Key Management Service (KMS)

- create and control the encryption keys used to encrypt your data.
- integrated with other AWS services including EBS, S3, Amazon Redshift, Elastic Transcoder, WorkMail, Relational Database Service
- encryption keys are bound by region.

Customer Master Key (CMK)

- can't be exported - **ALWAYS LIVE IN KMS**
- alias
- creation date
- description
- key state
- **key material** (either customer provided or AWS provided)

Setup of CMK

- create alias and description
- choose material option (KMS generated key or your own key material)

API Calls to know

```
aws kms encrypt --key-id KEYHERE --plaintext fileb://secret.txt --output
text --query CipherTextBlob | base64 --decode > encryptedsecret.txt

aws kms decrypt --ciphertext-blob fileb://encryptedsecret.txt --output
text --query Plaintext | base64 ---decode > decryptedsecret.txt

aws kms re-encrypt --destination-key-id KEYHERE --ciphertext-blob
fileb://encryptedsecret.txt | base64 > newencryption.txt ## encrypt but
destroy plaintext version

aws kms enable-key-rotation --key-id KEYHERE ## need perm acces here
```

Envelope Encryption

Process of encrypting envelope key

- Customer Master Key is used to decrypt the data key (envelope key)
- Envelope Key is used to decrypt the data