

**Task - Work on S3 managed keys / aws customer-managed keys / encrypting files before uploading to S3 using customer-managed aws keys and also using S3 managed keys.**

### **AWS Key Management Service (KMS)**

AWS Key Management Service (KMS) makes it easy for us to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide us with logs of all key usage to help meet your regulatory and compliance needs.

In simple word, it can easily create and control the key used to encrypt or digitally sign our data

Benefits:

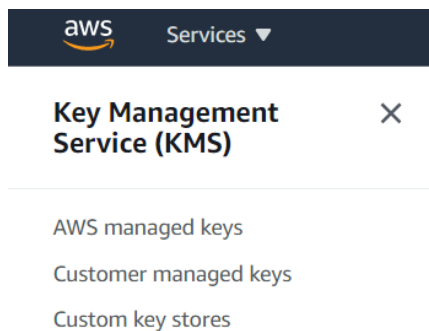
- Fully managed  
We control access to your encrypted data by defining permissions to use keys while AWS KMS enforces your permissions and handles the durability and physical security of your keys.
- Centralized key management:  
AWS KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications. We can easily create, import, rotate, delete, and manage permissions on keys from the AWS Management Console or by using the AWS SDK or CLI.
- Digitally sign data  
AWS KMS enables us to perform digital signing operations using asymmetric key pairs to ensure the integrity of your data. Recipients of digitally signed data can verify the signatures whether they have an AWS account or not.

This is the first view of AWS KMS



Here we can see in aws kms there is two methods -

1. Customer managed keys
2. Aws managed keys

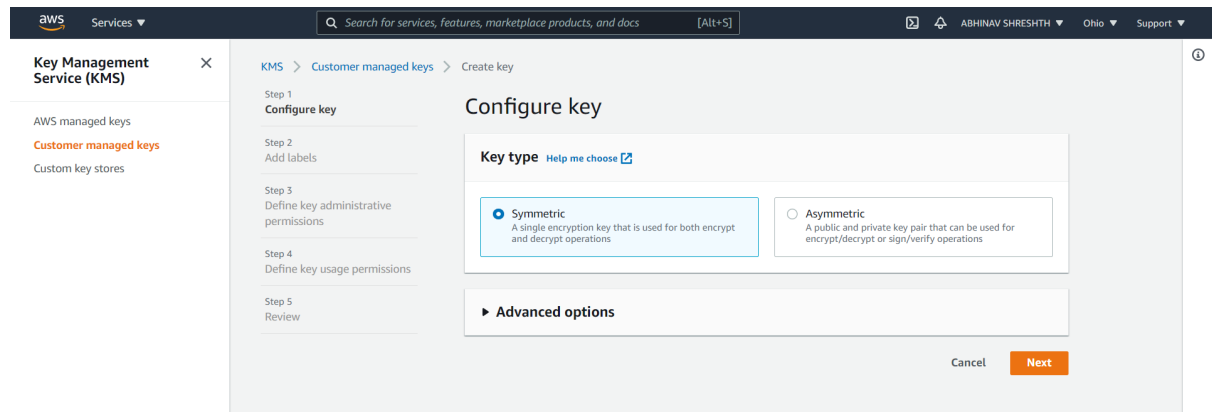


Difference between Aws managed keys and customer-managed keys

	<b>AWS-managed CMK</b>	<b>Customer-managed CMK</b>
Creation	AWS generated on the customer's behalf	Customer-generated
Rotation	Once every three years automatically	Once a year automatically through opt-in or on-demand manually
Deletion	Can't be deleted	Can be deleted
Scope of use	Limited to a specific AWS service	Controlled via KMS/IAM policy
Key Access Policy	AWS managed	Customer managed
User AccessManagement	IAM policy	IAM policy

Encryption is the process of taking a message and scrambling it's contents so that only certain people can look at your message.

There are two types of encryption: symmetric and asymmetric encryption.



**Symametic Encryption:** according to Wikipedia, Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

The main [advantage](#) of symmetric encryption over asymmetric encryption is that it is fast and efficient for large amounts of data; the [disadvantage](#) is the need to keep the key secret - this can be especially challenging where encryption and decryption take place in different locations.

**Asymmetric Encryption:** according to google Asymmetric encryption is a type of encryption that uses two separates yet mathematically related keys to encrypt and decrypt data

## Master key

A key created by AWS KMS can only be used within the AWS KMS service. The master key is commonly used to encrypt data keys so that the encrypted key can be securely stored by your service. However, AWS KMS master keys can also be used to encrypt or decrypt arbitrary chunks of data that are no greater than 4 KiB. Master keys are categorized as either customer-managed keys or AWS managed keys. Customer managed keys are created by a customer for use by a service or application. AWS managed keys are the default keys used by AWS services that support encryption.

## Data key

A symmetric key generated by AWS KMS for your service. Inside of your service or custom application, the data key is used to encrypt or decrypt data. It can be considered a resource by a service or

application, or it can simply be metadata associated with the encrypted data.

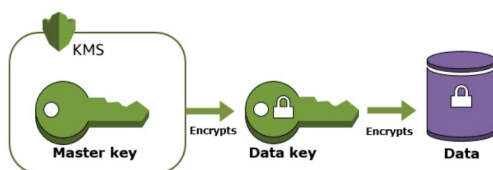
### Envelope Encryption

When you encrypt your data, your data is protected, but you have to protect your encryption key. One strategy is to encrypt it. Envelope encryption is the practice of encrypting plaintext data with a data key, and then encrypting the data key under another key.

You can even encrypt the data encryption key under another encryption key, and encrypt that encryption key another encryption key. But, eventually, one key must remain in plaintext so you can decrypt the keys and your data. This top level plaintext key encryption key is known as the master key



And AWS KMS helps you to protect your master keys by storing and managing them securely. Master keys stored in AWS KMS, known as customer master keys (CMKs), never leave the AWS KMS FIPS validated hardware security modules unencrypted. To use an AWS KMS CMK, you must call AWS KMS.



### Key policy

When you create a CMK, you determine who can use and manage that CMK. These permissions are contained in a document called the key policy. You can use the key policy to add, remove, or change permissions at any time for a customer-managed CMK. But you cannot edit the key policy for an AWS managed CMK. For more information, see [Using key policies in AWS KMS](#).

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Ohio

Support

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

KMS

Customer managed keys

Create key

Step 1

Configure key

Step 2

Add labels

Step 3

Define key administrative permissions

Step 4

Define key usage permissions

Step 5

Review

Configure key

Key type

Help me choose

☒ Symmetric

A single encryption key that is used for both encrypt and decrypt operations

☐ Asymmetric

A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

Advanced options

Key material origin

Help me choose

☐ KMS

☒ External

☐ Custom key store (CloudHSM)

You can import a symmetric 256-bit key from your key management infrastructure into KMS and use it like any other customer master key.

☒ I understand the security, availability, and durability implications of using an imported key.

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Ohio

Support

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

KMS

Customer managed keys

Create key

Step 1

Configure key

Step 2

Add labels

Step 3

Define key administrative permissions

Step 4

Define key usage permissions

Step 5

Review

Add labels

Alias

You can change the alias at any time. Learn more

Alias

cmk1-ext

Description - optional

You can change the description at any time.

Description - optional

cmk1-ext description

Tags - optional

You can use tags to categorize and identify your CMKs and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

This key has no tags.

Add tag

You can add up to 50 more tags.

Cancel

Previous

Next

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

Step 1  
Configure key

Step 2  
Add labels

Step 3  
Define key administrative permissions

Step 4  
Define key usage permissions

Step 5  
Review

KMS > Customer managed keys > Create key

Define key administrative permissions

Key administrators

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

< 1 >

<input checked="" type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	AWSServiceRoleForEMRCleanup	/aws-service-role/elasticmapreduce.amazonaws.com/	Role
<input checked="" type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/	Role
<input checked="" type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/	Role
<input checked="" type="checkbox"/>	EMR_DefaultRole	/	Role
<input checked="" type="checkbox"/>	EMR_EC2_DefaultRole	/	Role
<input checked="" type="checkbox"/>	EMR_Notebooks_DefaultRole	/	Role

Key deletion

☒ Allow key administrators to delete this key.

Cancel

Previous

Next

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

Step 2  
Add labels

Step 3  
Define key administrative permissions

Step 4  
Define key usage permissions

Step 5  
Review

This account

Select the IAM users and roles that can use the CMK in cryptographic operations. [Learn more](#)

< 1 >

<input checked="" type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	AWSServiceRoleForEMRCleanup	/aws-service-role/elasticmapreduce.amazonaws.com/	Role
<input checked="" type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.amazonaws.com/	Role
<input checked="" type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	/aws-service-role/trustedadvisor.amazonaws.com/	Role
<input checked="" type="checkbox"/>	EMR_DefaultRole	/	Role
<input checked="" type="checkbox"/>	EMR_EC2_DefaultRole	/	Role
<input checked="" type="checkbox"/>	EMR_Notebooks_DefaultRole	/	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Add another AWS account

Cancel

Previous

Next

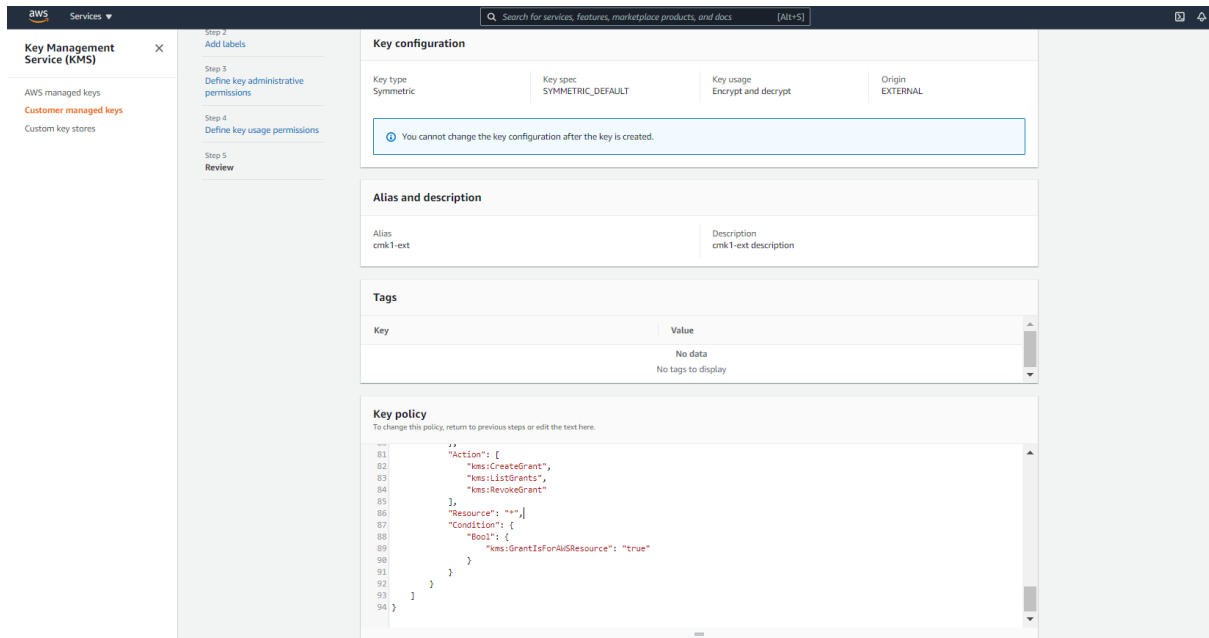
Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use



```

{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::431440931115:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::431440931115:role/aws-service-role/elasticmapreduce.amazonaws.com/AWSServiceRoleForEMRCleanup",
          "arn:aws:iam::431440931115:role/aws-service-role/support.amazonaws.com/AWSServiceRoleForSupport",

```

```
        "arn:aws:iam::431440931115:role/aws-service-
role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor",
```

```
"arn:aws:iam::431440931115:role/EMR_DefaultRole",
```

```
"arn:aws:iam::431440931115:role/EMR_EC2_DefaultRole",
```

```
"arn:aws:iam::431440931115:role/EMR_Notebooks_DefaultRole"
```

```
    ]
```

```
  },
```

```
  "Action": [
```

```
    "kms:Create*",
```

```
    "kms:Describe*",
```

```
    "kms:Enable*",
```

```
    "kms:List*",
```

```
    "kms:Put*",
```

```
    "kms:Update*",
```

```
    "kms:Revoke*",
```

```
    "kms:Disable*",
```

```
    "kms:Get*",
```

```
    "kms:Delete*",
```

```
    "kms:ImportKeyMaterial",
```

```
    "kms:TagResource",
```

```
    "kms:UntagResource",
```

```
    "kms:ScheduleKeyDeletion",
```

```
    "kms:CancelKeyDeletion"
```

```
  ],
```

```
  "Resource": "*"
},
```

```
{
```

```
{
```

```
  "Sid": "Allow use of the key",
```

```
  "Effect": "Allow",
```

```
  "Principal": {
```

```
    "AWS": [
```



```

        "arn:aws:iam::431440931115:role/aws-service-
role/elasticmapreduce.amazonaws.com/AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::431440931115:role/aws-service-
role/support.amazonaws.com/AWSServiceRoleForSupport",
        "arn:aws:iam::431440931115:role/aws-service-
role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor",

"arn:aws:iam::431440931115:role/EMR_DefaultRole",

"arn:aws:iam::431440931115:role/EMR_EC2_DefaultRole",

"arn:aws:iam::431440931115:role/EMR_Notebooks_DefaultRole"
    ]
},
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::431440931115:role/aws-service-
role/elasticmapreduce.amazonaws.com/AWSServiceRoleForEMRCleanup",
            "arn:aws:iam::431440931115:role/aws-service-
role/support.amazonaws.com/AWSServiceRoleForSupport",
            "arn:aws:iam::431440931115:role/aws-service-
role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor",

"arn:aws:iam::431440931115:role/EMR_DefaultRole",

```

```

"arn:aws:iam::431440931115:role/EMR_EC2_DefaultRole",

"arn:aws:iam::431440931115:role/EMR_Notebooks_DefaultRole"

    ]

},

"Action": [

    "kms:CreateGrant",

    "kms:ListGrants",

    "kms:RevokeGrant"

],

"Resource": "*",

"Condition": {

    "Bool": {

        "kms:GrantIsForAWSResource": "true"

    }

}

}

]

}

```

This (above) is the key policy

The screenshot shows the AWS Management Console for the Key Management Service (KMS). A green success banner at the top states: "Success Your customer master key was created with alias cmk1-ext and key ID 4f0e984c-2bac-4ea7-b164-2c2d58f3bde4. To use this CMK, you must import key material." Below this, the breadcrumb navigation is "KMS > Customer managed keys > 4f0e984c-2bac-4ea7-b164-2c2d58f3bde4 > Import key material". The left sidebar shows "Key Management Service (KMS)" with options for "AWS managed keys", "Customer managed keys" (selected), and "Custom key stores". The main content area is titled "Download wrapping key and import token" and contains a "Wrapping key and import token" box. Inside this box, it instructs the user to select a wrapping algorithm (currently set to "RSAES\_OAEP\_SHA\_256") and click the "Download wrapping key and import token" button. A note at the bottom of the box states: "This wrapping key and import token will expire in 24 hours." At the bottom right of the main content area are "Cancel" and "Next" buttons. The footer of the console shows "Feedback", "English (US)", and copyright information for Amazon Internet Services Private Ltd.

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Ohio

Support

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

Step 1

Download wrapping key and import token

Step 2

Upload your wrapped key material

Upload your wrapped key material

Encrypted key material and import token

Use your wrapping key to encrypt your key material. Then, upload the wrapped key material and the import token that you downloaded. [Learn more](#)

CMK ARN

arn:aws:kms:us-east-2:431440931115:key/4f0e984c-2bac-4ea7-b164-2c2d58f3bde4

Alias

cmk1-ext

Wrapped key material

Choose file

Import token

Choose file

Expiration option

Set an expiration time. The key material is deleted at the expiration time.

☐ Key material expires

Cancel

Previous

Upload key material

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Cookie preferences

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

Step 1

Download wrapping key and import token

Step 2

Upload your wrapped key material

Upload your wrapped key material

Encrypted key material and import token

Use your wrapping key to encrypt your key material. Then, upload the wrapped key material and the import token that you downloaded. [Learn more](#)

CMK ARN

arn:aws:kms:us-east-2:431440931115:key/4f0e984c-2bac-4ea7-b164-2c2d58f3bde4

Alias

cmk1-ext

Wrapped key material

Choose file

Import token

Choose file

Expiration option

Set an expiration time. The key material is deleted at the expiration time.

☐ Key material expires

Cancel

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates

ImportParameters.zip

## Upload your wrapped key material

### Encrypted key material and import token


Use your wrapping key to encrypt your key material. Then, upload the wrapped key material and the import token that you downloaded. [Learn more](#)

CMK ARN

arn:aws:kms:us-east-2:431440931115:key/4f0e984c-2bac-4ea7-b164-2c2d58f3bde4

Wrapped key material

 Choose file


 Wrapped key material is required

Alias

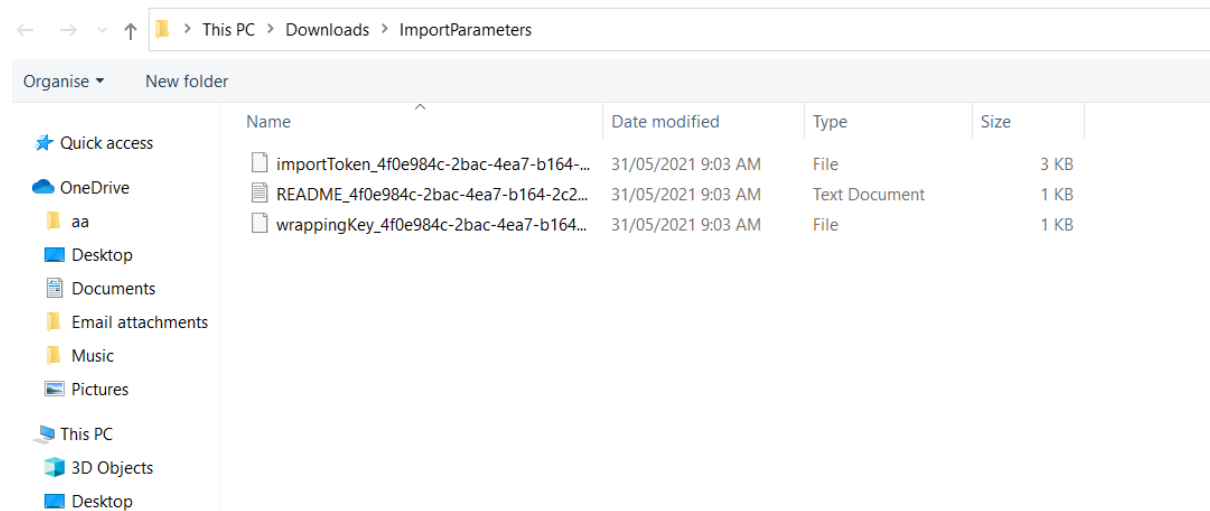
cmk1-ext

Import token

 Choose file

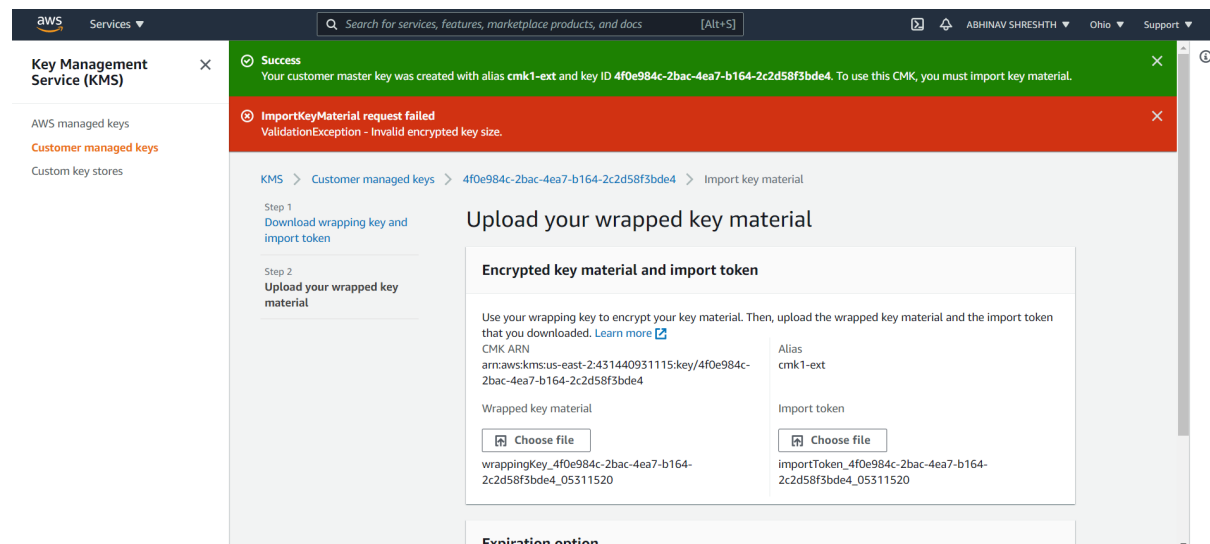
 Import token is required

Open



And I uploaded it

**Issue -** Got stuck



Rolling back –

## Encrypting using Customer managed keys –

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

ABHINAV SHRESHTH Mumbai

**Key Management Service (KMS)**

AWS managed keys

**Customer managed keys**

Custom key stores

KMS > Customer managed keys > Create key

Step 1  
**Configure key**

Step 2  
Add labels

Step 3  
Define key administrative permissions

Step 4  
Define key usage permissions

Step 5  
Review

### Configure key

**Key type** [Help me choose](#)

☒ **Symmetric**  
A single encryption key that is used for both encrypt and decrypt operations

☐ **Asymmetric**  
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

**Advanced options**

**Key material origin**  
[Help me choose](#)

☒ **KMS**

☐ External

☐ Custom key store (CloudHSM)

Cancel **Next**

After some steps –

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

ABHINAV SHRESHTH Mumbai

**Key Management Service (KMS)**

AWS managed keys

**Customer managed keys**

Custom key stores

KMS > Customer managed keys > Create key

Step 1  
Configure key

Step 2  
Add labels

Step 3  
Define key administrative permissions

Step 4  
Define key usage permissions

Step 5  
**Review**

### Review

**Key configuration**

Key type Symmetric	Key spec SYMMETRIC_DEFAULT	Key usage Encrypt and decrypt	Origin AWS_KMS
-----------------------	-------------------------------	----------------------------------	-------------------

**You cannot change the key configuration after the key is created.**

**Alias and description**

Alias cmk-aws-key	Description -
----------------------	------------------

**Tags**

Key	Value
No data	
No tags to display	

**Key policy**  
To change this policy, return to previous steps or edit the text here.

```

1 {
2   "Id": "key-consolepolicy-3",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Enable IAM User Permissions",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::431440931115:root"
10      },

```

After all the procedure

The screenshot shows the AWS Key Management Service (KMS) console. The left sidebar has a search bar and a list of services. The main content area displays the configuration for a specific key. The key ID is `edb6f9d5-5afa-4b5c-b506-9ef17360c3ea`. The key is in the 'General configuration' tab, showing its status as 'Enabled' and its creation date as 'May 31, 2021 17:18 GMT+5:30'. The key's ARN is `arn:aws:kms:ap-south-1:431440931115:key/edb6f9d5-5afa-4b5c-b506-9ef17360c3ea`. Below the general configuration, there are tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key rotation', and 'Aliases'. The 'Key policy' tab is selected, showing a 'Switch to policy view' button. The 'Key administrators' section is also visible, with an 'Add' button.

Key Management Service (KMS)

Search for services, features, marketplace products, and docs [Alt+S]

ABHINAV SHRESHTH Mumbai Support

Key ID: edb6f9d5-5afa-4b5c-b506-9ef17360c3ea

Key actions Edit

General configuration

Alias cmk-aws-key	Status Enabled	Creation date May 31, 2021 17:18 GMT+5:30
ARN arn:aws:kms:ap-south-1:431440931115:key/edb6f9d5-5afa-4b5c-b506-9ef17360c3ea	Description -	

Key policy Cryptographic configuration Tags Key rotation Aliases

Key policy Switch to policy view

Key administrators  
Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Add Remove

The screenshot shows the AWS S3 console. The left sidebar has a search bar and a list of services. The main content area displays the 'Bucket Key' settings for a bucket. The 'Bucket Key' section is expanded, showing the 'Choose from your AWS KMS keys' option selected. The key ARN is `arn:aws:kms:ap-south-1:431440931115:key/edb6f9d5-5afa-4b5c-b506-9ef17360c3ea`. The 'Create key' button is visible. A blue box contains a message: 'Bucket Key is disabled for objects uploaded, modified, or copied in this bucket. Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. [Learn more](#)'. The 'Bucket Key' section also includes a description: 'Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)'. The 'Disable' option is selected under the 'Bucket Key' section. The 'Specified objects' section is also visible.

Search for services, features, marketplace products, and docs [Alt+S]

ABHINAV SHRESHTH Mumbai Support

An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

• AWS Key Management Service key (SSE-KMS)  
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

☐ AWS managed key (aws/s3)  
arn:aws:kms:ap-south-1:431440931115:alias/aws/s3

☒ Choose from your AWS KMS keys

☐ Enter AWS KMS key ARN

AWS KMS key

arn:aws:kms:ap-south-1:431440931115:key/edb6f9d5-5afa-4b5c-b506-9ef17360c3ea Create key

**Bucket Key is disabled for objects uploaded, modified, or copied in this bucket**  
Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. [Learn more](#)

Bucket Key  
Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)

☒ Disable  
☐ Enable

Specified objects

Final document –

## Buckets (3)

Buckets are containers for data stored in S3. [Learn more](#) 

 Find buckets by name



	Name ▲	AWS Region
<input type="radio"/>	<a href="#">aws-emr-resources-431440931115-us-east-2</a>	US East (Ohio) us-east-2
<input type="radio"/>	<a href="#">aws-logs-431440931115-us-east-2</a>	US East (Ohio) us-east-2
<input type="radio"/>	<a href="#">deinternbucket</a>	Asia Pacific (Mumbai) ap-sou




Amazon S3 > deinternbucket

## deinternbucket



**Objects** | Properties | Permissions | Metrics | Management | Access Points

### Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#)  to get a list of all objects in your bucket. For others to access your objects, you'll need to set permissions. [Learn more](#) 

  Copy URL  Open  Download  Delete  Actions ▼  Create folder  Upload

 Find objects by prefix

<input type="checkbox"/>	Name ▲	Type ▼	Last modified ▼	Size ▼	Size
<input type="checkbox"/>	 <a href="#">j-2JODYL3ZZDV5Z/</a>	Folder	-	-	-
<input type="checkbox"/>	 <a href="#">Test.txt</a>	txt	May 31, 2021, 17:19:36 (UTC+05:30)	15.0 B	S

Here I am encrypting test.txt

**Amazon S3** ×

Read the S3 resources page for documentation and technical content. [Learn more](#) ×

**Buckets**

- Access Points
- Object Lambda Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

► **Storage Lens**

Feature spotlight [?](#)

► AWS Marketplace for S3

**Server-side encryption settings** [Edit](#)

Server-side encryption protects data at rest. [Learn more](#)

Default encryption  
Enabled

Server-side encryption  
AWS-KMS master-key (SSE-KMS)

AWS KMS key ARN  
[arn:aws:kms:ap-south-1:431440931115:key/edb6f9d5-Safa-4b5c-b506-9ef17360c3ea](#)

Bucket Key  
Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)

Disabled

**Tags (0)** [Edit](#)

Track storage cost of other criteria by tagging your objects. [Learn more](#)

Key	Value
No tags associated with this resource.	

As we can see this file is encrypted

**Amazon S3** ×

Read the S3 resources page for documentation and technical content. [Learn more](#) ×

**Buckets**

- Access Points
- Object Lambda Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

► **Storage Lens**

Feature spotlight [?](#)

► AWS Marketplace for S3

**Object overview**

Owner	S3 URI
AWS Region	<a href="#">s3://deinternbucket/Test.txt</a>
Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN)
Last modified	<a href="#">arn:aws:s3:::deinternbucket/Test.txt</a>
May 31, 2021, 17:19:36 (UTC+05:30)	Entity tag (Etag)
Size	<a href="#">7e059662e4ca87ab55541414b5bf9d84</a>
15.0 B	Object URL
Type	<a href="#">https://deinternbucket.s3.ap-south-1.amazonaws.com/Test.txt</a>
txt	
Key	
<a href="#">Test.txt</a>	

**Object management overview**

The following bucket properties and object management configurations impact the behavior of this object.

Check this link –

<https://deinternbucket.s3.ap-south-1.amazonaws.com/Test.txt>

access denied

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>YF3ASZ8JWBVJ8F4P</RequestId>
  <HostId>gnZACdoJUt0VIT50y91jqbTRhfcoRmBDaHSLvE0BfjTx8xuQk5d23u1BAGbRchDWS6JR/pztDjY=</HostId>
</Error>
```

Encrypting using AWS-managed keys –



aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Global

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > deinternbucket > Upload

Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 46.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	test2.txt	-	text/plain	46.0 B

Destination

Destination

s3://deinternbucket

Destination details

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Cookie preferences

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Global

Support

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > deinternbucket > Server-side encryption settings

Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#)

Server-side encryption

☐ Do not specify an encryption key

☒ Specify an encryption key

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

☐ Amazon S3 key (SSE-S3)

An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

☒ AWS Key Management Service key (SSE-KMS)

An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

☒ AWS managed key (aws/s3)

arn:aws:kms:ap-south-1:431440931115:alias/aws/s3

☐ Choose from your AWS KMS keys

☐ Enter AWS KMS key ARN

Bucket Key is disabled for objects uploaded, modified, or copied in this bucket

Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. [Learn more](#)

Bucket Key

Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use

Feedback

English (US)

© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

Cookie preferences

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

ABHINAV SHRESHTH

Upload succeeded

View details below.

The information below will no longer be available after you navigate away from this page.

Summary

Destination

s3://deinternbucket

Succeeded

1 file, 46.0 B (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 46.0 B)

Name	Folder	Type	Size	Status	Error
test2.txt	-	text/plain	46.0 B	Succeeded	-

In properties of test2.txt

**Storage class**  
Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class  
Standard

**Server-side encryption settings**  
Server-side encryption protects data at rest. [Learn more](#)

Default encryption  
Enabled

Server-side encryption  
AWS-KMS master-key (SSE-KMS)

AWS KMS key ARN  
[arn:aws:kms:ap-south-1:431440931115:key/51bf8220-3453-4411-b4f0-5e70464f4cf1](#)

Bucket Key  
Reduce encryption costs by decreasing calls to AWS KMS for new objects in this bucket. To specify a Bucket Key setting for an object, use the AWS CLI, AWS SDK, or Amazon S3 Rest API. [Learn more](#)

Disabled

Now checking the url <https://deinternbucket.s3.ap-south-1.amazonaws.com/test2.txt>

Successfully encrypted

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>0QXGZJQDTPW0E63T</RequestId>
  <HostId>x0sDe9gP27vrYW0y8L3is12VvWgnu6OG+xyWC2PgzeYw/dwNBpz9GBjcpmbTpEwq5Phnuf8bxvY=</HostId>
</Error>
```

Now switching back to key management service (KMS)

**Key Management Service (KMS)**

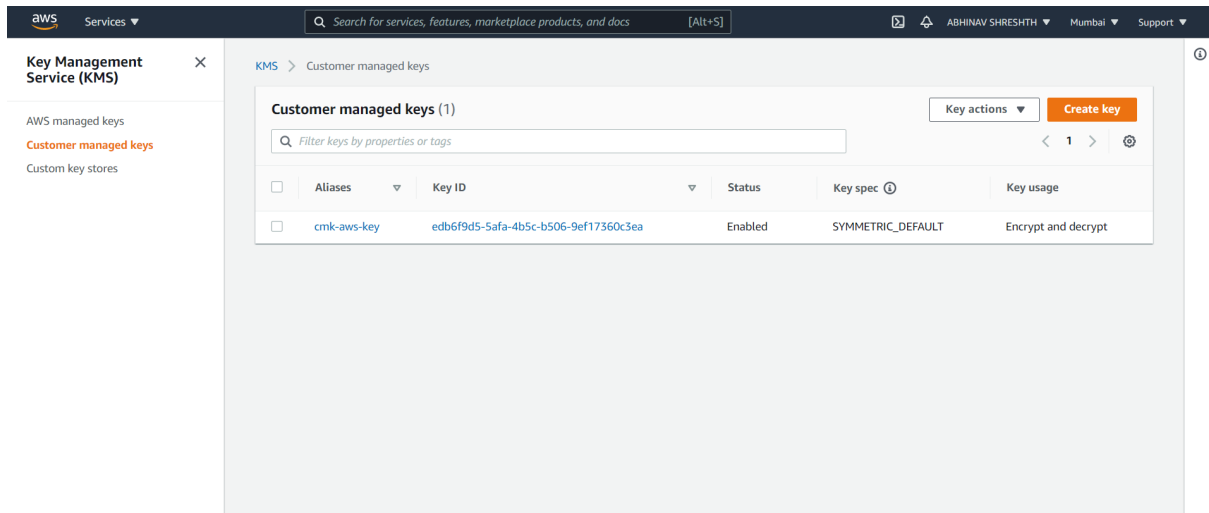
**AWS managed keys**  
Customer managed keys  
Custom key stores

KMS > AWS managed keys

**AWS managed keys (1)**

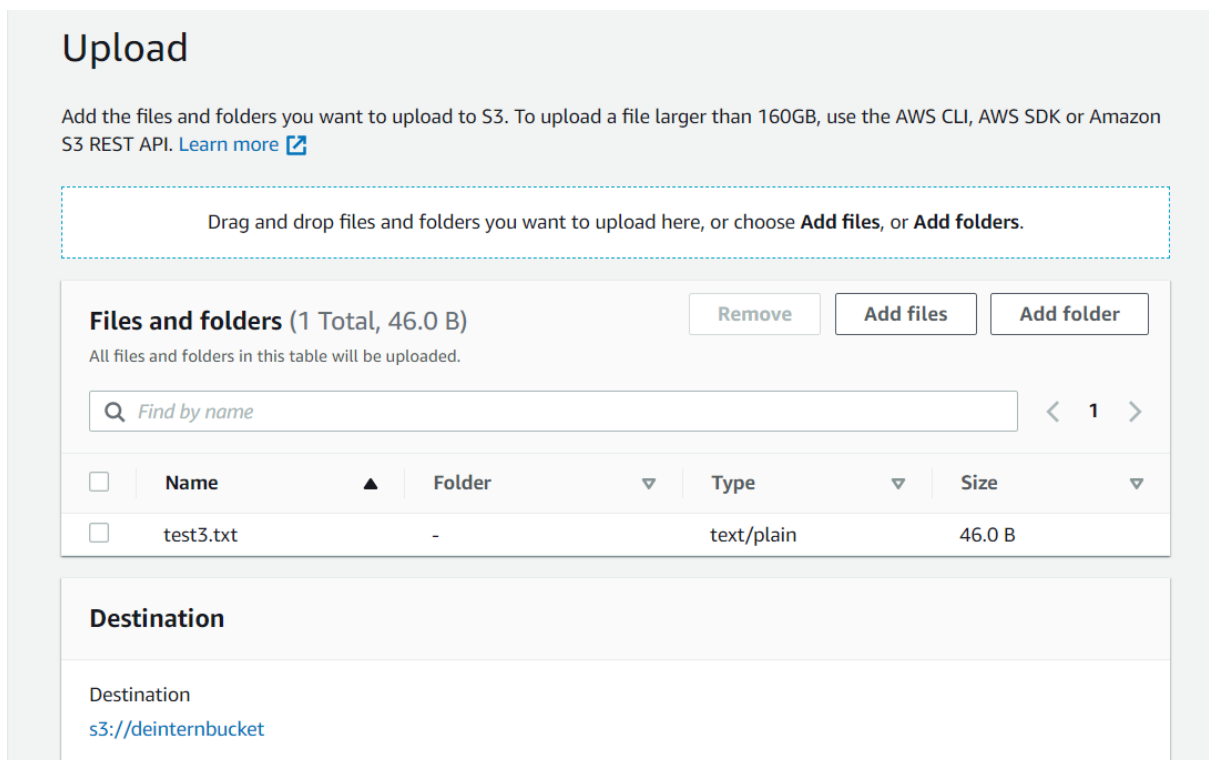
Filter keys by alias or key ID

Aliases	Key ID	Status
aws/s3	51bf8220-3453-4411-b4f0-5e70464f4cf1	Enabled



As we can see customer managed keys and AWS managed keys entry are present.

Now trying uploading test3.txt



### Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#)

**Server-side encryption**

☐ Do not specify an encryption key  
☒ Specify an encryption key

**Encryption key type**

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

☒ **Amazon S3 key (SSE-S3)**  
 An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

☐ AWS Key Management Service key (SSE-KMS)  
 An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

Uploading successful of test3.txt

**Upload succeeded**  
View details below.

The information below will no longer be available after you navigate away from this page.

#### Summary

Destination s3://deinternbucket	Succeeded 1 file, 46.0 B (100.00%)	Failed 0 files, 0 B (0%)
------------------------------------	---------------------------------------	-----------------------------

**Files and folders** | Configuration

**Files and folders** (1 Total, 46.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
test3.txt	-	text/plain	46.0 B	Succeeded	-

**Amazon S3**

- Buckets
  - Access Points
  - Object Lambda Access Points
  - Batch Operations
  - Access analyzer for S3
- Block Public Access settings for this account
- Storage Lens
  - Dashboards
  - AWS Organizations settings
- Feature spotlight
- AWS Marketplace for S3

### Standard

#### Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#) Edit

Default encryption  
Enabled

Server-side encryption  
Amazon S3 master-key (SSE-S3)

#### Tags (0)

Track storage cost of other criteria by tagging your objects. [Learn more](#) Edit

Key	Value
No tags associated with this resource.	

#### Metadata (1)

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#) Edit

Type	Key	Value
System defined	Content-Type	text/plain

Now checking the file test3.txt is successfully encrypted or not

The screenshot displays the AWS Management Console interface for the Amazon S3 service. The left-hand navigation pane shows the 'Amazon S3' section with options like Buckets, Access Points, and Storage Lens. The main content area is titled 'Object overview' and provides details for a specific object. The object's name is 'test3.txt', which is underlined in red. The details are organized into two columns: the left column lists metadata such as Owner, AWS Region (Asia Pacific (Mumbai) ap-south-1), Last modified date (May 31, 2021, 17:51:09 (UTC+05:30)), Size (46.0 B), Type (txt), and Key (test3.txt). The right column lists S3 URI (s3://deinternbucket/test3.txt), Amazon Resource Name (ARN) (arn:aws:s3:::deinternbucket/test3.txt), Entity tag (Etag) (03dc9417b274cd5b726fe8ad6bdf1de6), and Object URL (https://deinternbucket.s3.ap-south-1.amazonaws.com/test3.txt).

Object overview	
Owner	S3 URI
AWS Region	s3://deinternbucket/test3.txt
Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN)
Last modified	arn:aws:s3:::deinternbucket/test3.txt
May 31, 2021, 17:51:09 (UTC+05:30)	Entity tag (Etag)
Size	03dc9417b274cd5b726fe8ad6bdf1de6
46.0 B	Object URL
Type	https://deinternbucket.s3.ap-south-1.amazonaws.com/test3.txt
txt	
Key	
test3.txt	

<https://deinternbucket.s3.ap-south-1.amazonaws.com/test3.txt>

now this file is also got encrypted

+++++