CLOUD Act : pour AWS, la parade est dans le chiffrement des données

Outil de surveillance ? Levier d'espionnage économique ? Des voix se sont élevées dans ce sens contre le CLOUD Act.

Le 23 mars 2018, Donald Trump promulguait cette loi fédérale officiellement destinée à faciliter l'obtention de preuves numériques dans le cadre d'enquêtes criminelles.

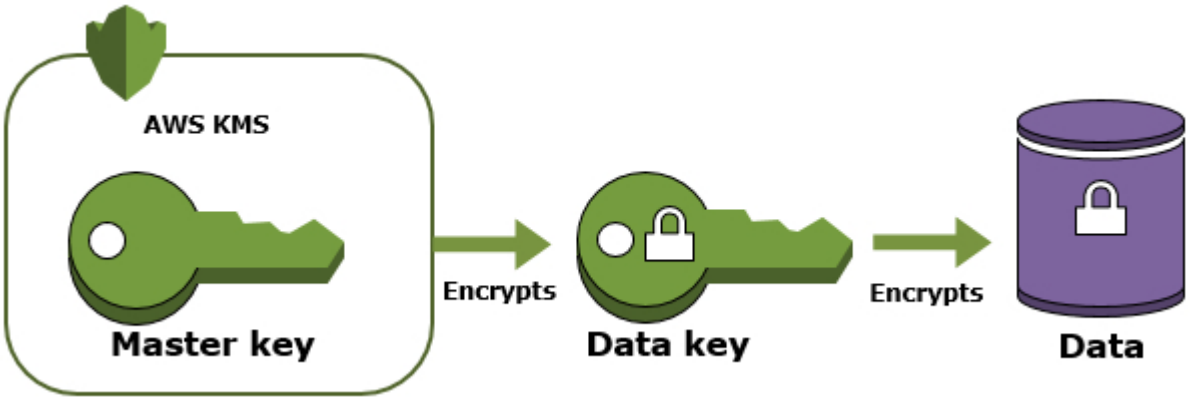
Depuis, la voie est ouverte à la signature d'accords de coopération entre gouvernements. Objectif : permettre à ces derniers de solliciter directement des prestataires de services numériques pour qu'ils leur fournissent des données, qu'importe le lieu de stockage.

Le texte ne comporte aucune disposition qui imposerait auxdits prestataires un quelconque déchiffrement des données qu'ils livrent.

AWS en fait son angle de communication. Les ressources compilées sur sa page web dédiée au CLOUD Act en témoignent pour l'essentiel. Elles mettent en avant l'offre KMS (Key Management Services)*.

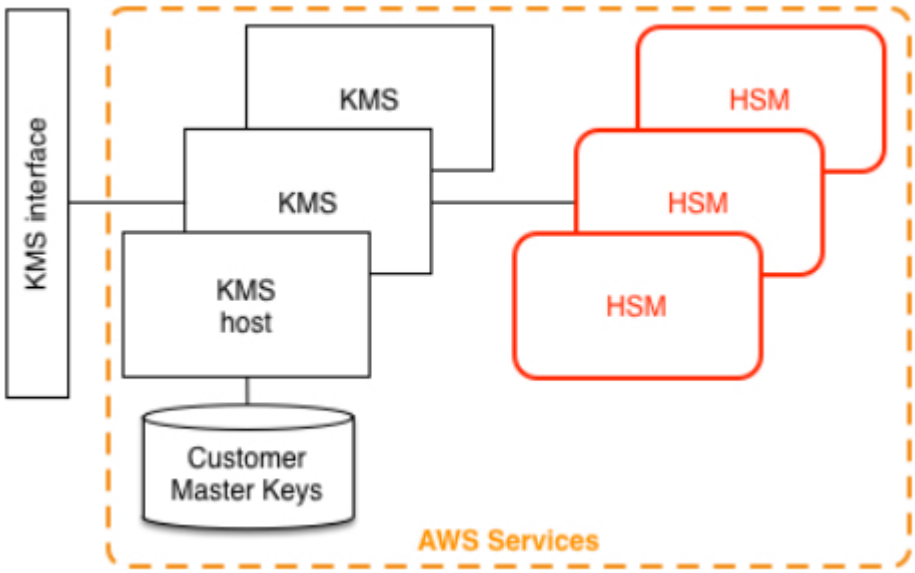
La réponse AWS : un double niveau de chiffrement

KMS permet de gérer un double niveau de chiffrement : celui des données à proprement parler et celui des clés utilisées à ces fins. C'est le principe du chiffrement « en enveloppe ».



Dans la terminologie d'AWS, les clés maîtresses (de premier niveau) sont nommées « clés principales client » (CMK). Elles sont stockées dans des modules de sécurité matériels (HSM) qu'elles ne quittent jamais sous une forme non chiffrée.

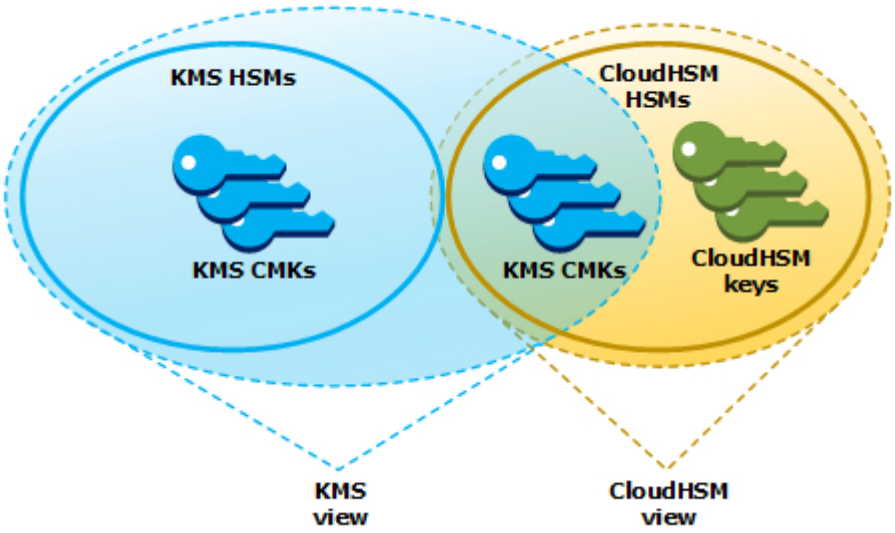
Le chiffrement d'enveloppe permet de combiner les points forts de plusieurs algorithmes. Typiquement, la rapidité des systèmes à clés symétriques et la séparation des rôles inhérente aux mécanismes à clés publiques.



Les CMK sont gérées par le client ou par AWS (ce cas se présente notamment lorsqu'on active le chiffrement côté serveur sur des ressources du cloud).

Le stockage, la gestion et le suivi des clés de deuxième niveau – dites « de données » – revient exclusivement au client.

Pour garder le contrôle des HSM qui protègent les clés principales, il est possible d'associer à KMS un magasin de clés personnalisé, dans le cadre de l'offre CloudHSM. Cas typique : la sauvegarde de clés dans différentes régions AWS.



La tarification d'un service comme KMS est minime, assure AWS. Le stockage de chaque clé principale client revient à 1 $ par mois. Il faut compter 0,03 $ pour 10 000 requêtes d'API (les 20 000 premières requêtes au cours du mois sont gratuites).

La branche cloud d'Amazon a dédié une équipe juridique à l'examen des « requêtes CLOUD Act ». Elle affirme en avoir reçu 25 ces 12 derniers mois. Aucune ne concernait la France. La plupart ont fait l'objet d'une contestation.

** Par ici, la liste des services AWS intégrés à KMS.*