Projet de Programmation

Chat entre passagers de voitures

Compte rendu du 18 janvier 2024

Leo Favre
Thomas Blot
Corentin Drezen
Mouhamadou Mansour Gueye
Mohamed Larinouna

18 janvier 2024

1 Communication

Les moyens de communication pour échanger avec M. Serge CHAUMETTE sont par ordre d'importance, Rocketchat, une plateforme de collaboration sécurisée via un chat dédié pour ce projet, ou par courriel avec une adresse de l'université de Bordeaux, en mettant en copie tous les membres du groupe, et un objet devant débuté par « PdP Chat voiture ».

Les réunions seront organisées selon les besoins des membres du groupe ou du responsable du projet.

2 Mise en place initial des outils de travail

Pour collaborer au mieux, nous allons utiliser GitHub. Cet outil, dont l'utilisation a été abordée en cours de PdP, nous permettra de travailler conjointement sur le projet et de conserver un historique de son évolution.

Il faut donc créer un projet sur GitHub, en le nommant « PdP Chat voiture », et ajouter à ce projet tous les membres du groupe ainsi que le responsable du projet.

Il est également nécessaire de créer un document texte intitulé « Readme »listant tous les moyens de communication à utiliser pour ce projet, ainsi qu'un autre document faisant état des disponibilités de tous les membres du groupe.

Les rapports, comptes rendus de réunion, cahier des charges, et autres documents devront être rédigé en Latex via Overleaf. Les comptes rendus devront impérativement être nommé de la façon suivante : « 2024_01_18_CR », et les autres documents devront eux aussi, si possible, respecter ce format.

3 Travail à réaliser pour la semaine du 22 janvier 2024

La première semaine se concentrera sur le déploiement des outils de travail, la rédaction du cahier des charges incluant les points importants et moins importants du projet, ainsi que les limites. Des créneaux de travail communs seront établis selon les disponibilités des membres du groupe, avec un minimum de 2 heures par semaine recommandé.

4 Warnings

Dans ce projet, il est important de veiller à une bonne répartition du travail, mais il faut faire attention à ne pas trop diviser les taches non plus. Le respon-

sable du projet se réserve le droit lors de la notation final du projet de ne pas mettre la même note à tous les membres du groupe.

5 Première discussion sur le cœur du projet

Le but de se projet est de réaliser une application « permettant à un passager P_A d'une voiture A de chater avec un passager P_B d'une voiture B, par exemple lorsque A et B sont coincés dans un embouteillage. P_A et P_B ne se connaissent pas à l'avance, mais il faut une acceptation mutuelle de P_A et de P_B pour que la communication puisse commencer, assurant ainsi une certaine sécurité. »

Il s'agit donc d'une application qui va permettre l'échange de certificat entre client-serveur et client-client dans le but d'obtenir le numéro du destinataire.

Une première discussion à donner lieu à cette possibilité de fonctionnement de l'application :

Les usagers devront dans un premier temps échanger avec un serveur et envoyé des documents permettant de l'inscrire, l'identifier et de vérifier son identité. Nous pensons dans un premier temps comme documents d'authentification à la plaque d'immatriculation de la voiture de l'usager ainsi que de sa carte grise, et d'un numéro de téléphone liée à ces documents.

Une fois que le serveur aura validé ces documents, ils seront stockés dans une base de données. Cette opération ne se fera donc qu'une fois par l'usager.

Le serveur donnera alors à l'usager une clé privé P, une clé secrète S et chiffrera avec sa clé privé Sca l'identifiant Id de l'usager et lui transmettra aussi Sca(Id).

Lorsqu'un usager A souhaitera par la suite lancer une communication avec un usager B, il lui transmettra d'abord son identifiant chiffré par le serveur Sca(Id) ainsi que son identifié chiffré par sa propre clé privé SA(Id).

L'usager B pourra alors déchiffrer Sca(Id) grâce à la clé publique du serveur en faisait Pca(Sca(Id) pour obtenir Id, pourra déchiffrer SA(Id) grâce à la clé publique de A en faisant PA(SA(Id) pour obtenir Id.

Si B trouve que les deux identifiants déchiffrés sont identiques, c'est que A est bien l'usagé qu'il prétend être et a été validé par le serveur, B peut alors choisir d'accepter ou non la communication.

Ces étapes sont représentées sur les figures 1 et 2.

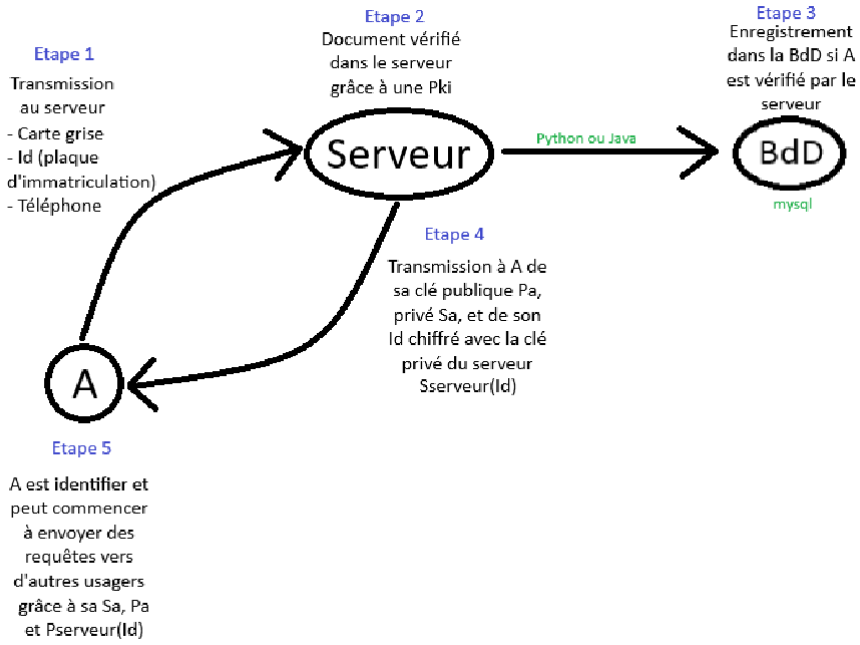

FIGURE 1 – Inscription d'un usager

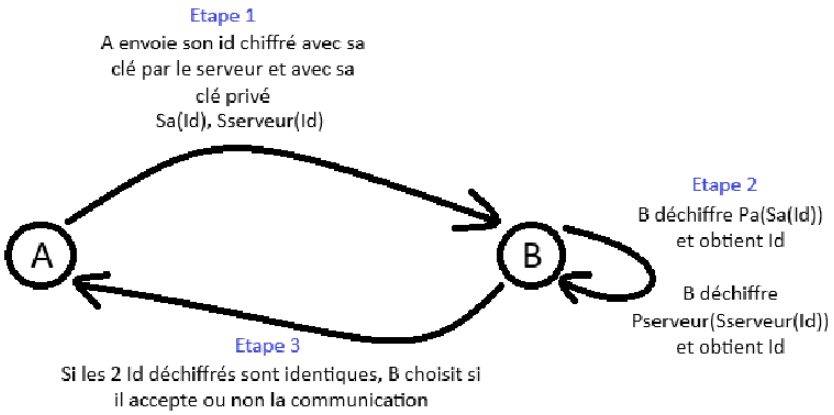

FIGURE 2 – Communication entre usagers

6 Extensions envisageables

Plusieurs extensions à l'application peuvent être envisagés :

— Une blacklist pour bloquer certains usagers déjà rencontré
— Un chat print secondaire ou un challenge comme « de quel couleur est ma voiture » pour certifié que la personne est bien proche de nous.

7 Autres informations

Si durant le projet nous avons besoin de matériel, d'accès à des sites ou licences payantes, ou de quoi que ce soit d'autres de payant, il faudra d'abord en référer aux responsables du projet. Idéalement, tout le matériel dont nous aurons besoin doit être consigné dans le cahier des charges établi au début du projet.

Le fonctionnement de notre application est susceptible de se rapprocher de celui de site de rencontre qui recommande des profils « proche »de nous, ou de Linkedin. Il peut être intéressant de comprendre le fonctionnement des algorithmes de ces sites.

C'est encore à réfléchir si une fois la communication entre deux usagers confirmé et approuvé, si le numéro de téléphone est simplement envoyé à l'autres ou si l'application proposera un service de chat depuis lequel ils parleront.

Il faudra trouver une Pki capable de certifié la validité des documents que fourniront les usagers pour créer leur profil tel que leur carte crise.