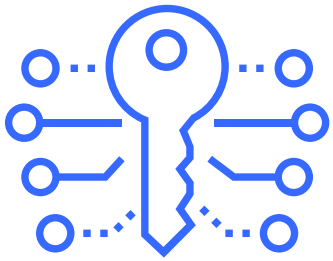
# Virtru Customer Key Server

**Obtenez une couche supplémentaire de sécurité et de confidentialité partout où vos données sont créées ou partagées, en hébergeant vos propres clés de chiffrement.**

Les entreprises souhaitent de plus en plus avoir un contrôle total de leurs données, y compris les clés de chiffrement qui protègent ces données. Toutefois, la plupart des approches BYOK (Bring Your Own Key) gérées dans le cloud ne permettent pas une stratégie Zero Trust, car elles exigent que vous fassiez confiance à un fournisseur tiers qui a accès à vos clés et votre contenu en texte brut.

**Virtru Customer Key Server (CKS) vous garantit un accès exclusif pour sécuriser vos données:**

- Créez une paire de clés supplémentaires qui ne quittent jamais votre environnement et protègent les clés de cryptage sous-jacentes pour une véritable sécurité “Hold Your Own Key”.
- Hébergez dans vos locaux, dans un cloud privé, ou sur n’importe quel service de cloud public.
- Ayez une visibilité sur tous les échanges de clés de chiffrement et politiques de sécurité.
- Intégrez votre solution SIEM pour renforcer la réponse aux menaces et la conformité.
- Empêchez tout tiers (y compris Virtru et d’autres fournisseurs de cloud, messagerie et sécurité) d’accéder à vos données.



## Des clés hébergées par le client pour une véritable confidentialité des données

### Protection de données

Hébergez vos propres clés afin que les tiers non autorisés ne puissent jamais accéder à vos données et que celles-ci restent toujours sous votre contrôle.

### Mise en conformité

Répondez aux exigences de souveraineté, de localisation et de protection des données, notamment RGPD, ITAR, HIPAA, PCI, CCPA, CJIS, etc.

### Surveillance et Prévention

Renforcez la confidentialité en vous assurant que toute demande d’accès aux données (y compris une assignation gouvernementale) doit parvenir à votre organisation.



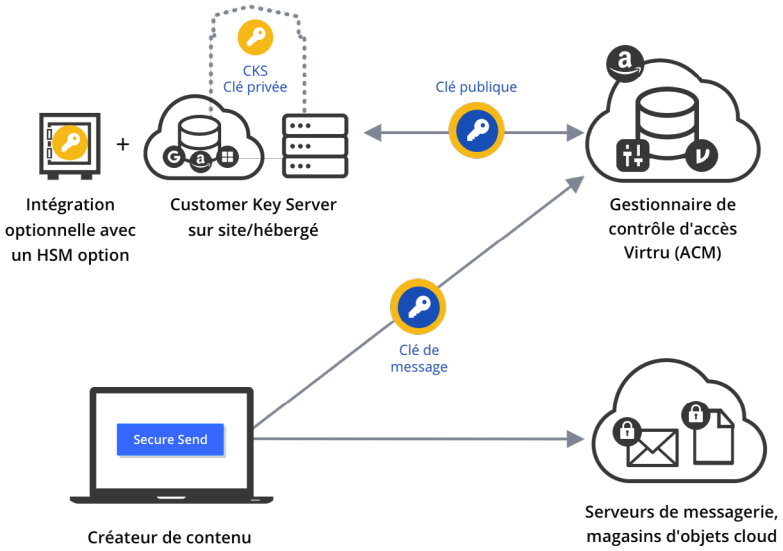
©Virtru Corporation. Tous droits réservés.

## Ce sont vos données et Virtru vous aide à ce qu'elles le restent

Virtru Customer Key Server (CKS) utilise un chiffrement asymétrique en plus du chiffrement natif de bout en bout de Virtru tout en s'alignant sur votre infrastructure informatique et de gestion de clés existante pour les implémentations à l'échelle de l'entreprise.

### Une expérience d'envoi sécurisée et privée

Lorsque vous chiffrez un email, une clé de message est générée puis chiffrée avec une clé publique. Le gestionnaire de contrôle d'accès Virtru (ACM) gère et authentifie les échanges de clés mais ne peut à aucun moment accéder à vos données. Le CKS héberge une clé privée qui est nécessaire pour déchiffrer la clé publique et accéder à la clé de message. Cette clé privée CKS ne quitte jamais votre environnement afin d'atteindre les niveaux de protection, confidentialité et conformité souhaités.




### Une expérience sécurisée mais simple pour les destinataires

Vos destinataires autorisés disposent également de paires de clés publiques / privées. Le CKS enveloppe les clés des messages avec la clé publique du client récepteur avant qu'elle ne soit transmise aux serveurs de Virtru. Le client récepteur contient la clé privée nécessaire pour accéder à la clé de message enveloppée puis déchiffrer le message. Cette expérience est transparente pour les destinataires afin d'assurer la facilité d'accès.

### Intégration du module de sécurité matériel (HSM)

Virtru Customer Key Server (CKS) gère les demandes de chiffrement et de déchiffrement sur la plate-forme Virtru et peut être intégré à votre HSM pour gérer les clés privées. Cette méthode s'appuie sur les protocoles PKCS (Public Key Cryptographic Standard) # 11 et KMIP, permettant l'intégration avec divers fabricants de HSM.

**Plus de 6 000 clients font confiance à Virtru pour la sécurité des données et la protection de la vie privée.**

NETFLIX Crédit Mutuel ARKEA wework AP éolane

virtru

Découvrez comment garantir la confidentialité avec Virtru CKS en nous contactant dès aujourd'hui sur **virtru.com/fr/contact-us**



©Virtru Corporation. Tous droits réservés.