StopCovid, FANNY Protocole

FANNY

Alice et Bob installent une application utilisant le protocole d'alerte FANNY*.

FANNY est un protocole servant à faire fonctionner une application d'alerte en cas d'exposition à un risque de contamination au virus COVID-19. Cette approche décentralisée porte une attention particulière sur l'anonymat !

Initialisation

Ici, **Alice**, lance son application, deux identifiants éphémères sont créés aléatoirement par son téléphone et stockés dans ce dernier.

L'identifiant **A** et l'identifiant secret **X**.

Ces deux identifiants sont supprimés et remplacés très régulièrement !

Ici, **Bob**, lance son application, deux identifiants éphémères sont créés aléatoirement par son téléphone et stockés dans ce dernier.

L'identifiant **B** et l'identifiant secret **Y**.

Ces deux identifiants sont supprimés et remplacés très régulièrement !

Utilisation d'un UUIDv4 pour générer les identifiants aléatoirement
** Fully ANoNYmous and decentralized pandemic witness protocol*

Rencontre

Après avoir activé leur application, Alice et Bob se croisent quelques minutes.

OK A et B sont au même endroit !

Avant d'oublier leurs noms qui de toutes façons vont bientôt changer, je dois les mettre en relation !

Utilisation d'une connexion peer to peer par WebRTC
Même si le serveur web était malhonnête et décidait de retenir les identifiants de A et B cela n'aurait pas d'intérêt, car ces derniers changent en permanence et ne désignent pas leurs détenteurs de façon définitive.

Présentations

Vous êtes au même endroit !

Vous devriez entrer en relation directe !

Je vais oublier vos noms qui de toutes façons vont bientôt changer …

Même si le serveur web était malhonnête et décidait de retenir les identifiants de A et B cela n'aurait pas d'intérêt, car ces derniers changent en permanence et ne désignent pas leurs détenteurs de façon définitive.

Interaction

Bonjour **A,** mon identifiant secret est **Y**

Peux-tu utiliser **Y** pour créer un témoin de cette rencontre avant que je ne le remplace ?

Bonjour **B,** mon identifiant secret est **X**

Peux-tu utiliser **X** pour créer un témoin de cette rencontre avant que je ne le remplace ?

Création d'un témoin de rencontre (token) par concaténation de X et Y
Utilisation pour la création du token (témoin de rencontre) d'un hachag sha256
Tout se déroule sur les téléphones des utilisateurs sans l'intervention d'un tiers

Echange de témoins

Merci **A,** j'accepte ta proposition de témoin de rencontre « **X Y** » je le sauvegarde pour une durée de 15 jours.

5.2

B, je te propose le témoin de rencontre « **X Y** » acceptes-tu de t'en souvenir pour une durée de 15 jours ?

5.1

Déclaration

Quelques jours plus tard, Bob a de la fièvre !

Bob à changé d'identifiant plusieurs fois, il ne se nomme plus B mais C , pour le moment !

Je me nomme **C** Je souhaite t'informer que je suis malade, voici les témoins de toutes les personnes que j'ai pu croiser et donc exposer.

D'accord **C**, je m'en charge ! Change à nouveau de nom et supprime de ta mémoire tous les témoins de rencontre que tu viens de me transmettre, afin que personne ne puisse les relier à toi.

S'ils dépassent les 15 jours et expirent avant d'être réclamés, je les supprimerai !

Réclamation

Quelques heures après que Bob ait déclaré être malade, Alice s'interroge !

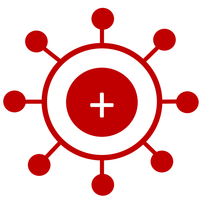
Alice à changé d'identifiant plusieurs fois, elle ne se nomme plus A mais D, pour le moment !

Je me nomme **D**. Je souhaite savoir si j'ai été exposé(e).

D'accord **D**, voici les témoins de rencontre signalés à risque de ta ville, département ou région… Qui n'ont pas encore expiré (qui ont moins de 15 jours).

Change de nom dès que possible !

Information



Parmi les témoins signalés à risque reçus j'en retrouve un « **X Y** » que j'avais sauvegardé.

J'ai donc été exposé, je peux supprimer les témoins que j'ai reçu.