cpl.thalesgroup.com

THALES

Thales High Assurance Protection Strategies for Google Cloud Platform

Secure workloads across hybrid and multi-cloud environments, including Google Cloud Platform Information technology workloads in Google Cloud Platform (GCP), can offer convenience and cost savings. However, you still need to follow security, privacy and compliance rules, as well as best practices for securing your data. Furthermore, you need rapid data mobility across all the clouds you use and those in your future, a need which can be compromised with cloud-vendor-specific encryption solutions.

For enterprises that elect to use encryption to protect their data, securing their encryption keys is of paramount importance. Your enterprise is looking to leverage all of the advantages the cloud has to offer, but some of the benefits come at a price. In return for flexibility, scalability and automation, encryption key ownership is often given up to the cloud service provider, taking the control out of your hands and increasing compliance complexity.

When it comes to encryption keys, it is all about control. By default GCP generates encryption keys on behalf of its customers and manages their lifecycles. For many organizations hosting sensitive data in the cloud, this lack of sole control and ownership over encryption keys does not meet their compliance or internal security requirements. Instead these organizations want full control over how and when encryption keys are used to protect and access encrypted data.

Thales offers a number of solutions based upon the high-assurance Luna Hardware Security Modules (HSMs) and the cloud-based Data Protection on Demand, to secure and protect your data regardless of its location. With Thales, enterprises have the flexibility to leverage cloud services, the ability to both own and control their encryption keys, and reduce the risk of unauthorized data access or data loss.

Google Cloud Platform

Google Cloud Platform offers organizations several different encryption key generation, management, and protection options:

Default Encryption	• Google managed encryption and encryption keys • Organizations have no access to the keys or control of key rotation
Customer-Managed Encryption Keys (CMEK)	• Organizations can manage their own keys (e.g. generation, rotation, deletion) • Google stores all key material
Customer-Supplied Encryption Keys (CSEK)	• Encryption keys are stored in the FIPS 140-2 Level 3 Luna HSM (on-premises), or Luna Cloud HSM (DPoD), root of trust • Provides organizations with full control over encrypted data and key lifecycles • Recommended solution for internal, critical and confidential data
Google Cloud EKM Service	• Provides organizations with enhanced control over how and when their encryption keys are used to protect and access encrypted data, by integrating with CipherTrust Key Broker for Google Cloud EKM, a service available on Thales Data Protection on Demand • Organizations hold their master keys in a FIPS 140-2 Level 3 Luna Cloud HSM, which acts as the trust anchor for the CipherTrust Key Broker solution

Customer Supplied Encryption Keys (CSEK)

CSEK is a Google Key Management Services (Google KMS) feature that enables organizations to leverage the benefits of Google cloud services while complying with complex regulations and policies by not giving up control over the creation of encryption keys. For higher-assurance applications and data, it is recommended that organizations retain sole control over the generation of encryption keys.

The integration between Google KMS and Thales solutions provides 100% confidence and key control, as opposed to storing keying material in the GCP. As a result, access to internal and highly sensitive data associated with GCP services such as Google Cloud Engine are completely under the customer's control while still being transparent to end users.

Luna Network HSM

Ensure access control over your encryption keys by generating and storing your own CSEK within the FIPS 140-2 Level 3 validated confines of Luna HSMs. Benefits include:

- High-assurance, tamper-evident keys-in-hardware protection
- High performance with up to 20,000 ECC and 10,000 RSA operations per second

Quickly secure a large number of standard applications with our broad partner ecosystem – documented, out-of-the-box integrations.

CipherTrust Key Broker for Google Cloud EKM

Enhancing Encryption Key Control and Data Security in Google Cloud Platform

Google's Cloud EKM is a cloud native API, that interacts with CipherTrust Key Broker for Google Cloud EKM 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) and are stored outside of Google Cloud in the Luna Cloud HSM. With this solution, there is no new hardware to buy and deploy, as all CipherTrust Key Broker services use Luna Cloud HSM as their root of trust.

Data Protection on Demand (DPoD)

- Cloud, subscription-based HSM and Key Broker services
- Key management capabilities deployed within minutes
- No need for specialized hardware or associated skills
- Secure storage of keys in the cloud maintaining strict access 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 to provide their joint customers with security and key management best practices while leveraging the power of Google Cloud.