Key rotation

Rotation in Cloud KMS

In Cloud Key Management Service, a *key rotation* is represented by generating a new key version of a key, and marking that version as the *primary* version.

Creating a new key version generates the new cryptographic key material, and marking that key version as primary causes it to be used to encrypt any new data. Each key has a designated primary version at any point in time, which Cloud KMS uses to encrypt data, by default.

Rotating a key doesn't disable or destroy previous key versions. The previous key versions will no longer be primary, but they remain available for decrypting data.

Reasons for rotating a key

Rotating keys makes it easy to comply with standardized security practices, such as Payment Card Industry Data Security Standard (https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss) (PCI DSS) requirements. Regularly rotating keys is a security best practice for the following reasons.

- To limit the number of encrypted messages available to cryptanalysis for a specific key version. Similarly, to limit the total number of enciphered bytes available to cryptanalysis for a specific key version. Key lifetime recommendations are algorithm-specific and based on either the number of messages produced or the total number of bytes enciphered. For example, the recommended key lifetime for symmetric keys in Galois/Counter Mode (GCM) is based on the number of messages encrypted, as noted at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf).
- To ensure your system is prepared in the event you need to rotate to a stronger algorithm. If key rotation is not part of your ongoing operation, a system tends to become dependent on specific keys, which makes it very difficult to initiate key rotation after an incident.

Similarly, to ensure your system is prepared if a key is leaked. The first time you try key rotation should not be during real-time recovery from an incident.

- To reduce the volume of ciphertext that would be unprotected if a key version is compromised.
- To prevent use of a key version that is compromised or suspected of being compromised.

Frequency of key rotation

Encryption keys may be rotated in two ways:

- *Regular rotation*: Regularly rotate the encryption key used, limiting the amount of data protected by a single key. Regular rotation may be required for internal business compliance.
- *Irregular rotation*: Ad-hoc rotation after a suspected incident, as an additional stopgap. Data encrypted with the previous version of the key may also need to be re-encrypted.

Having a regular rotation schedule, for example every 90 days, provides some security benefit without significant complexity. Regular rotation limits the amount of data encrypted with a single key, avoids key lock-in in case an irregular rotation is needed, and allows key version disablement to be used to restrict access to older data.

A more stringent and complex implementation could also have a disablement schedule, to re-encrypt older data and disable keys after a certain time period, e.g., 20 key versions enabled for up to 5 years of data. This is difficult to implement securely and correctly.

It is not recommended to rely solely on irregular rotation, but rather to use irregular rotation if needed in conjunction with a regular rotation schedule.

Automatic rotation

By providing a *rotation schedule*, Cloud KMS will automatically rotate your keys for you. A key's rotation schedule can be set using the `gcloud` command-line tool or the Google Cloud Console.

A rotation schedule is defined by a *rotation period* and a *next rotation time*. The rotation period is the time between when new key versions are generated automatically, and must be at least one day. The next rotation time is the date of the next scheduled rotation, which must be in the future. Automatic rotation will start at the next rotation time, and occur every rotation period thereafter.

If only the next rotation time is specified (with no rotation period), the key will be scheduled for a single rotation on that date, at which point the field will be cleared. Specifying only the rotation period without a next rotation time results in an error.

Key rotations performed manually via the `CreateCryptoKeyVersion` and `UpdateCryptoKeyVersion` methods do not affect a key's rotation schedule.

When enabling automatic rotation with the `gcloud` tool, you can specify any length of time for the rotation period. When enabling automatic rotation in the Cloud Console, the rotation period offers common options (e.g., 30 days) but you can also set it to a custom number of days.

Manual rotation

Manual rotation can be used for irregular key rotation, as well as for regular key rotation managed outside of Cloud KMS. Keys can be manually rotated using the `gcloud` tool or the Cloud Console.

Rotation considerations

- **Using the key rotation commands above, key rotation does NOT re-encrypt already encrypted data with the newly generated key version.** If you suspect unauthorized use of a key, you should re-encrypt (https://cloud.google.com/kms/docs/re-encrypt-data) the data protected by that key and then disable (https://cloud.google.com/kms/docs/enable-disable) or schedule destruction (https://cloud.google.com/kms/docs/destroy-restore) of the prior key version.

Last updated December 17, 2019.