Cloud External Key Manager

Beta

This product or feature is in a pre-release state and might change or have limited support. For more information, see the product launch stages (https://cloud.google.com/products/#product-launch-stages).

This topic provides an overview of Cloud External Key Manager (Cloud EKM). To create and manage external keys, see Managing Cloud EKM keys (https://cloud.google.com/kms/docs/managing-external-keys).

Overview

With Cloud EKM, you can use keys that you manage within a supported external key management partner (#supported) to protect data within Google Cloud. You can protect data at rest in BigQuery or Compute Engine persistent storage, or by calling the Cloud Key Management Service API directly.

Cloud EKM provides several benefits:

- **Key provenance:** You control the location and distribution of your externally-managed keys. Externally-managed keys are never cached or stored within Google Cloud. Instead, Cloud EKM communicates directly with the external key management partner for each request.
- **Access control:** You manage access to your externally-managed keys. Before you can use an externally-managed key to encrypt or decrypt data in Google Cloud, you must grant the Google Cloud project access to use the key. You can revoke this access at any time.
- **Centralized key management:** You can manage your keys and access policies from a single location and user interface, whether the data they protect resides in the cloud or on your premises.

In all cases, the key resides on the external system, and is never sent to Google.

Supported key managers

You can store external keys in the following external key management partner systems:

- Supported today:
  - Fortanix (https://www.fortanix.com/products/sdkms/)
  - Ionic (https://www.ionic.com/)
- Coming soon:
  - Equinix SmartKey (https://www.equinix.com/services/smartkey/)
  - Thales (https://www.thalesesecurity.com/products/hsm-management-and-monitoring)
  - Unbound Tech (https://www.unboundtech.com/)

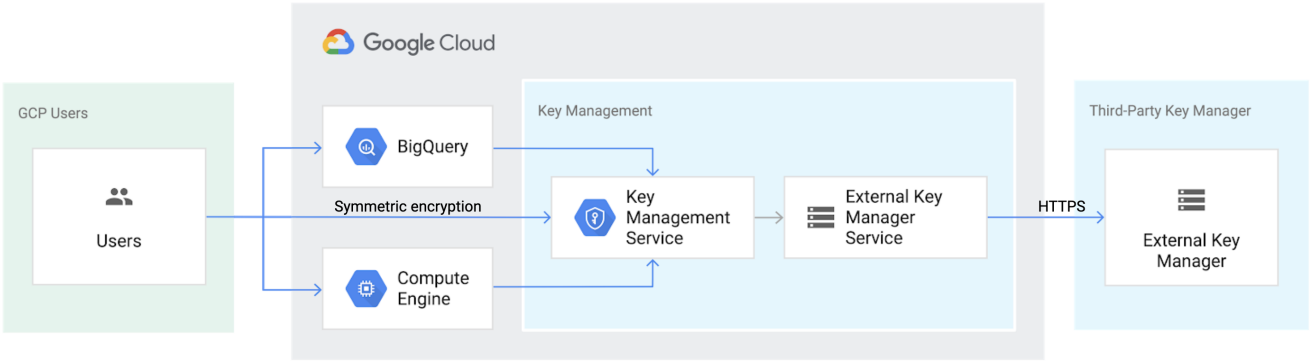
How it works

This section provides a broad overview of how Cloud EKM works with an external key. You can also follow the step-by-step instructions to create a Cloud EKM key (https://cloud.google.com/kms/docs/managing-external-keys#create_ekm_key).

1. First, you create or use an existing key in a supported external key management partner system (#supported). This key has a unique URI.
2. Next, you grant your Google Cloud project access to use the key, in the external key management partner system.
3. In your Google Cloud project, you create a Cloud EKM key, using the URI for the externally-managed key.

Within Google Cloud, the key appears alongside your other Cloud KMS and Cloud HSM keys, with protection level `EXTERNAL`. The Cloud EKM key and the external key management partner key work together to protect your data. The external key is never exposed to Google.

The following diagram shows how Cloud KMS fits into the key management model.



Caution: Both the Cloud EKM key version and the external key 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 re-create an identical Cloud EKM key version by using the same external key URI.

You can learn about the considerations (#considerations) and restrictions (#restrictions) when using Cloud EKM}.

What's next

- Read more about Cloud EKM (https://cloud.google.com/kms/docs/managing-external-keys).
- Start using the API (https://cloud.google.com/kms/docs/accessing-the-api).
- Take a look at the Cloud KMS API Reference (https://cloud.google.com/kms/docs/reference/rest/).
- Learn about Logging (https://cloud.google.com/kms/docs/audit-logging#enabling_audit_logging) in Cloud KMS. Logging is based on operations, and applies to keys with both HSM and software protection levels.

Considerations

- When you use a Cloud EKM key, Google has no control over the availability of your externally-managed key in the external key management partner system. Google can't recover your data if you lose keys you manage outside of Google Cloud.

- Review the guidelines about external key management partners and regions (#regions) when choosing the locations for your Cloud EKM keys.
- Communicating with an external service over the internet can lead to problems with reliability, availability, and latency. For applications with low tolerance for these types of risks, consider using Cloud HSM or Cloud KMS to store your key material.
    - If an external key is unavailable, Cloud KMS returns a `FAILED_PRECONDITION` error and provides details in the `PreconditionFailure` (https://cloud.google.com/kms/docs/reference/ekm_errors#input_errors) error detail.

      Enable data audit logging (https://cloud.google.com/kms/docs/audit-logging#enabling_audit_logging) to maintain a record of all errors related to Cloud EKM. Error messages contain detailed information to help pinpoint the source of the error. An example of a common error is when an external key management partner does not respond to a request within a reasonable timeframe.
    - You need a support contract with the external key management partner. Google Cloud support can only provide support for issues in Google Cloud services and cannot directly assist with issues on external systems. You may need to work with support on both sides to troubleshoot interoperability issues.

Restrictions

The following restrictions apply to this beta release.

- Only symmetric keys are supported, and only for the following:
    - Customer managed encryption keys (CMEK) in Compute Engine (https://cloud.google.com/compute/docs/disks/customer-managed-encryption) or BigQuery (https://cloud.google.com/bigquery/docs/customer-managed-encryption).
    - Symmetric encryption and decryption using Cloud KMS directly (https://cloud.google.com/kms/docs/encrypt-decrypt).
- Data that is encrypted by Cloud EKM using an externally-managed key cannot be decrypted without using Cloud EKM.
- Operations with external keys are not covered by the Cloud KMS service-level agreement. For more information, see Product launch stages (https://cloud.google.com/products/#product-launch-stages).

- Automatic rotation is not supported.
- When you create the Cloud EKM key using the API or the `gcloud` command-line tool, it must not have an initial key version. This does not apply to Cloud EKM keys created using the Cloud Console.
- The quota on cryptographic operations for all Cloud EKM keys in a single Google Cloud location per project is 600 queries per minute.

External key managers and regions

Cloud EKM needs to be able to reach your keys quickly to avoid an error. When creating a Cloud EKM key, choose a Google Cloud location that is geographically near the location of the external key management partner key. Refer to the partner's documentation for details about that partner's location availability.

You can use Cloud EKM in any Google Cloud location supported for Cloud KMS, except for `global`.

Consult your external key management partner's documentation to determine which locations they support.

Multi-region use

When you use an externally-managed key with a multi-region, the metadata of the key, including the information needed to communicate with the external key management partner, is available in multiple datacenters within the multi-region. If your application fails over from one datacenter to another within the multi-region, the new datacenter initiates key requests. The new datacenter may have different network characteristics from the previous datacenter, including distance from the external key management partner and the likelihood of timeouts. We recommend only using multi-regions with Cloud EKM if the external key management partner provides a level of coverage that corresponds to the coverage of the available Cloud EKM multi-regions.

API changes

The following API changes were made to support this beta release.

- `EXTERNAL` has been added as a new enum value to `ProtectionLevel` (https://cloud.google.com/kms/docs/reference/rest/v1/ProtectionLevel).
- A new `ExternalProtectionLevelOptions` (https://cloud.google.com/kms/docs/reference/rest/v1/projects.locations.keyRings.cryptoKeys.cryptoKeyVersions#CryptoKeyVersion.ExternalProtectionLevelOptions) field type has been added to `CryptoKeyVersion`. This field type includes a new field called `externalKeyUri`.
- `EXTERNAL_SYMMETRIC_ENCRYPTION` has been added as a new `CryptoKeyVersionAlgorithm` (https://cloud.google.com/kms/docs/reference/rest/v1/CryptoKeyVersionAlgorithm).

Last updated December 17, 2019.