Projet 2 - Technologies Internet

Aurélien Valeille – Nicolas Baillod – Kevin Kairouz – Jordan Margizian

Installation du projet

- Installer nodejs
- Dezipper le fichier du projet
- Dans un terminal, se rendre au répertoire du projet dézippé
- Installer express, jquery, bodyparser, jsonfile et node-RSA avec la commande : npm install <nom de la dépendance> --save

Utilisation du projet

Faire la commande node app.ls et aller sur localhost:3000.

Afin de pouvoir accéder à l'application, il faut se créer un compte. Sur la page sign-up, il faut se créer un nom d'utilisateur et un mot de passe. Du coté serveur, un fichier au nom de l'utilisateur est créé dans le répertoire Database/users. Il contient le nom d'utilisateur, le mot de passe, la clé publique et la clé privée. La clé privée est stockée dans le même fichier pour une question de simplicité. Tout ceci est dans un format JSON.

Il est également ajouté dans le fichier carnetAdresse contenant tous les noms d'utilisateurs avec leur clé publiques. Le carnet d'adresse sera récupéré puis affiché lorsqu'un utilisateur voudra afficher le carnet d'adresse.

L'utilisateur peut maintenant s'authentifier sur la page login et ainsi accéder à toutes les fonctions de l'application.

Afin d'écrire un mail, l'application recherche si le destinataire existe, c'est-à-dire s'il possède un fichier dans Database/users. S'il n'existe pas, il y a un message d'erreur. Le message est chiffré avec la clé publique du destinataire. Le message est ensuite enregistré dans un fichier portant le nom du destinataire dans le répertoire Database/emails.

Quand l'utilisateur clique sur « Messages reçus », la fonction de déchiffrement effectue la lecture du fichier comportant les mails de l'utilisateur afin de déchiffrer tous les messages. Les mails déchiffrés sont stockés dans le répertoire Database/emails avec le nom ….D.json. Ensuite les mails sont affichés grâce au fichier .pug situé dans le répertoire views.

Améliorations possibles

- Affichage d'information à l'utilisateur avec des boîtes de dialogue
- Trouver un moyen plus sécurisé pour stocker la clé privée
- Utiliser une communication avec les paires pour le mini-serveur
- Affichage plus ergonomique des pages messages reçus et carnet d'adresses