

# Chiffrement : Whatsapp plonge 600 millions de clients en mode secret

WhatsApp aura mis six mois à concrétiser l'[implémentation](#), dans son application mobile de messagerie instantanée, du protocole de chiffrement open source TextSecure, celui-là même qu'Edward Snowden a vanté à plusieurs reprises pour son efficacité, selon nos confrères d'[ITespresso](#).

## Android au démarrage et iOS en préparation

Financé par des dons et des subventions, TextSecure est optimisé pour protéger les communications dans les systèmes de messagerie électronique asynchrone. Son développement est assuré par l'entreprise américaine Open Whisper Systems, cofondée par Moxie Marlinspike, expert en sécurité (à l'origine de plusieurs start-ups dans la sécurité dont quelques-unes rachetées par Twitter) qui en a fait son offre phare.

Dans un premier temps, le chiffrement ne sera accessible que sur Android, sans prise en charge des conversations de groupe et des messages dans lesquels se trouvent des contenus « multimédias » (autres que du texte). La feuille de route fait toutefois état du support de davantage de plates-formes – TextSecure étant disponible sur iOS et sur les principaux navigateurs web du marché – et de l'ajout d'une double vérification des clés de sécurité côté client.

WhatsApp revendiquant 600 millions d'utilisateurs, il a fallu réaliser un déploiement à grande échelle de TextSecure, en dimensionnant notamment l'infrastructure afin de résister aux pics de trafic. Côté confidentialité, le chiffrement se basant sur un jeu de clés auxquelles n'ont accès que les deux personnes qui s'échangent des messages, WhatsApp assure que les données ne peuvent pas être lues par des tiers, y compris

des autorités qui les saisiraient.

## **Des interrogations sur le ciblage des profils**

Mais ce dernier point fait débat. Le code de WhatsApp étant propriétaire, il est impossible de voir comment s'est effectuée l'intégration de SecureText. Se pose alors la question d'éventuels détournements des données personnelles, qui pourraient par exemple être collectées par... Facebook ([propriétaire de WhatsApp](#)).

Des voix s'élèvent pour réclamer le passage en Open Source du client WhatsApp afin de s'assurer que le chiffrement soit bien effectif avant que les données atteignent les serveurs. On s'inquiète également des collectes qui pourraient être effectuées « à la source », c'est-à-dire directement dans l'application, dans l'optique de profiler les utilisateurs en fonction des messages qu'ils envoient. Le flou est d'autant plus grand que la politique de confidentialité de WhatsApp n'a toujours pas été mise à jour pour dissiper ces doutes.

Enfin, une autre population risque d'être mécontente de la décision de WhatsApp, les autorités judiciaires comme le FBI qui a déjà sermonné Apple et Google pour avoir installé le chiffrement par défaut des contenus.

### **A lire aussi :**

[Chiffrement des données sur iOS 8 : juste de la poudre aux yeux ?](#)