Google Cloud | THALES

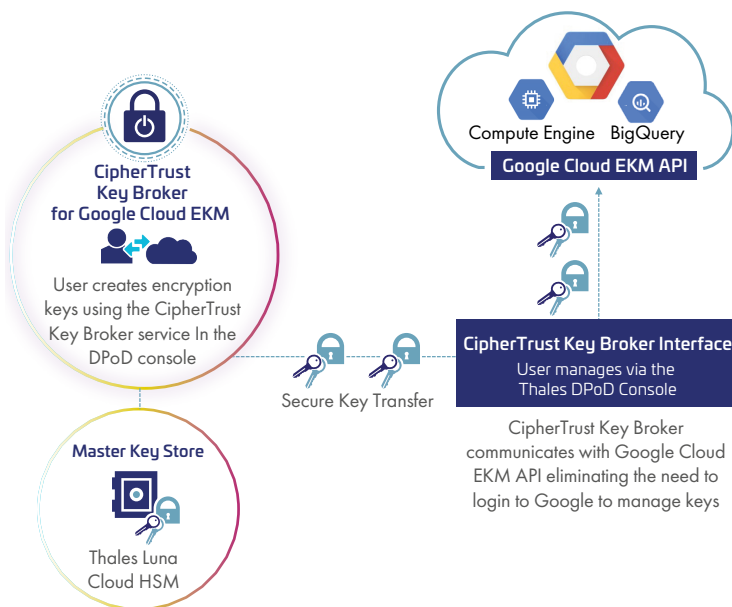# Enhancing Encryption Key Control and Data Security in Google Cloud Platform

Overview

When it comes to encryption keys, security best practice is all about control and separation between encrypted data-at-rest and the keys. Google Cloud encrypts customer data-at-rest by default and offers organizations multiple options to control and manage their encryption keys. For many organizations hosting sensitive data or looking to migrate workloads to the cloud, they require enhanced control and ownership over their encryption keys in order to meet compliance or internal security requirements. Google's Cloud External Key Manager (EKM) API helps organizations achieve this next level of control over how and when their encryption keys are used to protect and access encrypted data. To help organizations benefit from this enhanced level of control, Thales has integrated their CipherTrust Key Broker service with Google's Cloud EKM. The CipherTrust Key Broker for Google Cloud EKM is a service available on the industry leading Thales Data Protection on Demand platform.

CipherTrust Key Broker for Google Cloud EKM

Create and control encryption keys outside of Google Cloud

CipherTrust Key Broker is integrated with Google Cloud EKM to make it easy for organizations to follow security and key management best practices, while leveraging the power of Google Cloud for compute and analytics. Organizations are able to securely create and control their own encryption keys separate from where their sensitive data is being hosted. By generating encryption keys using CipherTrust Key Broker, organizations can verify the origin and quality of the keys they are providing to the cloud provider, while maintaining the original version of the key outside of the Google Cloud environment. Organizations hold their master keys in a Thales Luna Cloud HSM, which acts as the trust anchor for the CipherTrust Key Broker solution. This provides a FIPS 140-2 Level 3 certified root-of-trust, and ensures separation between sensitive data and encryption keys, helping to fulfill compliance and security requirements.

How it Works

CipherTrust Key Broker for Google Cloud EKM
User creates encryption keys using the CipherTrust Key Broker service In the DPoD console

Master Key Store
Thales Luna Cloud HSM

Secure Key Transfer

Compute Engine   BigQuery
Google Cloud EKM API

CipherTrust Key Broker Interface
User manages via the Thales DPoD Console

CipherTrust Key Broker communicates with Google Cloud EKM API eliminating the need to login to Google to manage keys

Google's Cloud EKM is a cloud native API, that interacts with CipherTrust Key Broker service via a single URL, which simplifies configuration, deployment and is easy to consume. Keys created externally by the CipherTrust Key Broker are then managed from a single location in a user friendly console in Thales Data Protection on Demand (DPoD). Master keys are always stored outside of Google Cloud in the Luna Cloud HSM. With this solution, there is no new hardware to buy and deploy, as CipherTrust Key Broker uses Luna Cloud HSM as a root-of-trust.

Features and Benefits

Meet security mandates and compliance:
- **Key access justifications - decide when and why data can be decrypted:** This provides a detailed justification each time a key is requested to decrypt data, along with a mechanism for users to explicitly approve or deny usage of the key using an automated policy that they set. Organizations can deny Google the ability to decrypt their data for any reason. As a result, they ultimately control the access to their data — a level of control not yet available from most leading cloud providers.
- **Enhanced key usage policies and access control:** Control who can access encryption keys, and create policies around why, where and how a key can be used. The crypto operations and master encryption keys are always stored outside of Google Cloud, which enforces that access to data-at-rest for compute and analytics requires an external key.
- **Maintain key provenance:** Maintain strict control of the location and distribution of important keys and gain visibility into who has access to keys, when they have been used and where they are located.
- **Audited / distributed key availability:** Externally archive and remove encryption keys and key caches from the cloud environment in which sensitive data is hosted.

Streamline operations and centralize key management:
- **Simplifies the management of encryption keys including:** Secure key generation, storage, distribution, deactivation and deletion outside of the cloud environment where data is stored. Securely generating, delivering and managing their own encryption keys helps organizations reduce the risk of unauthorized access to data.
- **Low latency and high performance:** CipherTrust Key Broker for Google Cloud EKM is a user friendly solution that provides fast round trip latency, without compromising on performance when carrying out key management operations and controls.

Simplify configuration and deployment:
- **Cloud native API:** Google's EKM is a cloud native API, that interacts with the CipherTrust Key Broker via a single URL which simplifies configuration, deployment and is easy to consume. Keys created externally by the CipherTrust Key Broker are then managed from a single location in a user friendly console in Thales Data Protection on Demand.
- **Key store and configuration:** Key rings can be created in one of the regions recommended by the CipherTrust Key Broker, providing additional control over where encryption keys reside. CipherTrust Key Broker gives the ability to disable the usage of the keys in the key store.
- **Key caching - manage the balance between security and low latency:** Appropriately balance risk, control, security, performance and operational complexity when protecting cloud workloads.
- **Quick integration and deployment:** CipherTrust Key Broker for Google Cloud EKM is available in the Thales Data Protection on Demand platform, a cloud subscription-based HSM service that offers:
  - Key management capabilities deployed within minutes
  - No need for specialized hardware or associated skills
  - Secure generation and storage of master keys in a Luna Cloud HSM (separate from Google Cloud), maintaining strict access and controls

Thales is Here to Help

Contact Thales to help you assess and define the data protection strategy that best suits your organizational requirements, and for integration guides to help speed your deployment.

Thales and Google Partnership

For more than 25 years, Thales has been a market leader continuously innovating to meet the evolving security and compliance needs of businesses around the world. The most trusted brands in the world rely on Thales to provide external key management, protecting their sensitive data in the cloud, on-premises and in hybrid IT infrastructures. As security experts, Thales provides Google Cloud users with greater control over security policies and key management, with the ability to manage encryption keys separate from their encrypted data, ensuring security and facilitating compliance. Thales is integrated with Google's Cloud EKM to provide their joint customers with security and key management best practices while leveraging the power of Google cloud for compute and analytics.

> cpl.thalesgroup.com <

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