

Olvid : après la CSPN, l'open source

Intégration MDM, interfaçage avec les annuaires d'identités, *plug-in* Keycloak pour l'IAM... Autant d'éléments qui figurent sur la feuille de route d'Olvid. Et qui traduisent la volonté de son éditeur* : pousser cette messagerie sécurisée vers les entreprises.

En ce début d'année, le logiciel bénéficie d'un coup de projecteur. Pas tant pour cette stratégie que pour la concrétisation d'une promesse : son [passage](#) en *open source*. Une démarche prévue pour 2021... et réalisée *in extremis*, le 31 décembre. Elle englobe le code source des applications mobiles (iOS, Android ; licence GPLv3) et les protocoles cryptographiques qui sous-tendent Olvid.

Pour avoir une idée du fonctionnement de ces protocoles, on pourra consulter les [spécifications techniques](#) d'Olvid. Pour une approche à plus haut niveau, il y a les rapports de [certification CSPN](#) (attribuée à la version iOS en septembre 2020 et à la version Android en mai 2021).

La CSPN iOS a pris en considération quatre éléments : authentification des utilisateurs, authentification des échanges, chiffrement des messages et des pièces jointes, chiffrement des sauvegardes du carnet de contacts. Idem sur Android, avec un élément supplémentaire : les appels VoIP. À travers ces derniers, Olvid a instauré un début de modèle économique freemium : émettre ces appels [nécessite](#) une licence payante (4,99 € TTC/mois/utilisateur ; achat *in-app*).

AWS inside

Les messages, comme les appels, sont relayés *via* un serveur hébergé chez AWS. Ce serveur assure exclusivement la mise en relation de ces communications entre contacts. Il ne récupère aucun élément d'identification. Un point-clé d'Olvid, « fondé uniquement sur la confiance mutuelle des interlocuteurs ». L'établissement de cette confiance repose notamment sur l'échange de codes.

Des clients de bureau (Windows, Mac et Linux) sont dans les cartons. Avec, nous promet-on, une synchronisation sans dispositif maître. Pour le moment, on peut utiliser une version web, à condition de disposer d'un appareil Android compatible qui servira de passerelle.

** Une start-up parisienne du même nom, à la tête de laquelle on trouve deux docteurs en cryptographie. Dont Matthieu Finiasz, par ailleurs président-cofondateur de CybelAngel.*

Illustration principale © Buida Nikita Yourievich – Shutterstock