cpl.thalesgroup.com

THALES
Building a future we can all trust

Soluciones de gestión de claves de CipherTrust Data Security Platform para Google

La amplia gama de colaboraciones de Thales con Google optimiza la capacidad de las empresas para migrar con seguridad su información confidencial entre la nube pública y las infraestructuras de TI híbridas y privadas. Thales y Google ofrecen un abanico de funciones que permiten que los equipos de seguridad posean y controlen sus claves de cifrado para así cumplir con los mayores requisitos reglamentarios, fruto de las cargas de trabajo altamente distribuidas hoy en día.

Resumen de autoría de claves de cifrado de Google y soluciones de control

Google Cloud Platform (GCP) ofrece una gama de mecanismos de gestión de claves de cifrado controlados por el cliente. Para permitir el cifrado de datos en reposo y gestionar las claves fuera de la infraestructura de Google, Google Cloud ofrece el cifrado de claves gestionado por el cliente (CMEK) y la gestión de claves externa (EKM). Para cifrar datos en uso con claves que se alberguen en el procesador y no estén disponibles para Google, este ofrece Confidential Computing. El cifrado ubicuo de datos de Google se puede ver mejorado por extensiones de EKM. Además, el motor VMware de Google Cloud se aprovecha del protocolo de interoperabilidad de gestión de claves, o KMIP, tanto para cifrar las máquinas virtuales como para gestionar los motores con autocifrado en VMWare VSAN. Google Workspace ofrece cifrado del lado del cliente que protege el contenido a la vez que permite al cliente controlar las claves de cifrado de los datos. La variedad de soluciones en CipherTrust Data Security Platform de Thales ofrece gestión de claves de cifrado para la amplia gama de mecanismos de gestión de claves de cifrado controladas por el cliente de GCP.

CipherTrust Data Security Platform

CipherTrust Data Security Platform de Thales permite a los usuarios localizar, proteger y controlar los datos en la plataforma Google Cloud, Google Workspace, otras nubes y entornos in situ, incluidos entornos de nube híbrida. Como núcleo de la plataforma, CipherTrust Manager es un gestor centralizado exhaustivo de claves y políticas de protección de datos, incluido un servidor KMIP líder del sector. CipherTrust Cloud Key Manager permite la gestión del ciclo de vida de claves de cifrado multinube con soporte exhaustivo por parte de Google. CipherTrust Data Discovery and Classification puede escanear tanto Google Drive como Gmail, y es posible usar CipherTrust Transparent Encryption en la plataforma Google Cloud como infraestructura como un servicio (IaaS) y soluciones como CipherTrust Tokenization a soluciones nativas en la nube implementadas en GCP.

Soluciones de KMIP en la plataforma Google Cloud

El cifrado VM de VMware vSphere habilita el cifrado de máquinas virtuales. El cifrado VM protege los archivos en máquinas virtuales, los archivos en discos virtuales y los archivos de volcado clave al cifrar la entrada y salida de la máquina virtual antes de almacenarse en un disco. VMware vSAN aúna el almacenamiento adjunto en el servidor para brindar un almacén de datos compartido resiliente y cifrado, apto para cualquier carga de trabajo virtual, incluidas aplicaciones indispensables para la empresa.

Tanto el cifrado VM de vSphere y vSAN se aprovechan del protocolo de interoperabilidad de gestión de claves (KMIP) para la gestión de claves de cifrado y el almacenamiento de claves, por lo que ambas soluciones se pueden beneficiar del servidor KMIP en CipherTrust Manager para la gestión del ciclo de vida completo de claves y la separación de funciones.

Google soporta la pila de VMware en Google Cloud mediante el motor VMware de Google Cloud (GCVE). Ahora, las aplicaciones y cargas de trabajo diseñadas para ejecutarse en VMWare se pueden migrar fluidamente a la nube junto con soporte de KMIP por parte de CipherTrust Manager.

Gestión externa de claves

La gestión de claves externa (EKM) de la plataforma Google Cloud es una implementación líder de «guarde su propia clave» (HYOK), para la cual CipherTrust Cloud Key Manager (CCKM) actúa como un servicio de EKM, o EKMS. EKM soporta un número en aumento de servicios de la plataforma Google Cloud, visibles aquí. HYOK con EKM ofrece a los clientes la propiedad de claves con revocación por defecto, dado que las claves solo existen de manera efímera en Google Cloud. Sus sólidos controles de acceso se basan en la asignación de acceso granular (justificación de acceso a claves (KAJ)) a claves para cada proyecto en Google Cloud antes de poder usarse.

Cifrado ubicuo de datos

La función de cifrado ubicuo de datos (UDE) de Google conlleva dos innovaciones significativas en la seguridad computacional. CipherTrust Cloud Key Manager soporta tanto Confidential Computing como Split Trust.

Confidential Computing en el contexto de UDE se aprovecha de las Compute Engines protegidos por hardware de la plataforma Google Cloud, aportando garantías sólidas de la privacidad de los datos en uso. Un aspecto crucial de Confidential Computing es la certificación: la capacidad de verificar que un entorno remoto está protegido y es apto para enviar datos o claves confidenciales. En el contexto de UDE, la certificación permite la verificación remota de que ciertas instancias computacionales de la plataforma Google Cloud operan con protecciones por hardware de Confidential Computing.

CipherTrust Cloud Key Manager verifica las garantías apoyando al Confidential Computing. Las reglas de acceso a claves ahora incluyen los requisitos de Confidential Computing; en este caso, las peticiones de acceso a claves solo se aceptarán si se aporta una garantía verificable de un entorno de Confidential Computing.

Split Trust, como componente de UDE, incrementa la confianza al no apoyarse en una única entidad para proteger una clave completa. En su lugar, la DEK se puede separar y cada fragmento se puede enviar a varios servicios de protección de claves. Split Trust incrementa la confianza en la nube al garantizar que ni Google ni un anfitrión, aplicación o usuario con acceso a CipherTrust Cloud Key Manager puedan descifrar de manera unilateral los datos de un cliente. CipherTrust Cloud Key Manager cuenta con soporte completo de Split Trust.

Split Trust cumple con la idea del cifrado ubicuo de datos:

- Los datos en uso se cifran con cifrado de memoria aportada por software de Confidential Computing
- Los datos en movimiento están cifrados en línea
- Los datos en reposo se cifran con la potencia adicional de claves de cifrado de datos de Split Trust

Claves de cifrado gestionadas por el cliente

Los clientes que prefieran un mecanismo de «traiga su propia clave» pueden utilizar las claves de cifrado gestionadas por el cliente de Google, que soportan una amplia gama de servicios de la plataforma Google Cloud, que se pueden encontrar aquí.

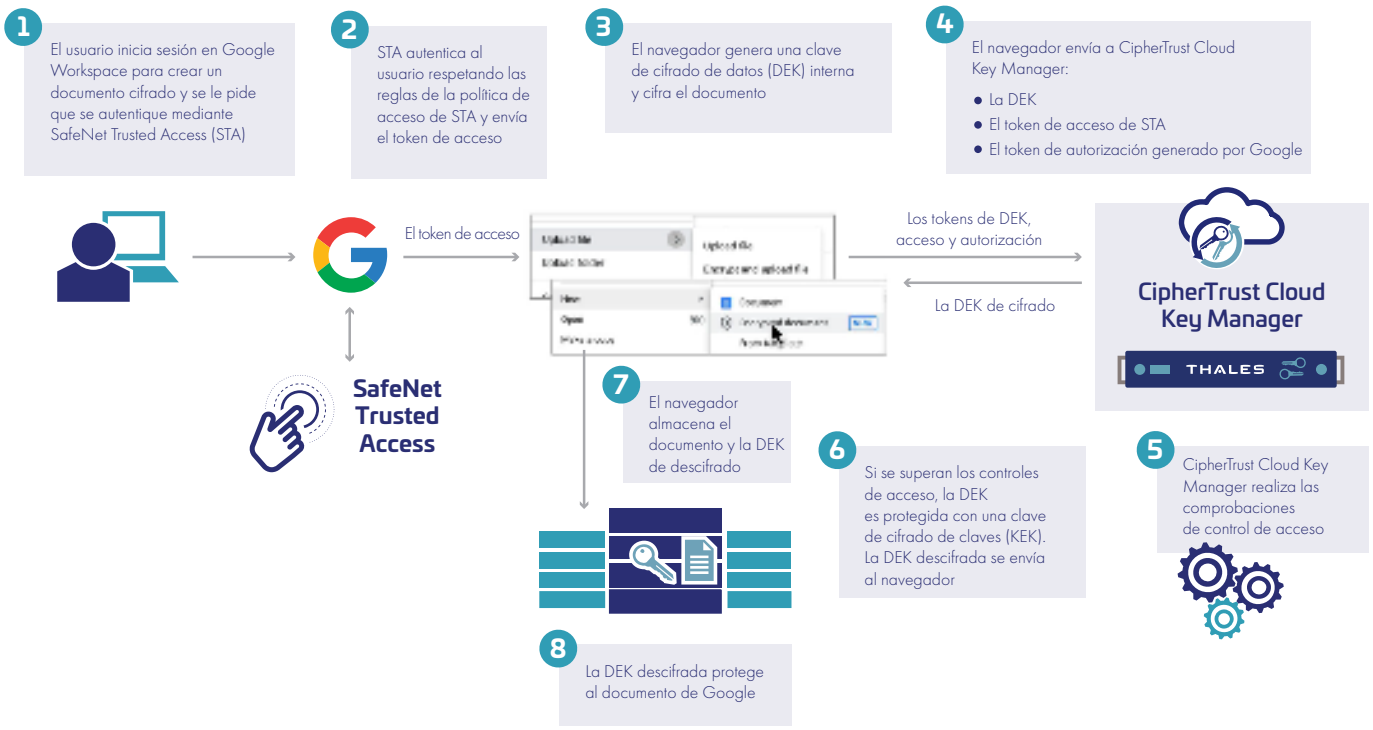

Fig. 1. Flujo de trabajo de autenticación y cifrado

Cifrado de Google Workspace del lado del cliente

El cifrado de Google Workspace del lado del cliente cifra el contenido de Workspace en el propio navegador del usuario mediante una DEK creada por el navegador. De esta forma, y adhiriéndose al concepto de «seguridad compartida», Google recomienda que los clientes usen un gestor de claves externo (EKM) y un proveedor de identidad (IDP) para garantizar que solo los individuos autorizados y autenticados puedan acceder a los documentos protegidos. La EKM es CipherTrust Cloud Key Manager. Al recibir una petición de cifrado o descifrado, incluida la DEK, un token de autenticación de cualquier IDP soportada por CCKM y un token de autorización de Google Workspace, CCKM garantiza que las peticiones vienen de un individuo legítimo y que son válidas, y a continuación procede con el cifrado o descifrado, protegiendo el acceso a Google Drive, Gmail, Google Calendar o llamadas en Google Meet para los usuarios verificados y sus funciones (p. ej., solo lectura, lectura y escritura).

Los clientes que usan cifrado en Google Workspace del lado del cliente pueden disfrutar de un mayor nivel de seguridad y menores gastos de implementación haciendo gala de la solución integrada de principio a fin de Thales, que controla las claves de cifrado de manera separada a los datos confidenciales en la nube, además de proteger las identidades. CipherTrust Cloud Key Manager, usado junto con SafeNet Trusted Access (STA), ofrece a los clientes una solución de gestión de claves y un IDP independiente de parte de un solo proveedor, lo que contribuye a alcanzar las metas empresariales con una implementación fluida y una experiencia de usuario superior.

Google y CipherTrust Data Security Platform de Thales

Las soluciones de gestión de claves de cifrado de Thales se expanden rápidamente con las innovaciones de la plataforma Google Cloud y Google Workspace. Además, las soluciones de localización, protección y control de datos de Thales en CipherTrust Data Security Platform pueden mejorar la seguridad de la plataforma Google Cloud y otras soluciones de multinube y nube híbrida, tanto para entornos IaaS como de computación nativa en la nube.

Acerca de Thales

Las personas en las que confía para la protección de su privacidad confían en Thales para proteger sus datos. Cuando se trata de seguridad de datos, las empresas se enfrentan a un número cada vez mayor de momentos decisivos. Tanto si se trata de elaborar una estrategia de cifrado, como de migrar a la nube o de cumplir los requisitos normativos, puede confiar en Thales para asegurar su transformación digital.

Tecnología decisiva para momentos decisivos.