virtru

Guide pratique sur la gestion des clés de chiffrement

Comprendre les méthodes de gestion des clés et les solutions de chiffrement courantes

Guide pratique sur la gestion des clés de chiffrement

Comprendre les méthodes de gestion des clés et les solutions de chiffrement courantes

Dans ce guide

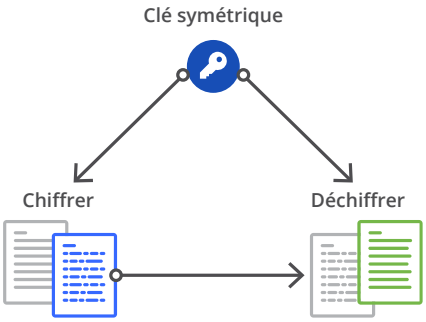
INTRODUCTION

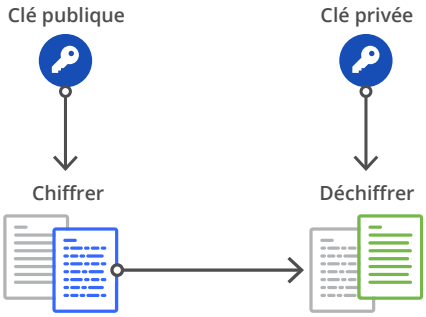
Sans chiffrement, il n'y a pas de clés. Il est donc important de savoir comment fonctionne le chiffrement moderne avant de nous intéresser au sujet plus vaste que constitue la gestion des clés.

D'un point de vue général, le chiffrement est un concept simple : le contenu sous forme de texte brut (tel qu'un e-mail ou un document) doit être protégé afin que seul le ou les destinataires visés puissent y accéder et le lire.

Pour ce faire, l'utilisation d'une clé est nécessaire afin de brouiller le texte brut en texte chiffré.
En fonction du type de chiffrement utilisé, les destinataires auront besoin d'une clé de chiffrement pour reconvertir ce texte chiffré dans sa forme originale, en texte brut.

De nos jours, deux formes de chiffrement sont couramment utilisées :





Le **chiffrement à clé symétrique** emploie la même clé pour chiffrer et déchiffrer les données. Un fichier PDF protégé par mot de passe en est un bon exemple. Le créateur de ce PDF sécurise le document à l'aide d'un code d'accès, et les destinataires autorisés utilisent ce même code d'accès pour visualiser le PDF en texte brut.

Le chiffrement symétrique peut protéger des données au repos, mais il n'est généralement pas considéré comme un moyen efficace d'envoyer en toute sécurité des données chiffrées sur différentes plateformes. Après tout, comment l'expéditeur peut-il s'assurer que la clé est transmise en toute sécurité au destinataire ?

Le **chiffrement asymétrique** a été conçu pour répondre à cette problématique. Le chiffrement asymétrique emploie deux clés : l'une pour chiffrer les données, l'autre pour les déchiffrer. Il est souvent appelé chiffrement à clé publique, car les personnes qui l'utilisent rendent publique la clé de chiffrement, mais gardent privée celle de déchiffrement.

Avec le chiffrement asymétrique, n'importe qui peut envoyer un e-mail ou un fichier chiffré à l'aide de la clé publique du destinataire, mais seul ce dernier peut le lire, puisqu'il est le seul à posséder la clé de déchiffrement privée. Le fait que plusieurs clés soient créées dans le cadre du chiffrement asymétrique complique un peu la gestion des clés.

Quel que soit le type de chiffrement employé, les clés sont nécessaires à la fois pour chiffrer et pour déchiffrer le contenu que vous protégez. Vous devez donc veiller à les sécuriser, comme vous le feriez pour le contenu lui-même.

Cela semble plutôt simple, non ? En réalité, pas tout à fait.

Dans le monde actuel, les interactions se font de plus en plus en ligne. Cela implique des risques en matière de sécurité lorsque vous devez partager des données confidentielles, notamment des clés de chiffrement. De plus, le nombre de méthodes que les organisations utilisent pour communiquer en ligne ne cesse d'augmenter.

Même si vous créez et stockez des fichiers chiffrés dans une application donnée, vous pouvez également être obligé de déplacer ces mêmes fichiers vers une autre application ou de les partager sous forme de pièces jointes à un e-mail. Une clé de chiffrement particulière peut ne pas être compatible avec certaines plateformes, ce qui vous oblige souvent à devoir gérer plusieurs échanges de clés pour une même donnée. Pour que ce processus se déroule de manière efficace, les clés de chiffrement doivent être diffusables de manière simple et sécurisée.

Nous abordons ces complexités de la même manière que la plupart des autres problèmes : nous partons du principe que nos fournisseurs de technologie les résoudront.

Pour garantir que vos données en ligne restent protégées, il est essentiel que vous compreniez les différentes composantes de la gestion des clés de chiffrement, afin de savoir quelles questions il est pertinent de poser lors de l'évaluation de technologies de chiffrement nouvelles et existantes.

Lorsque vous confiez aveuglément la gestion de vos clés à des tiers, vos informations sont exposées et susceptibles d'être consultées à votre insu ou sans votre consentement.

1

Les quatre piliers de la gestion des clés

La quantité de données volées n'a jamais été aussi importante qu'en 2018, année au cours de laquelle 4,5 milliards d'enregistrements ont été piratés rien qu'au premier semestre. En outre, le vol de propriété intellectuelle coûte jusqu'à 600 milliards de dollars aux entreprises américaines chaque année.

Bien que le chiffrement joue un rôle essentiel pour la sécurité des données, il n'est efficace que si les méthodes utilisées pour protéger et distribuer les clés le sont également. Auparavant, pour satisfaire ce principe, il était nécessaire de sacrifier la commodité d'utilisation pour préserver la confidentialité.

En matière de gestion des clés, les **quatre grands enjeux** suivants doivent être pris en compte dans tout plan global de sécurité des données :

Stockage de clés

Les fournisseurs de services de messagerie électronique et de partage de fichiers courants, tels que Microsoft, Dropbox ou Google, stockent généralement les clés de chiffrement et le contenu que ces dernières protègent sur leurs serveurs, ce qui signifie qu'ils peuvent accéder à vos données non chiffrées et les lire quand ils le souhaitent.

Par principe, il ne faut pas que la personne ou l'entreprise qui stocke votre contenu chiffré conserve également les clés chiffrant ce contenu. Il est donc recommandé de garder les clés de chiffrement séparées du contenu qu'elles protègent. Une bonne pratique connue sous le nom d'architecture à connaissance répartie, qui permet d'empêcher tout accès non désiré de tiers aux données non chiffrées.

Gestion de politiques

Bien que les clés de chiffrement soient principalement utilisées pour protéger des données, elles peuvent également être liées à des politiques permettant l'utilisation de fonctionnalités de contrôle relatives à un contenu donné. La gestion des politiques vous permet d'ajouter de telles fonctionnalités et de les ajuster.

En définissant des politiques relatives aux clés de chiffrement, le propriétaire du contenu peut spécifier quels sont les destinataires autorisés à accéder au contenu, puis révoquer les clés, faire expirer l'accès à celles-ci ou encore empêcher leur partage, ce qui rend également impossible celui des données non chiffrées. Ces politiques peuvent également vérifier à quel moment les clés de chiffrement ont fait l'objet d'un accès, permettant ainsi aux propriétaires de contenu de savoir quand leur contenu chiffré a été lu, et par qui.

Authentification

Comme les clés permettent aux utilisateurs de déverrouiller vos données chiffrées, il est important de vérifier l'identité des destinataires avant de leur octroyer l'accès à celles-ci. L'authentification est le processus consistant à vérifier que la personne tentant d'accéder au contenu est liée à la politique de la clé de chiffrement, avant d'autoriser l'accès à la clé de chiffrement et, finalement, au contenu protégé.

Certains outils, comme le portail sécurisé que votre médecin utilise peut-être pour vous transmettre des informations, vous demandent de créer un nom d'utilisateur et un mot de passe uniques afin de vérifier votre identité. Ce n'est qu'après vous être connecté que vous pouvez visualiser le contenu déchiffré.

D'autres méthodes d'authentification emploient vos identifiants Web existants, tels que ceux d'un compte Google, Microsoft ou Facebook, afin de vous authentifier. Ce type de méthode d'authentification crée une expérience plus fluide puisqu'il n'exige pas que l'utilisateur se souvienne d'identifiants de connexion supplémentaires.

Autorisation

Cette fonctionnalité procède à la vérification des actions que les utilisateurs peuvent réaliser sur des données chiffrées une fois qu'ils ont été authentifiés. L'autorisation applique les politiques relatives aux clés de chiffrement et garantit que vous gardez toujours le contrôle sur les données qui sont partagées.

Par exemple, imaginons que vous souhaitez partager un fichier chiffré avec deux personnes, mais qu'uniquement une seule d'entre elles puisse l'imprimer ou le télécharger. Vous créez donc des politiques de gestion des clés pour restreindre l'accès de l'autre personne. L'autorisation fait respecter ces règles et garantit leur bonne transmission à vos destinataires lorsqu'ils tentent d'accéder au fichier chiffré.

2

Le garant d'une confidentialité et d'une sécurité optimales

L'utilisation d'une structure de gestion des clés adaptée permet un partage des clés à la fois sûr et convivial. Une fois que vous avez compris chacun des quatre piliers, vous pouvez commencer à déterminer quel est le système de clés adéquat pour votre organisation.

En comparaison avec les autres méthodes de chiffrement, le chiffrement côté client de Virtru constitue ce qui se fait de mieux en matière de sécurité et de facilité d'utilisation.

Pour garantir la sécurité, Virtru permet aux administrateurs de surveiller les données entrant et sortant de leur domaine et de consulter les historiques d'audits correspondant aux moments où les clés ont fait l'objet d'un accès. Il leur est ainsi possible de savoir quand les e-mails ont été lus et par qui.

Stockage de clés

Les clés de chiffrement ne sont jamais stockées au même emplacement que le contenu chiffré. Ce dernier est stocké sur l'infrastructure de serveur cloud du fournisseur de la plateforme d'e-mails et de fichiers. Les clés symétriques sont hébergées sur AWS (Virtru fournit une couche d'authentification supplémentaire), tandis que les clés asymétriques peuvent être hébergées exclusivement chez les clients.

Gestion de politiques

Possibilité de révoquer des accès, de définir des dates d'expiration, d'empêcher les transferts et de tatouer des documents lors du chiffrement. Virtru peut également accéder à des historiques d'audits granulaires relatifs au contenu partagé.

Authentification

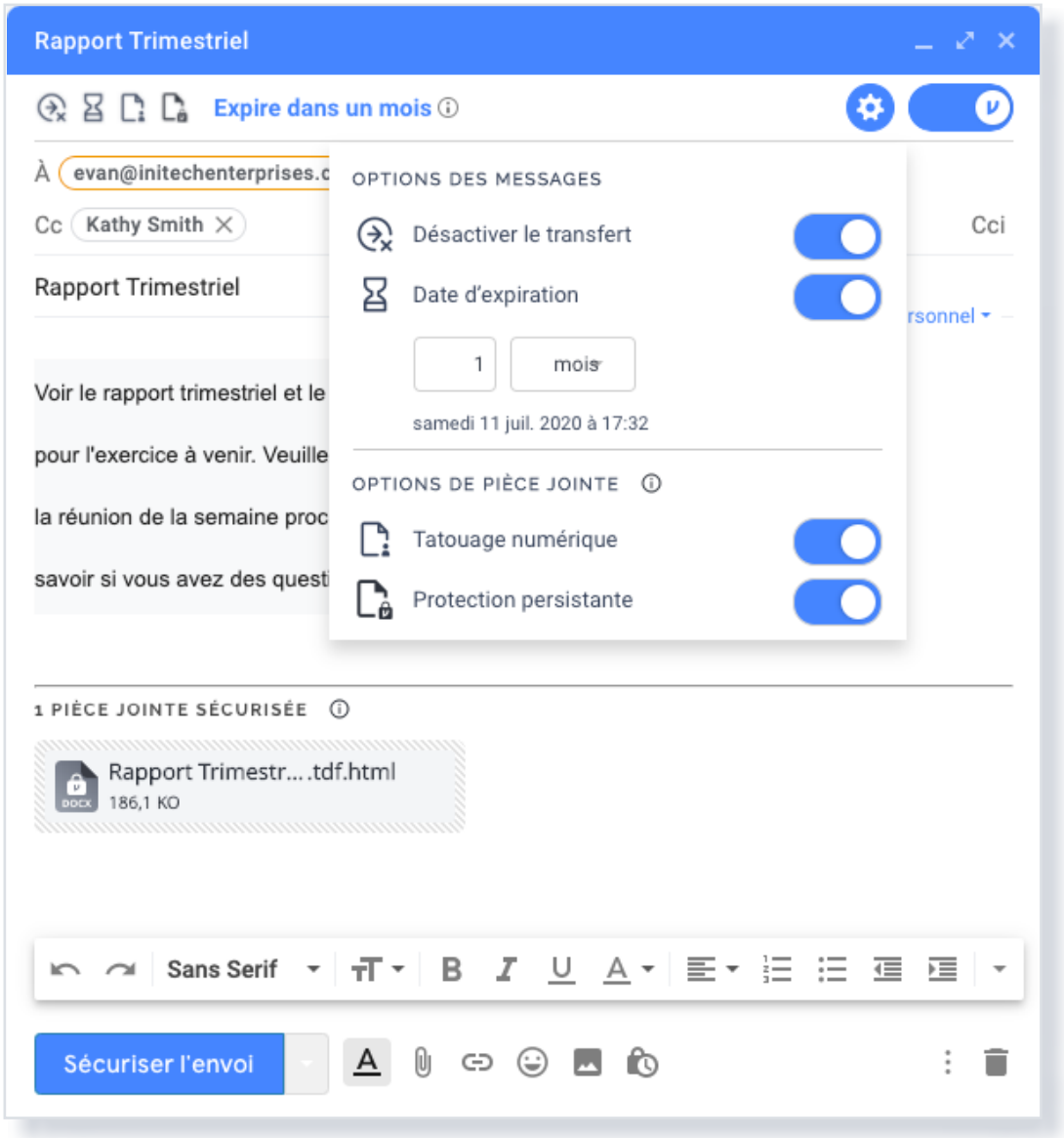
Le processus de vérification est simplifié du fait de l'utilisation des identifiants d'une adresse électronique existante ou d'un lien de vérification envoyé par message.

Autorisation

Processus géré de manière exclusive par le gestionnaire de contrôle d'accès (ACM) Virtru.

Aspect tout aussi important, Virtru garantit également une expérience totalement fluide en permettant le chiffrement directement au sein des plateformes de messagerie et de partage de fichiers existantes, telles que Gmail, Google Drive et Microsoft Outlook. Virtru se connecte facilement à ces outils pour chiffrer les données côté client, avant même qu'elles ne quittent votre appareil.

Une interface conviviale permet aux administrateurs de surveiller les données entrant et sortant de leur domaine depuis un tableau de bord centralisé, ainsi que de consulter les historiques d'audits correspondant aux moments où les clés ont fait l'objet d'un accès. Il leur est ainsi possible de savoir quand les e-mails ont été lus et par qui.



3

Trois solutions de gestion des clés

Virtru propose plusieurs options de gestion des clés pour offrir un chiffrement des e-mails et des fichiers simple d'utilisation, qui protège les données où qu'elles soient partagées et empêche les tiers d'accéder à des contenus non chiffrés. Une architecture distribuée avec un double niveau de protection permet de contrôler qui est autorisé à accéder aux clés protégeant vos données les plus confidentielles.

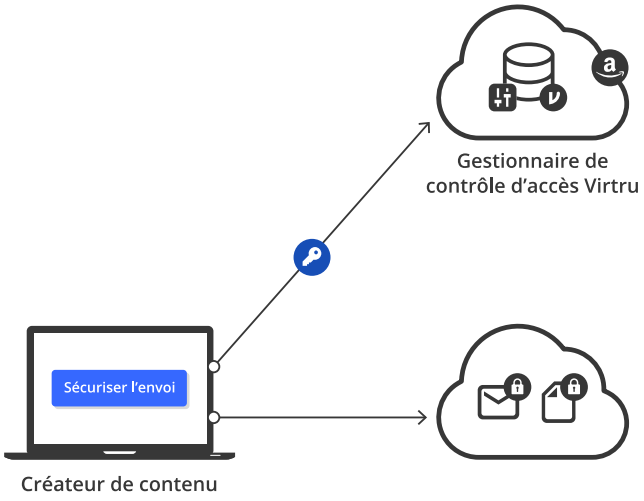
1 Clés entièrement hébergées

Grâce à notre option de gestion des clés entièrement hébergée, votre organisation est opérationnelle en quelques minutes seulement. Le gestionnaire de contrôle d'accès Virtru est au cœur de l'infrastructure de gestion des clés SaaS et entièrement hébergée de Virtru. Il gère les clés de chiffrement et les politiques de contrôle d'accès qui leur sont liées, et authentifie les demandes de clés de chiffrement pour contrôler l'accès aux e-mails et aux fichiers protégés. Le gestionnaire de contrôle d'accès (ACM) de Virtru est hébergé dans AWS pour garantir des performances et des disponibilités optimales.

Une clé de données symétrique unique, fonctionnant suivant le mode Galois/Counter AES 256 bits, est créée pour protéger les e-mails et les fichiers des clients. Elle est ensuite transmise au gestionnaire de contrôle d'accès Virtru via un canal TLS sécurisé. Le service de gestion des clés (KMS) d'Amazon renforce la protection des clés de données symétriques à l'aide d'une couche supplémentaire de chiffrement symétrique, elle-même protégée par un ensemble de modules matériels de sécurité (HSM) gérés par AWS.

Ces clés sont toutes hébergées dans des emplacements distincts, et le contenu qu'elles protègent est également stocké séparément. Cela permet d'établir une architecture à connaissance répartie dont l'importance est cruciale pour les organisations cherchant à se conformer aux exigences du RGPD, de la CNIL et de la loi FERPA qui limitent l'accès des tiers aux données confidentielles.

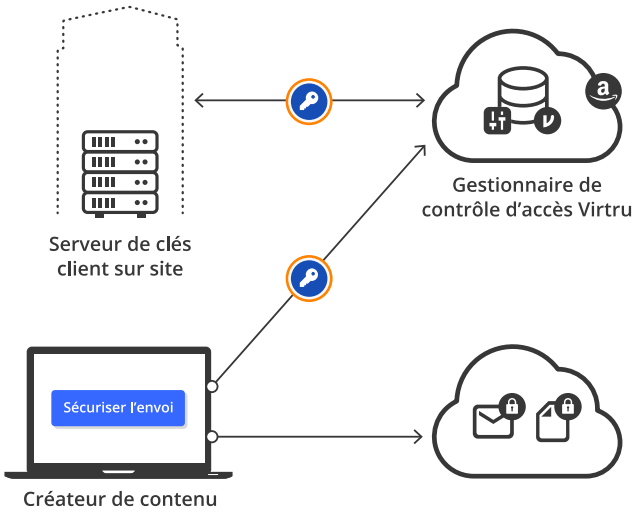
Toutefois, comme nous l'avons mentionné, le moyen le plus sûr de gérer les clés de chiffrement est de les héberger soi-même, et Virtru offre cette possibilité aux organisations via sa fonctionnalité de serveur clé client (CKS).



2 Clés hébergées par le client

Entièrement hébergé sur site, Virtru CKS ajoute une couche supplémentaire de chiffrement asymétrique et permet aux organisations de stocker et de gérer elles-mêmes les paires de clés asymétriques, ce qui leur donne un accès complet et exclusif aux clés de chiffrement de leurs données.

Cette approche a recours à des paires de clés de chiffrement asymétriques RSA 2048 bits hébergées dans votre environnement. Vos clés RSA servent à chiffrer l'ensemble des clés de données côté client afin qu'elles ne soient jamais transmises ou stockées en clair. Virtru CKS est hébergé sur site ou dans votre cloud privé et se sert de conteneurs Docker pour des déploiements rapides. Virtru CKS est utilisé conjointement au gestionnaire de contrôle d'accès Virtru pour recevoir et honorer les demandes de clés des utilisateurs autorisés.



Envisagez d'utiliser Virtru CKS si vous cherchez à :

- disposer d'un chiffrement côté client des e-mails facile à utiliser sans avoir à confier les clés de chiffrement ou le contenu non chiffré à des tiers ;
- être la seule entité pouvant répondre aux demandes d'accès et aux réquisitions judiciaires émanant des pouvoirs publics ;
- répondre aux exigences en matière de domiciliation des données en déterminant vous-même les emplacements où vos clés de chiffrement sont stockées ;
- détruire des clés de chiffrement pour rendre des e-mails définitivement illisibles.

Avant Virtru CKS, les organisations pouvaient s'appuyer sur des approches de type Bring Your Own Key (BYOK). Bien que celles-ci leur permettaient d'utiliser leurs propres clés, elles les obligeaient tout de même à confier l'hébergement des clés protégeant leur contenu à leur fournisseur de cloud ou de services de sécurité. Cela équivaut à louer un coffre-fort dans une banque mais à ensuite laisser cette dernière en détenir la clé. Dans une telle configuration, le fournisseur de services cloud ou de sécurité peut toujours accéder au contenu en texte brut sous-jacent.

Virtru est le premier service de distribution de clés de type « Zero Trust », c'est-à-dire qu'il ne permet jamais à des tiers d'accéder à des contenus non protégés ou aux clés de protection des données.

À quels types de clés et de contenus les fournisseurs de services cloud ont-ils accès ?

Configuration de la gestion des clés	Clés de protection des données	Contenu sous forme de texte brut	Clés détenues par le client
Solutions existantes de clés gérées par le client*	OUI	OUI	NON
Clés entièrement hébergées par Virtru	OUI	NON	Sans objet
Virtru CKS	NON	NON	NON

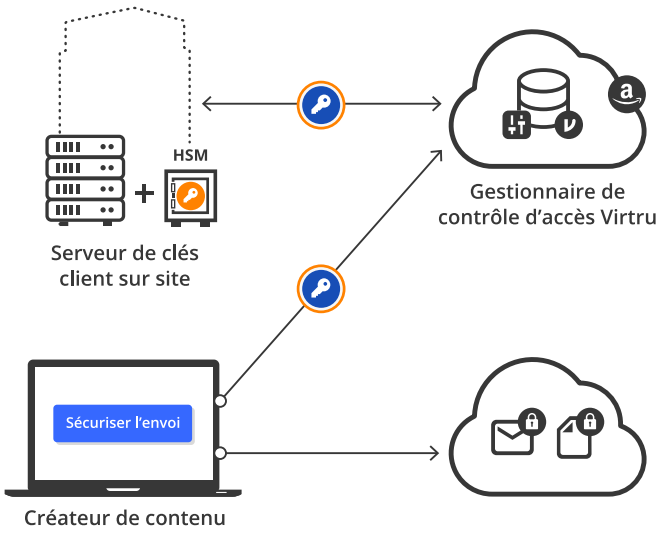
**Telles que Box KeySafe, Intralinks CMK et SafeNet KeySecure*

3 Clés HSM

Si vous avez besoin d'un niveau de sécurité supplémentaire, vous pouvez renforcer l'efficacité de Virtru CKS en utilisant un module matériel de sécurité (HSM). Un module HSM est un appareil physique hébergé sur site par une organisation, qui sert à ajouter une couche de chiffrement supplémentaire à Virtru CKS. Virtru a validé des intégrations HSM avec le module HSM TrustWay de Atos, et une large gamme d'autres modules HSM peut être activée via notre prise en charge de la norme PKCS (Public Key Cryptographic Standard) #11.

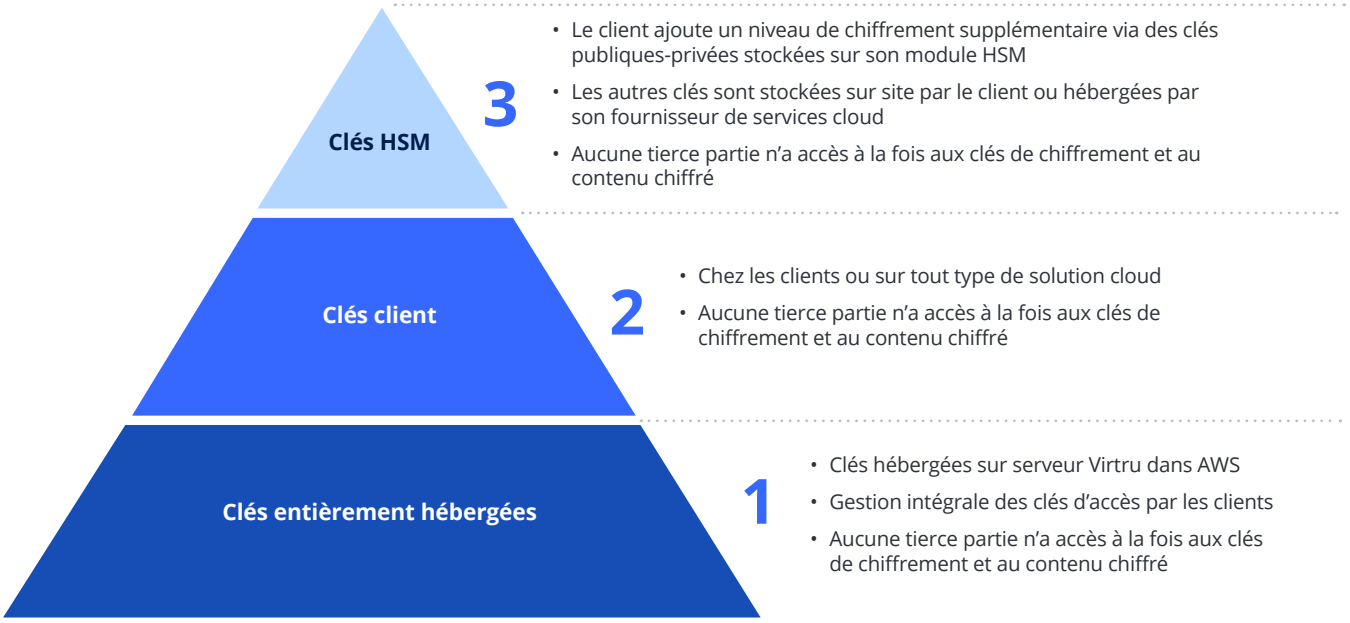
Avec cette option de déploiement, vos clés de chiffrement RSA sont stockées dans votre module HSM et Virtru CKS ne sert qu'à faciliter la communication entre le module HSM et le gestionnaire de contrôle d'accès Virtru. Sur la base du protocole de la norme PKCS #11, CKS gère les demandes de chiffrement et de déchiffrement sur la plateforme Virtru en accédant de manière sécurisée à vos clés privées gérées par le module HSM. Le gestionnaire de contrôle d'accès Virtru prend toujours en charge les workflows d'autorisation en amont.

Ce modèle est particulièrement intéressant pour toute personne souhaitant utiliser PGP ou S/MIME sans avoir à gérer manuellement les échanges de clés ou à exiger de leurs destinataires qu'ils installent un logiciel quelconque.



Que vous ayez besoin de vous conformer aux réglementations, de protéger votre propriété intellectuelle ou simplement d'empêcher des tiers d'accéder à votre contenu, les trois options de gestion des clés proposées par Virtru offrent à votre organisation une infrastructure de protection des données sûre et simple d'utilisation.

De multiples options pour renforcer la sécurité



Liste de contrôle pour l'évaluation des besoins en gestion des clés de chiffrement

Cette liste de contrôle vous aidera à évaluer les besoins de votre organisation en matière de gestion des clés de chiffrement et à déterminer quelles sont les solutions appropriées pour répondre à vos exigences :

- **Votre organisation utilise-t-elle un quelconque type de chiffrement des e-mails ou des fichiers ?**
  - Votre chiffrement protège-t-il les e-mails et les fichiers à la fois au repos et lors de leur transfert ?
  - Votre organisation utilise-t-elle le chiffrement côté client pour partager des données confidentielles ?
  - Votre fournisseur de chiffrement a-t-il déjà eu accès à des données chiffrées ?
  - Votre fournisseur de chiffrement a-t-il déjà eu accès à des clés de chiffrement ?
- **Votre organisation partage-t-elle des données auxquelles vous ne voudriez pas que votre fournisseur de services de messagerie ou de partage de fichiers accède ?**
- **Confiez-vous vos données confidentielles à vos fournisseurs de technologie ?**
- **Souhaitez-vous avoir la possibilité de répondre directement aux demandes de surveillance émanant des pouvoirs publics concernant les données de votre organisation ?**
- **Votre organisation commercialise-t-elle des produits qui sont en concurrence avec ceux de l'un de vos fournisseurs de technologie (c'est-à-dire Microsoft, Google, Amazon, etc.) ?**
- **Les employés de votre organisation ont-ils accès à des données confidentielles, comme des informations personnelles, des informations de santé protégées ou des données de propriété intellectuelle ?**
  - Si oui, votre solution de chiffrement actuelle est-elle conforme aux normes réglementaires mises en place par la loi FERPA, la CNIL, le RGPD ou la législation HDS ?
- **Votre organisation est-elle soumise à des exigences en matière de domiciliation des données ?**
  - Si oui, votre fournisseur de services cloud garantit-il que les données des e-mails et des fichiers de votre organisation ne quitteront pas vos locaux ?
- **Avez-vous besoin de savoir où vos données sont partagées en externe ?**

Améliorez la sécurité de vos e-mails et de vos fichiers dès aujourd'hui

Protégez les données de votre organisation partout où elles sont partagées et empêchez les tiers d'accéder à des contenus non chiffrés. Le chiffrement côté client des e-mails et des fichiers qu'offre Virtru est le moyen le plus sûr de respecter les exigences en matière de confidentialité, de conformité et de domiciliation des données.

Réservez une démonstration pour découvrir par vous-même notre système en action. virtru.com/fr/contact-sales

Chez Virtru, nous permettons aux organisations d'exploiter leurs données simplement tout en gardant le contrôle, quel que soit l'emplacement où elles sont stockées et partagées. À l'origine du format de données de confiance (Trusted Data Format, TDF), la norme sectorielle ouverte pour la protection des données persistante, Virtru propose des technologies de confidentialité flexibles et faciles d'utilisation fondées sur sa plateforme de protection des données qui régit l'accès aux données tout au long de leur cycle de vie : de la création au partage, en passant par la transmission, le stockage et l'analyse. Plus de 20 000 organisations de toutes tailles et de tous secteurs font confiance à Virtru pour la sécurité des données et la protection de la confidentialité. Pour plus d'informations, rendez-vous sur virtru.com/fr ou suivez-nous sur Twitter @virtruprivacy.

virtru