cpl.thalesgroup.com

THALES
Building a future we can all trust

# CipherTrust Data Security Platform Key Management Solutions for Google

Thales's many collaborations with Google accelerate the ability of enterprises to safely migrate sensitive data between public cloud, hybrid and private IT infrastructures. Thales and Google offer a range of capabilities that enable security teams to own and control their encryption keys to help fulfill heightened regulatory requirements amidst today's highly distributed workforce.

## Google encryption key ownership and control solutions overview

Google Cloud Platform (GCP) offers a range of customer-controlled encryption key management mechanisms. To enable encryption of data-at-rest and manage keys outside of Google's infrastructure, Google Cloud provides: Customer-Managed encryption keys (CMEK) and External Key Management (EKM). To encrypt data-in-use with keys that remain resident in the processor and unavailable to Google, Google provides Confidential Computing. Google Ubiquitous Data Encryption leverages extensions in EKM. And Google Cloud VMware Engine leverages the Key Management Interoperability Protocol, or KMIP, to encrypt both Virtual Machines and to manage self-encrypting drives in VMware VSAN. Google Workspace offers Client-side encryption that protects content while enabling customer control of the data encryption keys. Various solutions in the CipherTrust Data Security Platform from Thales provide encryption key management for the range of GCP customer-controlled encryption key management mechanisms.

## CipherTrust Data Security Platform

The CipherTrust Data Security Platform from Thales enables users to discover, protect and control data in Google Cloud Platform, Google Workspace, other clouds, and on premises including hybrid cloud environments. At the center of the platform, CipherTrust Manager is a comprehensive centralized key and data protection policy manager, including an industry-leading KMIP server. CipherTrust Cloud Key Manager provides multicloud encryption key life cycle management with comprehensive Google support. CipherTrust Data Discovery and Classification can scan both Google Drive and Gmail and it's possible to bring CipherTrust Transparent Encryption to Google Cloud Platform Infrastructure as a Service (IaaS) and solutions like CipherTrust Tokenization to cloud-native solutions deployed on GCP.

## Google Cloud Platform KMIP Solutions

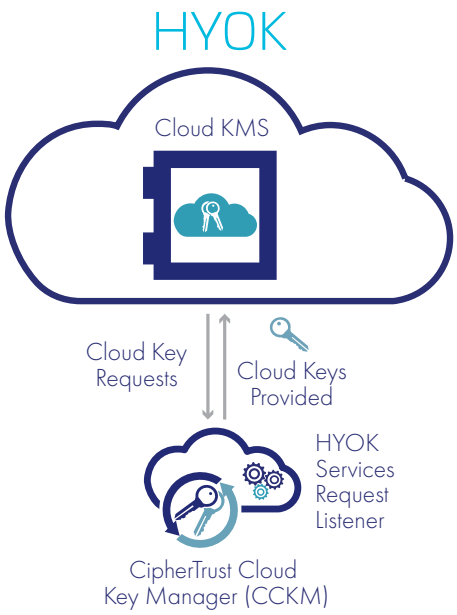
VMware vSphere VM Encryption enables encryption of virtual machines. VM Encryption protects virtual machine files, virtual disk files, and core dump files by encrypting the input/output from the virtual machine before it gets stored on disk. VMware vSAN pools server-attached storage to provide a resilient and encrypted shared datastore suitable for any virtualized workload, including business-critical applications.

Both vSphere VM Encryption and vSAN leverage the Key Management Interoperability Protocol (KMIP) for encryption key management and key vaulting, so both solutions can leverage the KMIP server in CipherTrust Manager for full key lifecycle management and role separation.

Google supports the VMware stack in Google Cloud using the Google Cloud VMware Engine (GCVE). Now apps and workloads designed to run within VMware can be seamlessly migrated to the cloud, along with KMIP support from CipherTrust Manager.

## External Key Management

Google Cloud Platform External Key Management (EKM) is a leading "hold your own key" (HYOK) implementation, for which CipherTrust Cloud Key Manager (CCKM) acts as an EKM Service, or EKMS. EKM supports a growing number of Google Cloud Platform services visible here. HYOK with EKM delivers customer key ownership with revocation by default, as keys exist in Google Cloud only ephemerally. Powerful access controls are based on granting granular access (Key Access Justification (KAJ)) to keys for each Google Cloud Project before they can be used.




## Ubiquitous Data Encryption

Google's Ubiquitous Data Encryption (UDE) capability involves two significant computing security innovations. CipherTrust Cloud Key Manager supports both Confidential Computing and Split Trust.

**Confidential Computing** in the context of UDE leverages hardware-secured Google Cloud Platform Compute Engines, providing strong guarantees of data-in-use privacy. A crucial aspect of confidential computing is attestation – the ability to verify that a remote environment is protected and suitable for delivery of sensitive data and/or keys. In the context of UDE, attestation allows remote verification that certain Google Cloud Platform Compute Instances are operating with hardware-secured Confidential Computing protections.

In support of confidential computing, CipherTrust Cloud Key Manager can verify the attestations. Key access rules now include requirements for confidential computing – in this case, requests to access keys will only be accepted if a verifiable attestation of a confidential computing environment is provided.

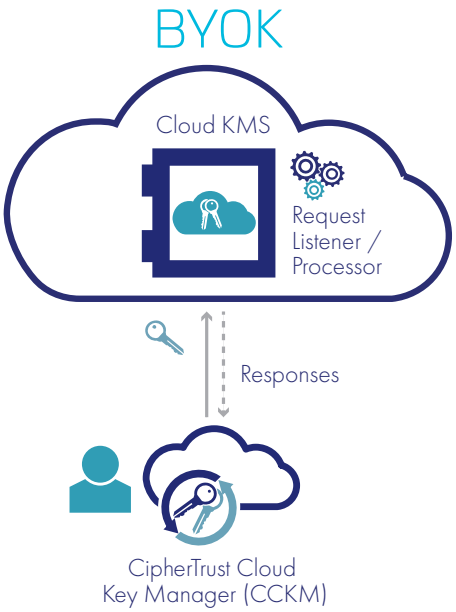
**Split Trust**, as a component of UDE, increases trust by not relying on a single entity to wrap an entire key. Instead, the DEK may be split and each fragment sent to multiple key wrapping services. Split Trust increases cloud trust by ensuring that neither Google nor a host, application or user with access to CipherTrust Cloud Key Manager, can unilaterally decrypt customer data. CipherTrust Cloud Key Manager has full support for Split Trust.

Split trust fulfills the notion of ubiquitous data encryption:

- Data in use is encrypted with memory encryption provided by confidential computing hardware
- Data in motion is encrypted on the wire
- Data at rest is encrypted with the additional power of Split Trust data encryption keys

## Customer-Managed Encryption Keys

Customers who may prefer a Bring Your Own Key mechanism can utilize Google Customer-Managed Encryption Keys, which supports a large number of Google Cloud Platform services, visible here.



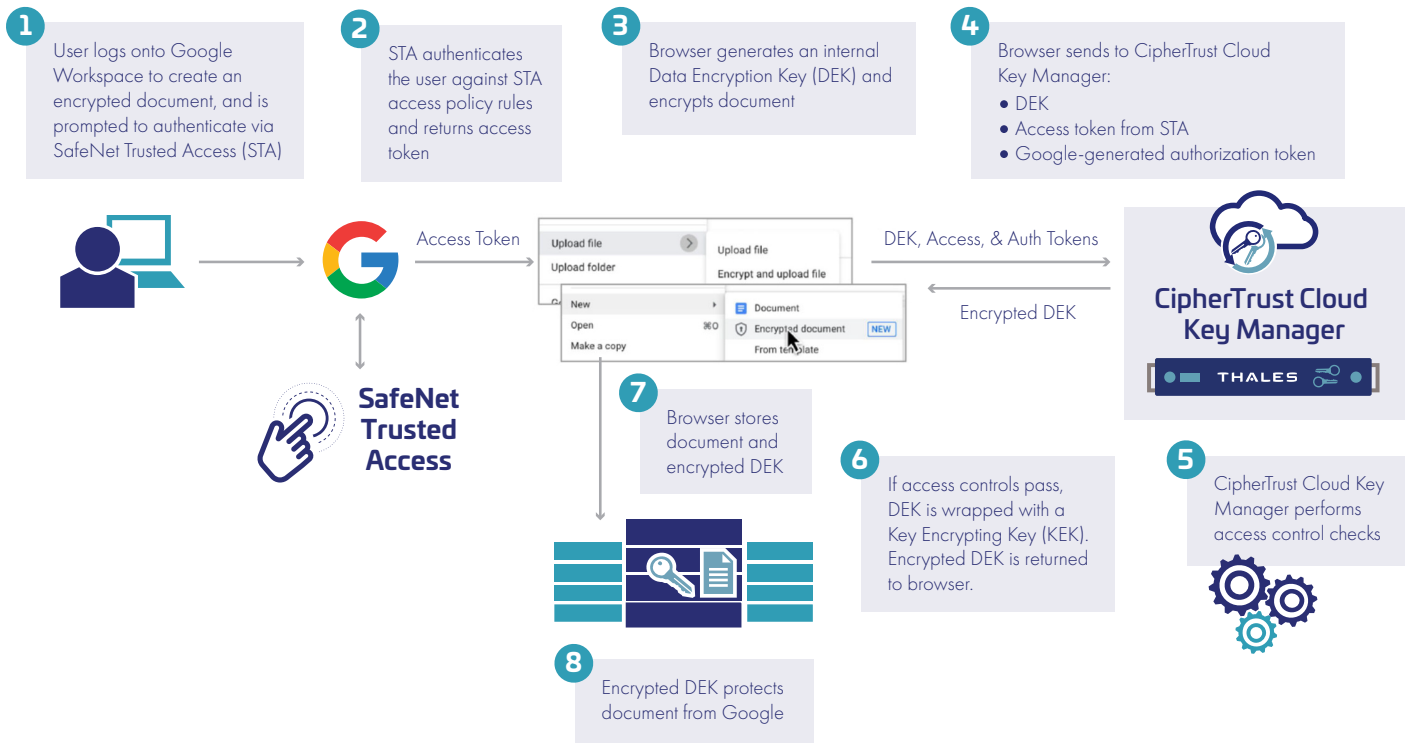



**Fig 1. Authentication & Encryption Workflow**

## Google Workspace Client-side encryption

Google Workspace Client-side encryption encrypts Workspace content from within the user's browser using a DEK created by the browser. Adhering to a concept of 'shared security', Google recommends that customers use an external key manager (EKM) and Identity Provider (IDP) to ensure that only authorized and authenticated individuals can access protected documents. The EKM is CipherTrust Cloud Key Manager. Upon receipt of a wrap or unwrap request including the DEK, an authentication token from any IDP supported by CCKM and an authorization token from Google Workspace, CCKM ensures that the request is from a legitimate requestor and is valid, then performs the wrap or unwrap, securing access to Google Drive, Gmail, Google Calendar, or calls over Google Meet for verified users and their role (e.g., read only, read and write).

Customers using Google Workspace Client-side encryption can achieve stronger security and lower deployment overheads by benefiting from Thales's integrated end-to-end solution that controls encryption keys separate from their sensitive data in the cloud and protects identities. CipherTrust Cloud Key Manager used with SafeNet Trusted Access (STA) provides customers with key management and an independent IDP solution from a single vendor, helping to achieve business goals with a smooth deployment and superior user experience.

## Google and the CipherTrust Data Security Platform from Thales

Thales encryption key management solutions expand rapidly with Google Cloud Platform and Google Workspace innovations. And Thales data discovery, protection and control solutions in the CipherTrust Data Security Platform can enhance security for Google Cloud Platform and other multi- and hybrid cloud solutions for both IaaS and Cloud Native computing environments.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



**Contact us –** For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us