Basic AWS BYOK Service concepts

The following are the basic concepts you need to understand to be able to use Cryptomathic's BYOK service.

Keystore

A keystore in Cryptomathic's BYOK service is a collection of keys. The keystore is connected to a specific AWS account and a specific AWS region. You can create multiple keystores to manage keys in different AWS regions, AWS accounts, or to group your keys logically.

Please also refer to FAQ: *Which AWS regions are supported*.

Key

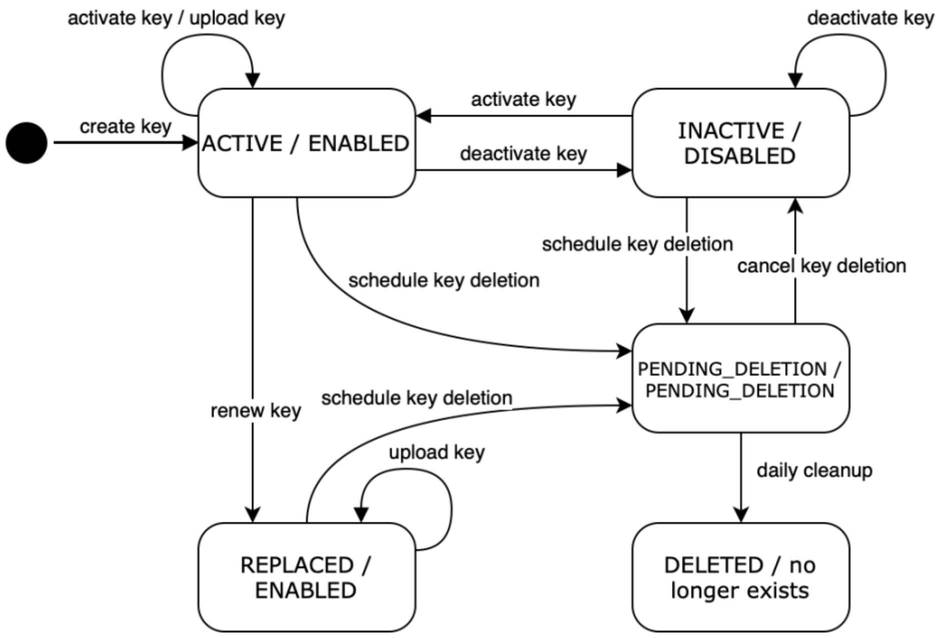
A key in Cryptomathic's BYOK service represents a key that was created using the service and is located in AWS Key Management Service (KMS) on the AWS account and in the region defined by the user.

Key Lifecycle

The life cycle of an individual BYOK key is described in the following table.

Operation	**Allowed in BYOK key state**	**Action**
Create key	N/A	A key is created in BYOK and in KMS, key material is generated and uploaded to KMS. BYOK key state is ACTIVE, KMS state ENABLED.
Deactivate key	ACTIVE, INACTIVE (no-op)	The key state in BYOK is set to INACTIVE, the KMS key is DISABLED, and the key material is removed from the KMS key making it EMPTY.
Activate key	INACTIVE, ACTIVE (no-op)	The key material is re-uploaded to the KMS key. The BYOK key state is set to ACTIVE, and the KMS state is set to ENABLED.
Upload key	ACTIVE, REPLACED	Re-uploads key material to KMS. If the KMS key state was EMPTY after a power-fail, the new state will be ENABLED. No change to the BYOK key state.
Renew key	ACTIVE	Creates a new BYOK key and KMS key from the existing key and redirects the alias. The original key is set to BYOK key state REPLACED.
Schedule key deletion	ACTIVE, INACTIVE, REPLACED, PENDING_DELETION (no-op), DELETED (no-op)	The BYOK key state is set to PENDING_DELETION, and the KMS key is set to PENDING_DELETION. Note that the KMS key cannot be used for crypto in this state. So any unintended bad effects of deleting the key in the future can be discovered immediately.

Cancel key deletion	PENDING_DELETION	Cancels BYOK and KMS key deletion. The BYOK key state is set to INACTIVE, and the KMS key state is set to DISABLED. The key material is removed from the KMS key making it EMPTY
Daily cleanup	PENDING_DELETION	If the scheduled deletion grace period has ended, sets the BYOK state to DELETED, and destroysthe key material. Audit log entries can still be accessed.
Delete keystore	All keys in the keystore must be DELETED already	The keystore is marked DELETED.Audit log entries can still be accessed.
Prepare download key	Any state except DELETED	A 2K RSA public key is supplied for later wrapping of the customer key material. The user id from the ID token is marked.
Download key	Any state except DELETED	Key material is downloaded (exported) to the customer wrapped with the previous prepared 2K RSA public key. The user id from the ID token must be different from the marked user. The public key and the user id mark on the key are cleared.
Update key	ACTIVE, INACTIVE	Updates the key properties: name, expires, tags, alias



AWS connection

Granting Cryptomathic's BYOK access and connection to your AWS account is achieved by creating a role and a policy in the AWS Identity Access Management (IAM) service on your AWS account. The service only needs access to specific parts of the KMS API, and we recommend you follow our guide to grant the access in accordance with the principle of least privilege. By allowing Cryptomathic's BYOK service to assume this role it is possible for the service to connect to your AWS account. Only the Cryptomathic BYOK service will be able to access your account using this role and only the specific parts of the KMS API that are needed are accessible.

Read this section *How to set up a role related to a key store* to learn how to create the role and policy on your AWS account.