SMS chiffrés avec Silence & Signal

Genma

April 16, 2017

Source :
https://www.libre-parcours.net/post/silence-ou-signal/

MERCI !!!

Les bases

Signal permet d'échanger :

- des appels vocaux chiffrés,
- des messages chiffrés,
- des SMS/MMS non chiffrés.

Silence permet d'échanger :

- des SMS/MMS chiffrés,
- des SMS/MMS non chiffrés.

Qui voit quoi ?

Silence

Lorsqu'on échange des messages via Silence, les opérateurs (de l'expéditeur et du destinataire) savent :

- qui a envoyé un message,
- à qui a été envoyé le message,
- à quelle heure.

Silence

Si vous souhaitez discuter de manière confidentielle avec une personne de sorte qu'on ne puisse jamais savoir que vous avez été en contact, n'utilisez pas Silence. Une réquisition auprès d'un des opérateurs permettra d'identifier la personne.

Les messages ne passent pas par Internet, aucun autre acteur n'est impliqué dans l'échange. C'est donc pratique pour discuter avec des gens dont vous vous foutez qu'on sache que vous leur parlez, tout en gardant une certaine confidentialité.

Signal

Dans le cas de Signal, les opérateurs qui font office de fournisseurs d'accès à Internet (soit l'opérateur téléphonique soit le FAI du réseau wifi que vous utilisez) voient que votre téléphone communique avec l'entité qui est derrière Signal : OpenWhisper Systems (OWS par la suite) et voit des échanges avec Google.

Google fournit la fonctionnalité qui permet en quelque sorte de réveiller votre téléphone pour qu'il aille vérifier auprès d'OWS qu'un message l'attend. Cela est très utile pour économiser la batterie de votre téléphone. Google ne sait pas avec qui vous communiquez ni ce que vous vous dites.

Signal

Les messages transitent par contre par OWS, l'association - fondation - entité qui édite Signal. OWS sait :

- avec qui vous communiquez,
- à quel moment,
- mais ne peut pas voir le contenu de vos échanges.

Conclusions

Conclusions

Si vous ne faites aucune confiance dans les opérateurs de votre pays, vous devriez plutôt utiliser Signal.

En revanche, cela nécessite de faire confiance dans une entité américaine (OWS) sur laquelle vous n'avez aucune maitrise.

Merci de votre attention.

Place aux questions.