General

* AWS KMS – easily create and control keys used for cryptographic operations; encrypt or digitally sign data within your own applications
* The service provides a highly available key generation, storage, management, and auditing solution for you to encrypt or digitally sign data within your own applications or control the encryption of data across AWS services
* you should use it to centrally manage the encryption keys that control access to your data.
* Use aws encryption sdk with aws kms to easily generate use and pretect symmetric encryption keys in your code
* For asymmetric keys use the service to create and manage private keys
* Use it to reducte your licensing costs and oeperational bueden
* Proving data security for regulatory or compliance purposes facilitates proving your data is consistently protected
* CMKs in AWS KMS
* AWS KMS APIs to encrypt data using aws encryption sdk
* Symmetric vs asyummetric key
* Iam roles and users to manage keys
* Iam roles and users to encrypt and dycrypt data
* Automatically rotated on an annual basis
* Temporarily disable keys so thye cannot be used by anyone
* Re-enable disabled keys
* Schedule deletion of keys that you no longer use
* Audit use of keys by inspectinglogs
* You start using the service by requesting the creation of a CMK. You control the lifecycle of the CMK as well as who can use or manage it. The key material for a CMK is generated within hardware security modules (HSMs) managed by AWS KMS. Alternatively, you can import key material from your own key management infrastructure and associate it with a CMK. You can also have the key material generated and used in an AWS CloudHSM cluster as a part of the custom key store feature in AWS KMS.
* Data encryption using AWS KMS
  + AWS KMS APIS to encrypt and decrypt using CMKs stored in the service
  + AWS services encrypt you data using your CMKs stored in the service
  + AWS Ecryption SDK that is integrated with AWS KMS

While AWS KMS does support sending data up to 4 KB to be encrypted directly, envelope encryption can offer significant performance benefits. Envelope encryption reduces the network load since only the request and delivery of the much smaller data key go over the network.

The data key is used locally in your application or encrypting AWS service, avoiding the need to send the entire block of data to AWS KMS and suffer network latency.

Customer Key Store

Billing

Security