

Cahier des charges

Objectif

Développer une application de messagerie sécurisée, basée sur le protocole Signal, avec communication multiplateforme, synchronisation entre appareils, déploiement sur les app stores, et hébergement des serveurs chez Infomaniak.

Description du projet

L'objectif principal de ce projet est de développer une application de messagerie sécurisée qui garantit la confidentialité des messages échangés entre les utilisateurs grâce à l'implémentation du protocole Signal de chiffrement. L'application sera conçue pour fonctionner sur diverses plateformes mobiles grâce à React Native et Tauri. Elle permettra aux utilisateurs de communiquer en temps réel de manière sécurisée, de synchroniser leurs conversations entre plusieurs appareils, et d'être disponible sur les principaux app stores. De plus, l'application sera hébergée chez Infomaniak pour garantir la disponibilité et la sécurité des données des utilisateurs.

Spécifications techniques

Messagerie sécurisée

L'application doit permettre aux utilisateurs d'envoyer des messages chiffrés de bout en bout à d'autres personnes. Ce chiffrement sera assuré par le protocole Signal, qui est décrit dans plusieurs documents de la fondation, et déjà implémenté par des entreprises de sécurité informatique dans une multitude de langages.

Elle fonctionnera avec la mise en place d'un serveur WebSocket, qui permettra l'échange des messages en temps réel, ainsi qu'une API plus classique, qui permettra de gérer les comptes utilisateurs et les connexions.

Le serveur de WebSocket ainsi que l'API seront protégés par les mécanismes classiques au web (entête CORS, authentification avec jeton, chiffrement SSL).

Multiplateforme

L'application doit être compatible avec les principales plateformes mobiles (iOS / Android), ainsi que les différentes plateformes bureautiques (Windows macOS Linux). Le choix de React Native couplé à Tauri permettra de garder une seule base qui permettra ensuite de build automatiquement l'application, notamment grâce à fastlane.

Synchronisations entre différents appareils

Les conversations et les messages doivent être synchronisés de manière transparente entre les différents appareils d'un utilisateur. Le mécanisme utilisé sera celui du QR code, comme on peut retrouver sur les différentes applications de chat.

Hébergement

Les différents serveurs de l'application seront hébergés sur les serveurs / VPS de chez Infomaniak. Cette dernière étant basée sur la confidentialité des données, le choix d'un hébergeur suisse est donc crucial même pour ce projet, où les données ne seront conservées que sur le client.

Déploiement

Le déploiement de l'application sera complètement automatisé grâce à fastlane, un service acquis en 2017 par Google. Il permet le build automatique, le déploiement en accès anticipé sur les différentes plateformes mobiles (TestFlight, Play Console), la soumission sur les app stores, et il est complètement intégrable avec GitLab Runner pour autant que le serveur soit sous macOS (afin de pouvoir build pour iOS).

Budget

Hébergement Jelastic Cloud Infomaniak

L'application mobile sera hébergée sur la plateforme Jelastic Cloud d'Infomaniak. Les coûts d'hébergement débutent à partir de 20.- par mois, mais ils seront adaptables en fonction de la consommation de ressources et de la configuration sélectionnée.

Coût estimé : À partir de 20.- par mois (ajustable selon la consommation)

Licence Développeur Apple

Une licence de développeur Apple, au coût de 99 \$ par an, sera nécessaire pour accéder aux outils de développement, effectuer des tests sur des appareils réels, et soumettre l'application à l'examen d'Apple.

Coût estimé : 99 \$ par an

Licence Développeur Android

Pour la publication de l'application sur le Google Play Store, l'obtention d'une licence de développeur Android est requise. Cette licence est un paiement unique de 25 \$.

Coût estimé : 25 \$ (unique)

Runner Gitlab macOS

Un runner Gitlab macOS sera utilisé pour automatiser la construction de l'application iOS. Les coûts associés commencent à partir de 15 .- par mois, mais peuvent varier en fonction des spécifications et de l'utilisation.

Coût estimé : À partir de 15 .- par mois (variable selon les spécifications)

Références

<https://signal.org/docs/>

<https://www.infomaniak.com/en/hosting/vps-cloud>

<https://developer.apple.com/programs/>

<https://developer.android.com/google/play/licensing>