What to do after key renewal

The Cryptomathic AWS BYOK Service will renew (or rotate) keys at most 24 hours before their rotation date.

The purpose of this guide is to describe what a user should do to make use of the new key instead of the old (rotated) key.

What happens when my key is approaching its rotation time?

14 days before rotation time the user will receive an email informing that the key is up for renewal (or rotation).

24 hours (at most) before rotation time the key will be renewed i.e. a new key will be created, and the new key material will be uploaded to the KMS. The alias of the old key will be updated to point to the new key. The original key will still be active and usable. Finally the user will receive an email about the renewal.

Recommended approach

Cryptomathic strongly suggest that user where applicable comply to the official AWS guidelines and therefore use *aliases* as described here:

https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually

This is applicable for services such as:

- S3 Server-site encryption
- S3 Encryption Client SDK
- DynamoDB Encryption Client SDK
- AWS Encryption SDK

New objects will be encrypted with the new key, and existing objects will be decrypted with the original key which is still enabled.

Other services

For services which do not support the use of aliases for referencing encryption keys a manual re-encryption must take place. For example for DynamoDB tables which are not encrypted using the DynamoDB Encryption Client SDK use the following guide:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/encryption.tutorial.html#encryption.tutorial-update