**ENCRYPTION**

**When**  we are sending our credit card information over the network then we do not want it to be seen and misused by anyone.Thus to ensure the security we use the in flight encryotion process.

Graphical user interface, text

Description automatically generated

SERVER SIDE ENCRYPTION

Diagram

Description automatically generated with medium confidence

Diagram

Description automatically generated with low confidence

**Text

Description automatically generated**

Text

Description automatically generated

Any time we listen of encryption then it is done by the kms.Aws manages the kms keys and we do not have to do much about it.It is very easy to control access to our data which is encrypted with kms.

There are two types of knms keys:

1/symmetric key:

In this we have only one key being used for encryption and decryption.

Aws services that are integrated with kms use the symmetric customer master keys.

A point to be noted is that we do not get access to the kms key but what we do is that we directly call the kms api to encryptour data.

2.Asymmetric

Text, letter

Description automatically generated

Diagram

Description automatically generateds

Graphical user interface, text, application, email

Description automatically generated

**HOW KMS WORKS**

**Graphical user interface, application

Description automatically generated**

**S**uppose we have a secret which we want to keep safe.So we will call the encrypt api then the kms after checking the iam permission wull do the encryption for us and send us back the encrypted data.

Next when we want to decrypt then we will call a decrypt api which will decryt our text and will send us back the decrypted data.

**whewGraphical user interface, text, application, email

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**When we have a data which is more than 4kb it has to be encrypted with the envelope encryption.**

Suppose w ehave a big file of size 10mb and we want to encrypt it.so we will call the generatedatakey api which will go to kms.Kms in return will generate a data key using the cmk and will send us back a plaintext data encypted file which we use to encrypt our data.

All the encryption is done at the client side only.

Now kms will send us and encrypted data key which we will put in our envelope along with the encrypted file.

DECRYPT ENVELOPE DATA

A picture containing diagram

Description automatically generated

**ENCRYPTION SDKGraphical user interface, text, application

Description automatically generated**

**Text

Description automatically generated**

KMS  **LIMITS**

There are some limits set to use the kms.There is a specified number of request quota which is set by aws to make a call to the generateDAtaKey api.

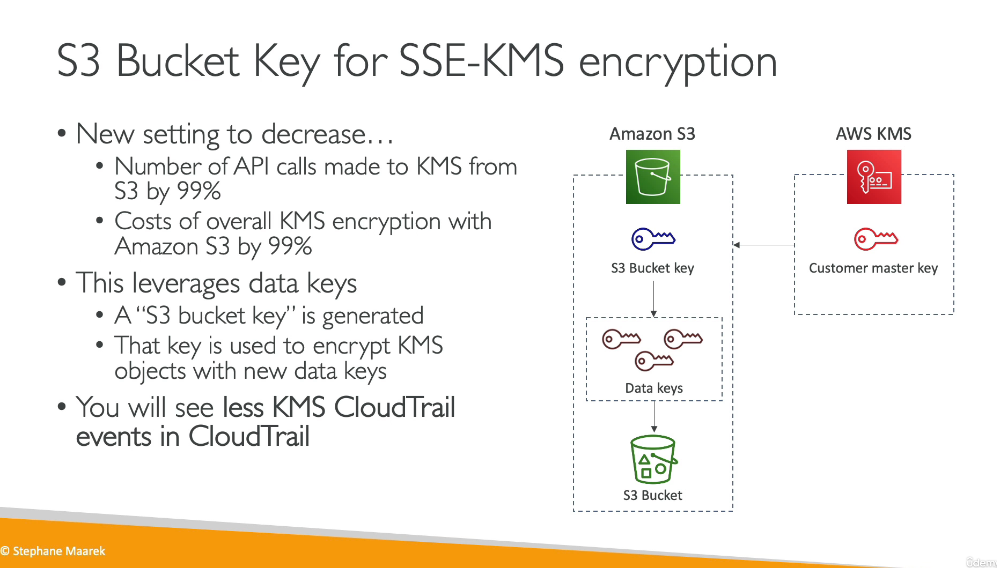
So when we exceed that quota then we will get the throttling exception.

So solution is to do an exponential backoff.or you can cache the dek.

Graphical user interface, text, application, email

Description automatically generated

**S3 BUCKET KEY FOR SSE KMS ENCRYPTION**

In order to reduce the number of calls to the aws kms. 

**AWS SECRET MANAGER**

**Text, letter

Description automatically generated**