2024 - TP4

RAPPORT DÉVELOPPEMENT AVANCÉ

Mathéo BIENVENU

SOMMAIRE

1 - EXPLICATIONS DE MES CHOIX ET DIFFICULTÉS RENCONTRÉES

Etape 1 :

Au sein de cette étape, j'ai récupéré le projet comme demandé. J'ai effectué les tests de l'authentification avec les JWTs dans Postman et j'ai simplement réalisé ce que l'on m'avait demandé sans rencontrer de difficulté.

La fonction after() est exécutée après le chargement des plugins actuels et des plugins de type "register". Elle est aussi exécutée avant la méthode ready().

Etape 2 :

La seconde étape a nécessité la création d'une nouvelle clé RSA de 2048 bits, ainsi qu'un fichier CSR que nous avons signé avec notre clé privée.

L'affichage retourné par Postman à l'adresse https://localhost:4567 nous permet de consulter les informations sur notre certificat.

L'utilisation de la méthode readFileSync(), qui est synchrone, consiste à attendre que la connexion soit sécurisée. On attend donc de lire et de vérifier les clés avant d'envoyer des requêtes à mon serveur.

Si nous utilisions une fonction asynchrone pour lire les fichiers, nous risquerions d'envoyer des requêtes au serveur sans avoir établi de connexion sécurisée, ce qui entraînerait des erreurs.

Etape 3 :

Cette étape s'est révélée assez complexe. J'ai commencé par lire attentivement l'énoncé afin de m'assurer de comprendre toutes les instructions nécessaires. J'ai suivi toutes les étapes et je pense avoir correctement procédé, mais je suis confronté à une erreur que je n'arrive pas à résoudre.

Le problème survient lorsque je lance les serveurs : j'obtiens une erreur indiquant que je ne peux pas signer avec une clé publique. Lorsque je change pour utiliser la clé privée, une autre erreur apparaît, stipulant que je ne peux pas utiliser une clé privée pour vérifier. Je ne comprends pas où je pourrais avoir commis une erreur.

2 - AMÉLIORATIONS POSSIBLES

Je pense qu'une amélioration pertinente serait l'introduction d'un JWT de rafraîchissement. Cette pratique, observée dans de nombreuses applications, a déjà été intégrée avec succès dans notre projet du semestre 6 pour renforcer la sécurité de notre API. Ce système est avantageux car il maintient une expérience utilisateur fluide sans compromettre la sécurité. Cependant, je ne vois pas d'autres améliorations pour le moment.

3 - CONCLUSION

Pour conclure, j'ai trouvé ce travail pratique très instructif. Néanmoins, je suis déçu de ne pas avoir trouvé de solution au problème lié à l'utilisation des clés privées et publiques.