

# SMS chiffrés avec Silence & Signal

Genma

May 2, 2017



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

Sources :

<https://www.libre-parcours.net/post/silence-ou-signal/>  
Mise à disposition selon les termes de la Licence Creative Commons  
BY-SA 4.0 International par Taziden.

Discussion de @Sebsauvage sur <https://framapiaf.org/@sebsauvage>  
MERCI !!!

SMS Chiffrés avec Signal ou Silence

# 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.

# Signal et les SMS 1/2

Signal, par sécurité, utilise une base de données de messages séparée de celle du système (ce qui empêche les autres applications de fourrer leur nez dans vos SMS et permet optionnellement de protéger l'application par mot de passe).

Si vous dé-installez Signal, vous perdez les messages reçus sur Signal depuis son installation. Avant de dé-installer Signal, pensez à exporter vos messages.

# Signal et les SMS 1/2

Corollaire: Après:

- avoir installé Signal.
- avoir fait de Signal l'application SMS par défaut.
- avoir importé tous les SMS de votre téléphone.

Vous pouvez supprimer tous les SMS dans l'ancienne application de SMS. Plus aucun autre logiciel ne pourra exploiter vos SMS, même en ayant l'autorisation de les lire.

# 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 maîtrise.

# Conclusions sur Signal

Signal peut envoyer n'importe quel type de fichier. Et il permet aussi de discuter de vive voix et même en vidéo (comme Skype), mais le tout bien chiffré.

# Conclusions sur Silence

Silence permet l'échange de messages chiffrés en l'absence d'accès à internet, ce que Signal ne sait plus faire (dommage !).

Silence est actuellement la seule manière d'échanger des messages chiffrés en SMS seul (sans accès internet).

Comment installer?

# Signal



## Signal Private Messenger

Super développeur

Open Whisper Systems Communication

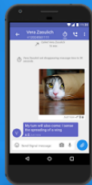
★★★★★ 129 002

PEGI 3

Ajouter à la liste de souhaits

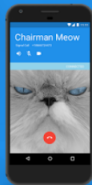
Installer

### Disappearing Messages



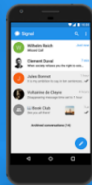
Keep your message history tidy

### Voice or Video Calls



Make crystal-clear voice or video calls from anywhere

### Stay Private



Everything is always end-to-end encrypted







# F-Droid

[Browse](#)[Forum](#)[Wiki](#)[Issues](#)[Contribute](#)[About](#)[Login](#)

## Silence

Send encrypted text messages (SMS/MMS)

Silence is an SMS/MMS application that allows you to protect your privacy while communicating with friends. Using Silence, you can send SMS messages and share media or attachments with complete privacy.

- Easy. Silence works like any other SMS application. There's nothing to sign up for and no new service your friends need to join.
- Reliable. Silence communicates using encrypted SMS messages. No servers or internet connection required.
- Private. Silence provides end-to-end encryption for your messages using the painstakingly engineered Signal encryption protocol.
- Safe. All messages are encrypted locally, so if your phone is lost or stolen, your messages are protected.

## Donate

F-Droid is powered by you

[Donate](#)[Flattr this](#)[!\[\]\(19d44b37fb4fa155bf9d60c77a3d3cb2\_img.jpg\) bitcoin](#)

15u8aAPK4jJ5N8wpWJ5guf

**Bank**

IBAN: GB92 BARC 2056

SWIFT: BARCGB

Comment l'utiliser?

# TODO

## Liste des choses à présenter - Ajouter

- Premier échange chiffré...
- Valider le correspondant via sa clef...

Merci de votre attention.  
Place aux questions.