cpl.thalesgroup.com

THALES
Building a future we can all trust

Les solutions de gestion des clés de CipherTrust Data Security Platform pour Google

Les nombreuses collaborations de Thales avec Google accélèrent la capacité des entreprises à migrer les données sensibles entre les infrastructures informatiques publiques, hybrides et privées en toute sécurité. Thales et Google offrent une gamme de fonctionnalités qui permettent aux équipes de sécurité de rester propriétaires et de contrôler leurs clés de chiffrement afin de répondre aux exigences réglementaires accrues dans le contexte de la forte dispersion de la main-d'œuvre aujourd'hui.

Aperçu des solutions de propriété et de contrôle des clés de chiffrement de Google

Google Cloud Platform (GCP) offre toute une gamme de mécanismes de gestion des clés de chiffrement contrôlés par le client. Afin de faciliter le chiffrement des données inactives et la gestion des clés en dehors de l'infrastructure Google, Google Cloud propose à la fois des clés de chiffrement contrôlées par le client (CMEK) et des modalités de gestion des clés externes (EKM). Pour chiffrer les données en cours d'utilisation à l'aide de clés qui restent résidentes dans le processeur et ne sont pas accessibles à Google, Google propose un service d'informatique confidentielle. Le service de chiffrement omniprésent des données (ou UDE pour Ubiquitous Data Encryption) de Google s'appuie sur des extensions d'EKM. Google Cloud VMware Engine s'appuie quant à lui sur le protocole KMIP (Key Management Interoperability Protocol) pour chiffrer les deux machines virtuelles et pour gérer les disques autochiffrés dans VMware VSAN. Google Workspace propose un chiffrement côté client qui protège le contenu tout en permettant au client de contrôler les clés de chiffrement des données. Les diverses solutions au sein de la plateforme CipherTrust Data Security Platform de Thales assurent la gestion des clés de chiffrement pour toute la gamme de mécanismes de gestion des clés de chiffrement contrôlés par le client de Google Cloud Platform.

CipherTrust Data Security Platform

La solution CipherTrust Data Security Platform de Thales permet aux utilisateurs de découvrir, de protéger et de contrôler les données dans Google Cloud Platform, Google Workspace, d'autres clouds et sur site, y compris dans les environnements cloud hybrides. Élément central de la plateforme, CipherTrust Manager est un système complet et centralisé de gestion des politiques de clés et de protection des données qui comprend un serveur KMIP à la pointe du secteur. CipherTrust Cloud Key Manager fournit une gestion multicloud du cycle de vie des clés de chiffrement avec une prise en charge complète de la suite Google. CipherTrust Data Discovery and Classification peut analyser à la fois Google Drive et Gmail. Il est en outre possible d'ajouter CipherTrust Transparent Encryption à l'infrastructure en tant que service (IaaS) Google Cloud Platform et des solutions telles que CipherTrust Tokenization aux solutions cloud-natives déployées sur GCP.

Les solutions KMIP de Google Cloud Platform

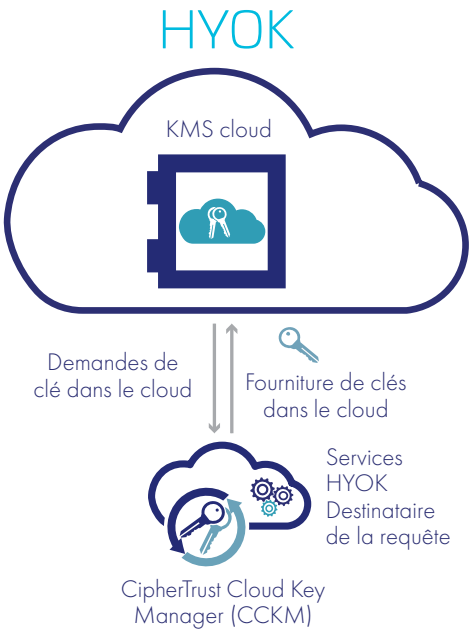
vSphere VM Encryption de VMware permet le chiffrement des machines virtuelles. VM Encryption protège les fichiers des machines et disques virtuels ainsi que les fichiers core dump en chiffrant les entrées/sorties de la machine virtuelle avant qu'elles ne soient stockées sur disque. vSAN de VMware regroupe le stockage attaché au serveur pour fournir un datastore partagé, résilient et chiffré, adapté à toute charge de travail virtualisée, y compris les applications critiques pour l'entreprise.

vSphere VM Encryption comme vSAN s'appuient sur le protocole KMIP (Key Management Interoperability Protocol) pour la gestion des clés de chiffrement et la mise en coffre des clés. Les deux solutions peuvent donc exploiter le serveur KMIP de CipherTrust Manager pour gérer de manière complète le cycle de vie des clés et la séparation des rôles.

Google prend en charge le stack VMware dans Google Cloud grâce à Google Cloud VMware Engine (GCVE). Désormais, les applications et les charges de travail conçues pour fonctionner dans VMware peuvent être migrées de manière transparente vers le cloud, avec la prise en charge de KMIP par CipherTrust Manager.

Gestion externe des clés

La modalité EKM (External Key Management) de Google Cloud Platform est un dispositif HYOK (Hold Your Own Key) de pointe, pour lequel CipherTrust Cloud Key Manager (CCKM) agit en tant que service EKM, ou EKMS. EKM prend en charge un nombre croissant de services Google Cloud Platform, que vous pouvez consulter ici. L'association d'une modalité HYOK à EKM permet au client d'être propriétaire des clés avec un pouvoir de révocation par défaut, car les clés n'existent dans Google Cloud que de manière éphémère. Pour chaque projet Google Cloud, de puissants contrôles d'accès sont mis en place. Ils sont basés sur l'octroi d'un accès granulaire (justification de l'accès aux clés [KAJ]) aux clés avant qu'elles ne puissent être utilisées.



Chiffrement omniprésent des données

La fonctionnalité de chiffrement omniprésent des données (UDE pour Ubiquitous Data Encryption) de Google comprend deux innovations majeures dans le domaine de la sécurité informatique. CipherTrust Cloud Key Manager prend en charge à la fois l'informatique confidentielle et Split Trust.

L'**informatique confidentielle**, dans le contexte d'UDE, s'appuie sur les moteurs de calcul sécurisés par matériel de Google Cloud Platform, fournissant de solides garanties de confidentialité des données en cours d'utilisation. Un aspect crucial de l'informatique confidentielle est le concept de l'attestation : la capacité à vérifier qu'un environnement distant est protégé et adapté en vue de la transmission de données sensibles et/ou de clés. Dans le contexte d'UDE, l'attestation permet de vérifier à distance que certaines instances de calcul de Google Cloud Platform fonctionnent avec des protections informatiques confidentielles sécurisées par matériel.

En soutien à l'informatique confidentielle, CipherTrust Cloud Key Manager peut vérifier les attestations. Les règles d'accès aux clés sont désormais assorties d'exigences en matière d'informatique confidentielle ; dans ce cas, les demandes d'accès aux clés ne seront acceptées que si une attestation vérifiable est fournie concernant le caractère confidentiel de l'environnement informatique.

Split Trust, en tant que composante d'UDE, accroît la confiance en permettant de ne pas dépendre d'une seule entité au moment d'encapsuler toute une clé. Au lieu de cela, la DEK peut être divisée et chaque fragment envoyé à plusieurs services d'encapsulage de clé. Split Trust augmente la confiance dans le cloud en garantissant que ni Google, ni un hôte, utilisateur ou application disposant d'un accès à CipherTrust Cloud Key Manager ne puisse unilatéralement déchiffrer les données des clients. CipherTrust Cloud Key Manager prend entièrement en charge Split Trust.

Split Trust répond à la notion de chiffrement omniprésent des données :

- Les données en cours d'utilisation sont chiffrées à l'aide d'une modalité de chiffrement de la mémoire fournie par un matériel répondant aux normes d'informatique confidentielle.
- Les données en transit sont chiffrées sur le fil.
- Les données inactives sont chiffrées avec la garantie supplémentaire apportée par les clés de chiffrement des données de Split Trust.

Les clés de chiffrement contrôlées par le client

Les clients préférant opter pour un mécanisme Bring Your Own Key peuvent utiliser les clés de chiffrement contrôlées par le client de Google, qui prennent en charge un grand nombre de services de Google Cloud Platform, dont vous trouverez la liste ici.

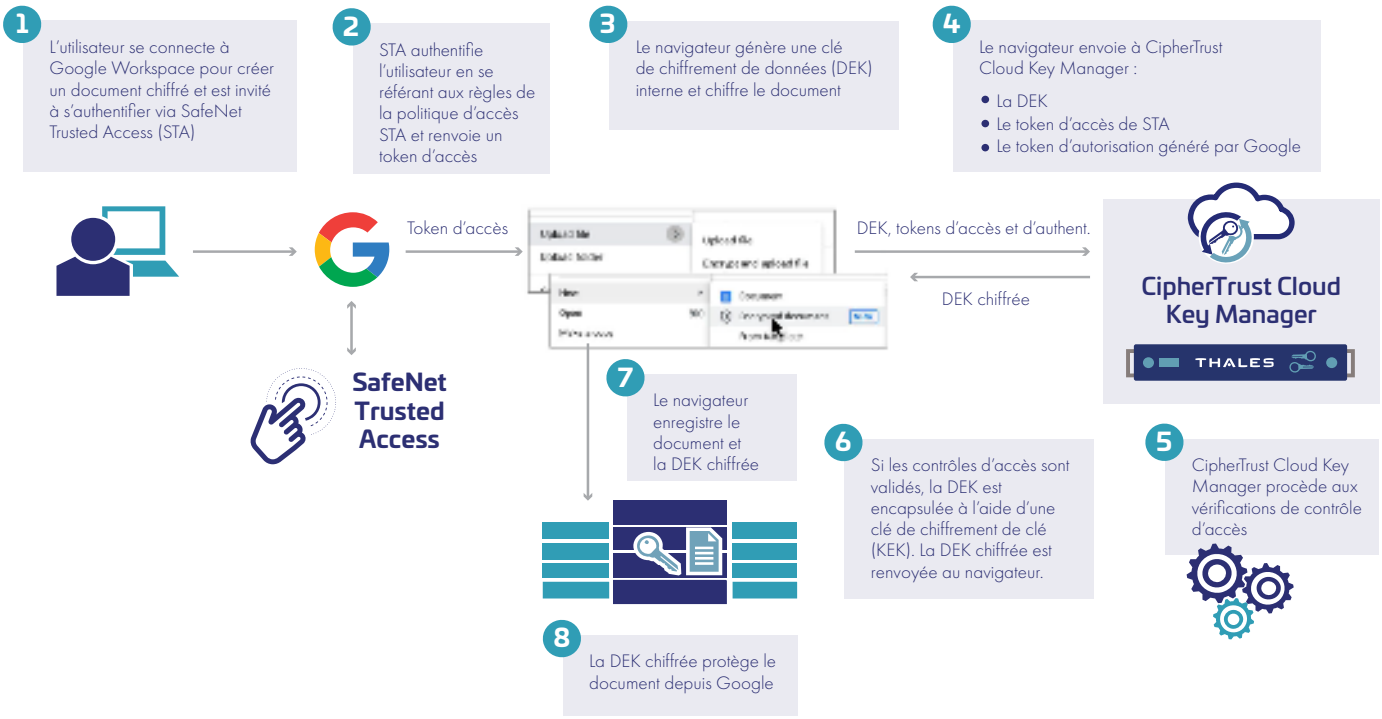


Fig. 1. Processus d'authentification et de chiffrement

Le chiffrement côté client de Google Workspace

Le chiffrement côté client de Google Workspace chiffre le contenu de Workspace à partir du navigateur de l'utilisateur, à l'aide d'une DEK créée par le navigateur. Adhérant au concept de « sécurité partagée », Google recommande à ses clients d'utiliser un gestionnaire de clés externe (EKM) et un fournisseur d'identité (IDP) pour s'assurer que seules les personnes autorisées et authentifiées puissent accéder aux documents protégés. L'EKM est CipherTrust Cloud Key Manager. À la réception d'une demande d'encapsulage ou de désencapsulage comprenant la DEK, un token d'authentification provenant d'un IDP pris en charge par CCKM et un token d'autorisation provenant de Google Workspace, CCKM s'assure que la demande provient d'un demandeur légitime et qu'elle est valide, puis procède à l'encapsulage ou au désencapsulage, sécurisant l'accès à Google Drive, Gmail, Google Agenda ou aux appels sur Google Meet pour les utilisateurs vérifiés et leur rôle (p. ex. lecture seule, lecture et écriture).

Les clients utilisant le chiffrement côté client de Google Workspace bénéficient d'une sécurité renforcée et d'une réduction des coûts de déploiement grâce à la solution intégrée de bout en bout de Thales qui contrôle les clés de chiffrement séparément de leurs données sensibles dans le cloud et protège les identités. Utilisé avec SafeNet Trusted Access (STA), CipherTrust Cloud Key Manager offre une solution de gestion des clés et IDP indépendante provenant d'un seul et même fournisseur, ce qui permet aux clients d'atteindre leurs objectifs commerciaux grâce à un déploiement sans heurts et une expérience utilisateur supérieure.

Google et la plateforme CipherTrust Data Security Platform de Thales

Les solutions de gestion des clés de chiffrement de Thales se développent rapidement au rythme des innovations de Google Cloud Platform et de Google Workspace. Et les solutions de découverte, de protection et de contrôle des données de Thales dans la plateforme CipherTrust Data Security peuvent renforcer la sécurité de Google Cloud Platform et d'autres solutions multicloud et hybrides pour les environnements informatiques IaaS et cloud-native.

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.