# S3 Encryption for Objects

If you are studying for AWS Developer Associate Exam, this guide will help you with quick revision before the exam. it can use as study notes for your preparation.

Dashboard Other Certification Notes

## S3 Encryption for Objects

- There are 4 methods of encrypting objects in S3
  - SSE-S3: encrypt S3 objects using keys handled and managed by AWS
  - SSE-KMS: use AWS KMS to manage encryption keys
  - SSE-C: use KMS custom keys to encrypt data
  - Client Side Encryption

### SSE-KMS

- Allows to do server side encryption in S3, keys are handled and managed by KMS
- KMS: user control + audit trail
- In order to SSE-KMS to work, we must set the following header: **x-amz=server-side-encryption": "aws:kms"**

### SSE-KMS Deep Dive

- Under the hood SSE-KMS uses *GenerateDataKey* and *Decrypt* KMS API calls
- These KMS API calls will show up in CloudTrails, useful for logging and audit
- In order to be able to perform SS3-KMS, we need:
  - A KMS key policy to authorize the user/role
  - An IAM policy to authorize access to KMS
- S3 calls to KMS for SSE-KMS will count against our KMS limits

### S3 Bucket Policies

#### Force SSL

- We can create an S3 bucket policy with a DENY condition of **aws:SecurityTransport=false**
- Note: using an allow on the same condition would allow anonymous *GetObject* if SSL is used

### Force SSE-KMS Encryption

- Deny any incorrect encryption header: make sure it includes `aws:kms`
- Deny no encryption header to ensure objects are not uploaded un-encrypted