

[Avec EKM, Box passe en mode contrôle des clés de chiffrement](#)

Finance, droit, santé, gouvernement : certaines organisations sont soumises à des obligations légales particulièrement contraignantes en matière de **protection des données**. Il s'agit bien souvent d'un obstacle majeur à la migration de leurs applications dans le **cloud**.

Tel est tout du moins l'avis de **Box**. Le spécialiste américain du stockage en ligne entend lever cette barrière grâce à une offre développée depuis 2012 en collaboration avec SafeNet (groupe Gemalto) et Amazon Web Services. Son nom : [Enterprise Key Management](#) (EKM). Sa fonction principale : proposer aux entreprises une gestion exclusive et centralisée de leurs clés de chiffrement. En instance de brevet, la solution est pour l'heure accessible en bêta. Une première version finale est prévue pour le printemps 2015, avec une échelle tarifaire qui « [dépendra] de la taille du déploiement ».

CEO et cofondateur de Box, Aaron Levie résume la philosophie d'EKM : il s'agit de maîtriser les nouveaux défis en matière de contrôle des contenus et de gestion des droits d'accès « sans entraver la collaboration, ni la productivité », rapporte nos confrères d'[l'Espresso](#).

Se différencier de l'approche HSM

A cet effet, Box se distancie de l'approche « classique » du chiffrement géré par les clients en s'appuyant sur des appliances cryptographiques – HSM, pour « Hardware Security Modules » – hébergées sur le cloud Amazon Web Services.

A l'heure actuelle, tout fichier ajouté dans un espace de stockage Box est associé à une clé unique, et ce pour chacune de ses versions. Avec EKM, toutes ces clés sont envoyées vers l'appliance, où elles sont à leur tour chiffrées avec une « clé maître » que l'entreprise est seule à posséder (Box ne peut ni la lire, ni la copier, au même titre que les journaux d'audit).

Toutes les opérations de (dé)chiffrement se font en mémoire ; jamais sur disque. Amazon gère l'initialisation des HSM SafeNet et mène régulièrement des contrôles de conformité. Un service inscrit dans le prolongement de CloudHSM, lancé en 2013 en tant que ressource au sein de l'offre Virtual Private Cloud – laquelle permet aux entreprises de constituer des environnements de cloud privé avec leurs propres infrastructures).

A lire aussi :

[Stockage Cloud : Box en piste pour une IPO le 22 janvier](#)

[Aaron Levie, Box : « le concept de localisation des données n'a pas de sens »](#)

Crédit photo : Maksim Kabakou / Shutterstock