derby.