DATA SHEET

Entrust KeyControl Vault for Cloud Keys

Control access to cloud-based cryptographic keys using KeyControl and Google Cloud Platform (GCP) External Key Manager (EKM)

Overview

In response to the rise of modern cybersecurity threats and stringent government regulations, cloud providers are increasingly adopting cryptographic services. These services are essential for maintaining the integrity and confidentiality of data, whether it's stored (data at rest) or being transmitted (data in transit).

In regulated sectors such as finance, insurance, and healthcare, choices are dictated by security and data management policies, governmental directives (like data sovereignty requirements), and the overall security strategy of the organization.

Consequently, these organizations consistently turn to cryptographic services offered by cloud providers such as Google to align with these regulatory requirements and enhance their overall security framework.

Data sovereignty legislation in the European Union, informed by the outcome of the Schrems II legal case, has led to many organizations having to think carefully about where their cryptographic keys and encrypted data reside and about the control and access to them. Google responded by introducing the EKM, which allows organizations to store and manage their cryptographic keys outside of the Google Cloud perimeter.

GCP allows users to use Cloud External Key Manager (EKM) in Google Cloud Key Management Service (KMS) for Google Projects.

Key Features

- Protection of your data in Google Cloud using keys securely generated and stored outside of Google's infrastructure
- External visibility and control over every key request with full key lifecycle management
- Hardware key protection using FIPS 140-3 Level 3 certified nShield HSMs (optional)
- Automated compliance engine for PCI DSS, DISA STIGs, NIST 800-130, HIPAA, and other standards via KeyControl Compliance Manager
- KeyControl can be deployed on premises, as a service, or as a hybrid solution
- Scalable to manage tens of millions of keys

ENTRUST

SECURING A WORLD IN MOTION

EKM provides the ability to encrypt data with external keys for a growing number of Google Cloud Platform services listed here, including BigQuery and Google Compute Engine (GCE).

In the context of EKM implementation, Entrust KeyControl Vault functions as an EKM service, empowering businesses to effectively manage and maintain ownership of the encryption keys used within GCP.

Using a Federal Information Processing Standards (FIPS) 140-2 certified platform, the KeyControl Vault for cloud key management simplifies management of these externally managed keys by automating their lifecycle; including key storage, backup, distribution, rotation, and key revocation.

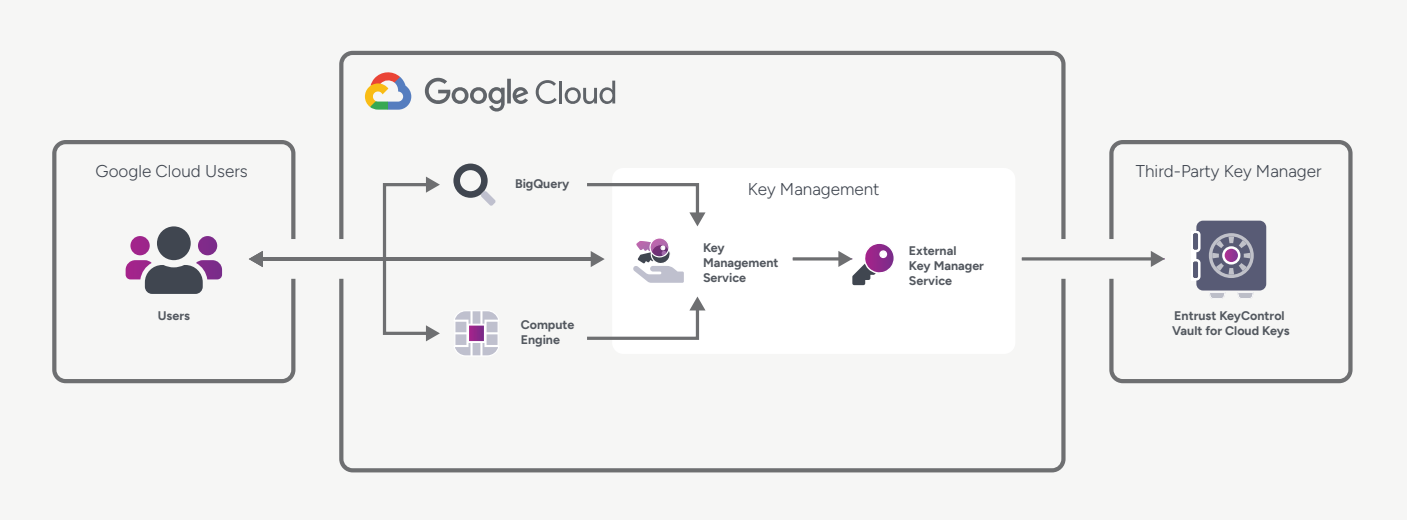
How does it work?

Using the Hold Your Own Key (HYOK) model, EKM enables cryptographic keys to reside outside Google's infrastructure.

Google's External Key Manager (EKM) works through a multi-step process:

1. You first need to create a key in the Entrust KeyControl Vault for cloud key management. This key, known as the externally managed key, has a unique URI and key path.
2. You then grant your Google Cloud Project access to use this key from the KeyControl Vault.
3. Within your Google Cloud Project, you create a Cloud EKM key using the URI or key path of the Cloud EKM key version. The Cloud EKM key works in conjunction with the externally managed key to ensure the security of your data, with the assurance that the external key remains undisclosed to Google.

The following diagram shows how Cloud KMS fits into the key management model. This diagram uses Compute Engine and BigQuery as two examples. Both the Cloud EKM key and the externally managed keys are required for each encryption and decryption request. If you lose access to either key, your data cannot be recovered. It is not possible to recreate an identical Cloud EKM key version by using the same external key URI or key path.



Protects your data with the highest level of assurance

Encryption is the first line of defense for protecting sensitive data processed or stored in the cloud. The Entrust KeyControl Vault secures cryptographic keys by generating and storing the keys separately from the data on a secure FIPS 140-2 certified key management system. Moreover, the KeyControl Vault can help you achieve the desired security posture and ensure that best practices are followed by implementing separation of duty, least privilege, dual control, and audit trail generation.

Facilitates compliance with regulatory requirements using Key Compliance Manager

Beyond the cyber threat risk, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements and standards is sometimes not possible when keys are not segregated from the cloud.

Entrust KeyControl Compliance Manager extends vault capabilities beyond a single dashboard view by automating support compliance with industry regulations such as Payment Card Industry Data Security Standard (PCI DSS), *Health Insurance Portability and Accountability Act* (HIPAA), or the General Data Protection Regulation (GDPR).These additions make it easier to demonstrate compliance to auditors, not only for the KeyControl Vault for Cloud Keys but for all vaults across your organization. Wherever you operate and whatever the regulation, Entrust KeyControl Compliance Manager can help you achieve and maintain compliance, improve your security, and manage your risk.

Benefits

Combines the benefits of GCP Services with full control over access to data

The Entrust KeyControl Vault provides maximum control, automation, and management over cryptographic keys for organizations that need to protect their data stored in GCP.

- EKM is based on the HYOK model, for organizations who want to retain full control over access to their data regardless of where it is stored or processed.
- The entire scope of the external key manager is outside the technical and operational control of GCP.
- Customers maintain control of the availability, durability, performance, and latency boundaries of key operations.

The KeyControl Vault can act as an emergency off switch by blocking access to all sensitive data across all GCP accounts in your organization. The external key store remains transparent for all applications or GCP services encrypting data in the cloud.

Internal and external key management

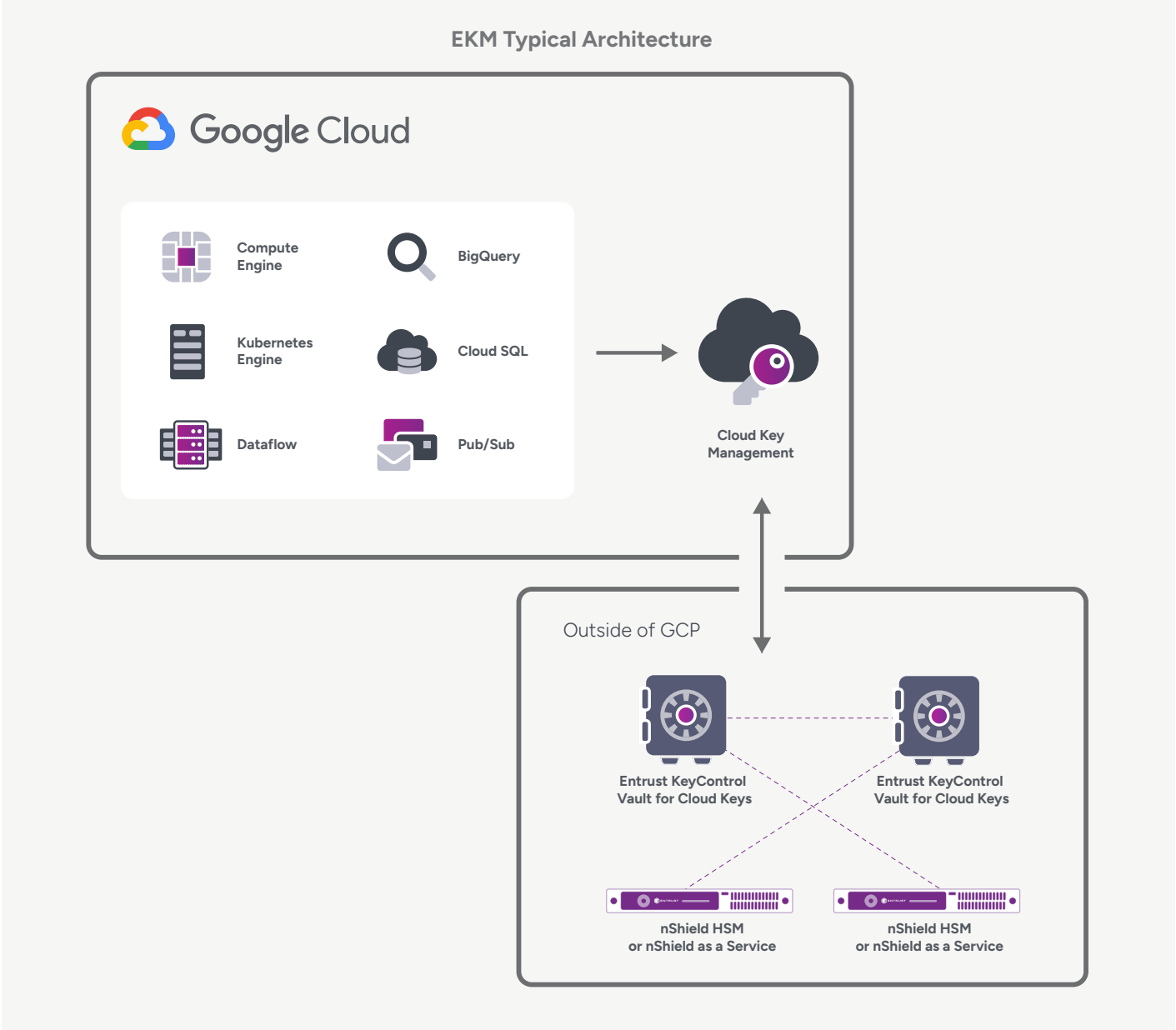
Thus, each double-encrypted data key cannot be used to decrypt an object without access to both:

- An internal key provided by the GCP KMS
- An external key provided by the Entrust KeyControl Vault

Using the concept of envelope encryption, the GCP service encrypts the data and then stores the data encryption key (DEK) alongside the encrypted data. The external and internal keys are both needed when an GCP service needs to decrypt the encrypted data.

Without online access to external keys, GCP services cannot encrypt and decrypt data. For redundancy two KeyControl Vaults are usually deployed in an active-active cluster across two separate sites.

EKM is compatible with all GCP services listed under the Cloud EKM key support services page. When integrating the KeyControl Vault with GCP EKM, customers maintain complete control over the lifecycle of their keys, including their creation, rotation, replication, and deletion. This approach ensures that customers have full ownership and management of their encryption keys.



Technical Specifications

Supported cryptographic algorithms for external keys:

- AES 256-bit key (256 random bits)

Management and monitoring:

- Centralized management with Web UI and REST API
- Syslog and Splunk integration

Certifications:

- FIPS 140-3 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

Platforms supported:

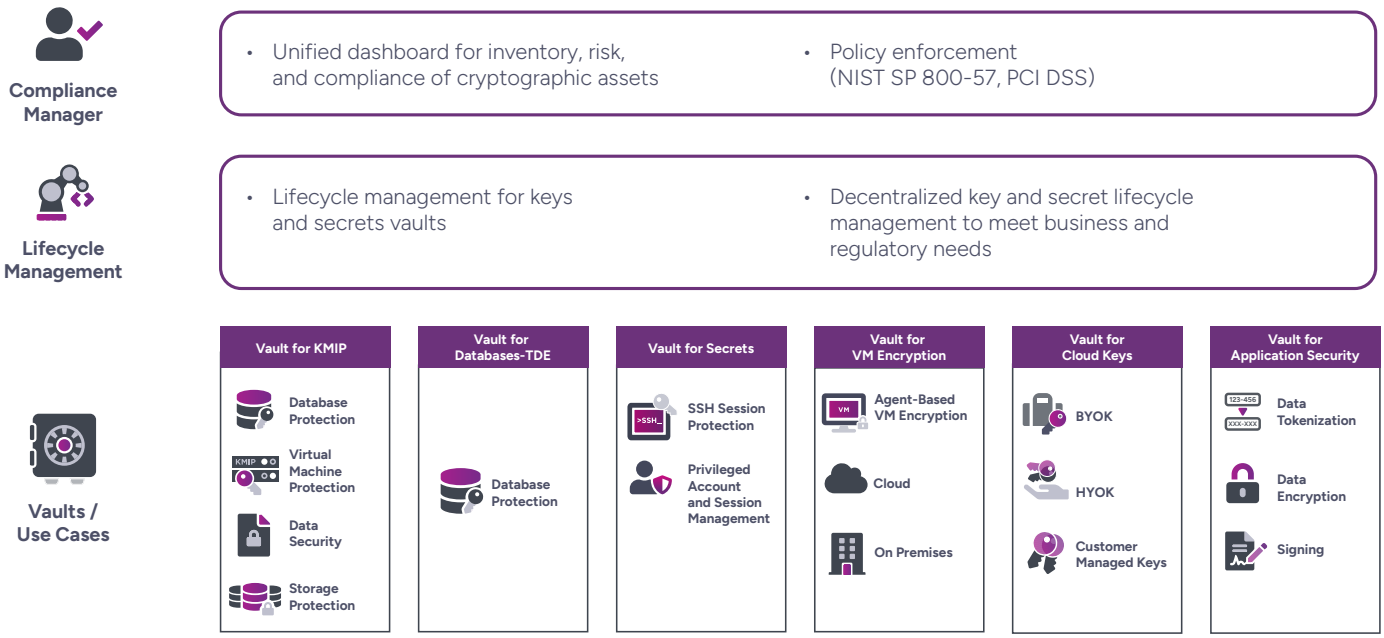
- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, NetApp, Nutanix
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)
- Hypervisor support: ESXi, KVM

Deployment media:

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

Entrust KeyControl Platform

Entrust KeyControl Vault for Cloud Keys is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



For more details on the KeyControl platform, KeyControl Compliance Manager, and the range of vaults, download the Entrust KeyControl Solution Brochure.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION