Cloud Key Management

Manage encryption keys on Google Cloud.

- Deliver scalable, centralized, fast cloud key management
- Help satisfy compliance, privacy, and security needs
- Apply hardware security modules (HSMs) effortlessly to your most sensitive data
- Use an external KMS to protect your data in Google Cloud and separate the data from the key
- Approve or deny any request for your encryption keys based on clear and precise justifications

Cloud Key Management Service

Cloud Key Management Service allows you to create, import, and manage cryptographic keys and perform cryptographic operations in a single centralized cloud service. You can use these keys and perform these operations by using Cloud KMS directly, by using Cloud HSM or Cloud External Key Manager, or by using Customer-Managed Encryption Keys (CMEK) integrations within other Google Cloud services.

With Cloud KMS you are the ultimate custodian of your data, you can manage cryptographic keys in the cloud in the same ways you do on-premises, and you have a provable and monitorable root of trust over your data.

BENEFITS

Scale your security globally

Scale your application to Google's global footprint while letting Google worry about the challenges of key management, including managing redundancy and latency.

Help achieve your compliance requirements

Easily encrypt your data in the cloud using software-backed encryption keys, FIPS 140-2 Level 3 validated HSMs, customer-provided keys or an External Key Manager.

Leverage from integration with Google Cloud products

Use customer-managed encryption keys (CMEK) to control the encryption of data across Google Cloud products while benefiting from additional security features such as Google Cloud IAM and audit logs.

Key features

Centrally manage encryption keys

A cloud-hosted key management service that lets you manage symmetric and asymmetric cryptographic keys for your cloud services the same way you do on-premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.

Deliver hardware key security with HSM

Toggle between software- and hardware-protected encryption keys with the press of a button. Host encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 validated HSMs. With this fully managed service, you can protect your most sensitive workloads without the need to worry about the operational overhead of managing an HSM cluster.

Provide support for external keys with EKM

Encrypt data in BigQuery and Compute Engine with encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. External Key Manager allows you to maintain separation between your data at rest and your encryption keys while still leveraging the power of cloud for compute and analytics.

Be the ultimate arbiter of access to your data

Key Access Justifications works with Cloud EKM to greatly advance the control you have over your data. It's the only product that gives you visibility into every request for an encryption key, a justification for that request, and a mechanism to approve or deny decryption in the context of that request. These controls are covered by Google's integrity commitments and are currently in beta.

All features

Symmetric and asymmetric key support	Cloud KMS allows you to create, use, rotate, automatically rotate, and destroy AES256 symmetric and RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 asymmetric cryptographic keys. With HSM, encrypt, decrypt, and sign with AES-256 symmetric and RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 asymmetric cryptographic keys.

Create external keys with EKM	Generate your external key using one of the following external key managers: Equinix, Fortanix, Ionic, Thales, and Unbound. Once you have linked your external key with Cloud KMS, you can use it to protect data at rest in BigQuery and Compute Engine.
Delay for key destruction	Cloud KMS has a built-in 24-hour delay for key material destruction, to prevent accidental or malicious data loss.
Encrypt and decrypt via API	Cloud KMS is a REST API that can use a key to encrypt, decrypt, or sign data such as secrets for storage.
High global availability	Cloud KMS is available in several global locations and across multi-regions, allowing you to place your service where you want for low latency and high availability.
Automated and at-will key rotation	Cloud KMS allows you to set a rotation schedule for symmetric keys to automatically generate a new key version at a fixed time interval. Multiple versions of a symmetric key can be active at any time for decryption, with only one primary key version used for encrypting new data. With EKM, create an externally managed key directly from the Cloud KSM console.
Statement attestation with HSM	With Cloud HSM, verify that a key was created in the HSM with attestation tokens generated for key creation operations.
Integration with GKE	Encrypt Kubernetes secrets at the application-layer in GKE with keys you manage in Cloud

	KMS. In addition, you can store API keys, passwords, certificates, and other sensitive data with the Secret Manager storage system.
Maintain key-data separation	With EKM, maintain separation between your data at rest and your encryption keys while still leveraging the power of cloud for compute and analytics.
Key data residency	If using Cloud KMS, your cryptographic keys will be stored in the region where you deploy the resource. You also have the option of storing those keys inside a physical Hardware Security Module located in the region you choose with Cloud HSM.
Key import	You may be using existing cryptographic keys that were created on your premises or in an external key management system. You can import them into Cloud HSM keys or import software keys into Cloud KMS.
Justified access	Get a clear reason for every decryption request that will cause your data to change state from at-rest to in-use with Key Access Justifications (beta).
Automated policy	Key Access Justifications (beta) lets you set automated policies that approve or deny access to keys based on specific justifications. Let your external key manager, provided by Google Cloud technology partners, take care of the rest.
Integrity commitment	Controls provided by Key Access Justifications are covered by Google's

	integrity commitments, so that you know they can be trusted.