

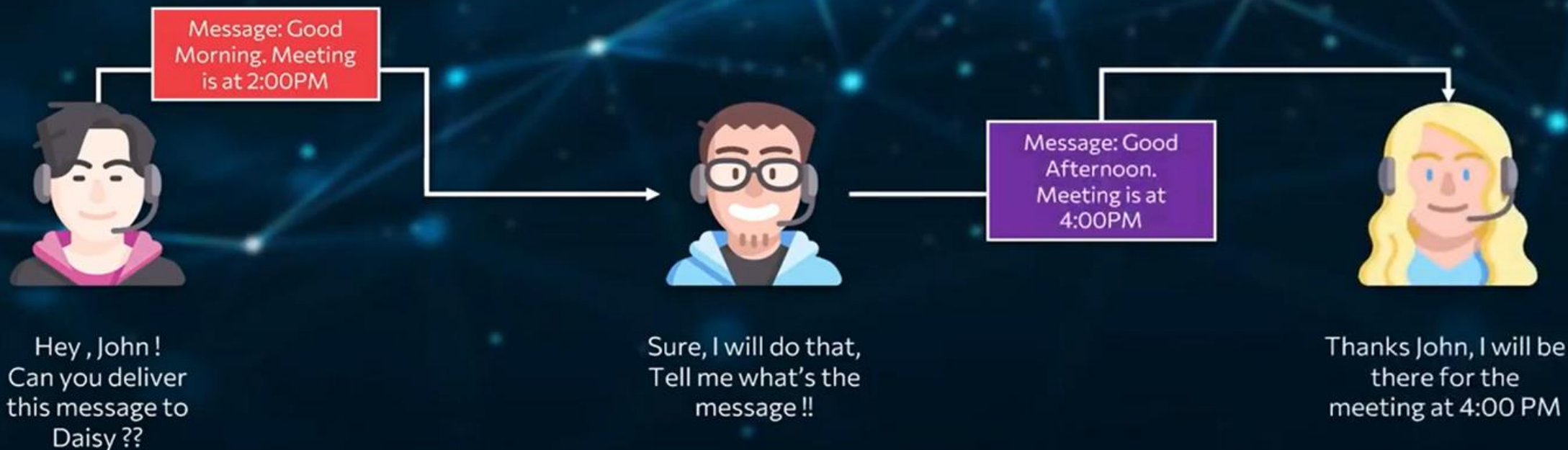
AWS Key Management Service (AWS KMS)

AWS Key Management Service (KMS)

- An easy way to control access to your data using managed encryption
- Integrated with AWS cloud services including Amazon EBS, Amazon S3, and Amazon RedShift to simplify encryption of your data
- Create, rotate, disable, enable, and define usage policies for master keys and audit their usage



Lets talk about, **Encryption**





Lets talk about,

Encryption





Lets talk about,

Encryption

Cipher Text

Message:
MIIEpAIBAAKCAG
EAosv38EqWiJOS
KZROVj63Q



Hey , John!
Can you deliver
this message to
Daisy ??

Plain Text



Sure, I will do that,
Tell me what's the
message !!

Message:
MIIEpAIBAAKCAG
EAosv38EqWiJOS
KZROVj63Q



Thanks John, I got
the message.

The Common Secure Key.





Lets talk about,

Encryption



The Encrypted
Message which is
being sent to the
USER.



The Encryption
Key to
Cipher/Decipher
the Message



The Decrypted
Message Read by
the USER. Using
the Encryption
Key.



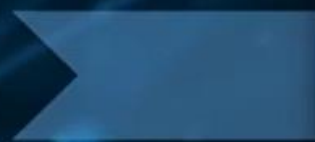


Lets talk about,

Encryption



The Encrypted
Message which is
being sent to the
USER.



The Encryption
Key using KMS to
Cipher/Decipher
the Message



The Decrypted
Message Read by
the USER. Using
the Encryption
Key.





Security and Encryption





Encryption of DATA



**Encryption in
Flight**

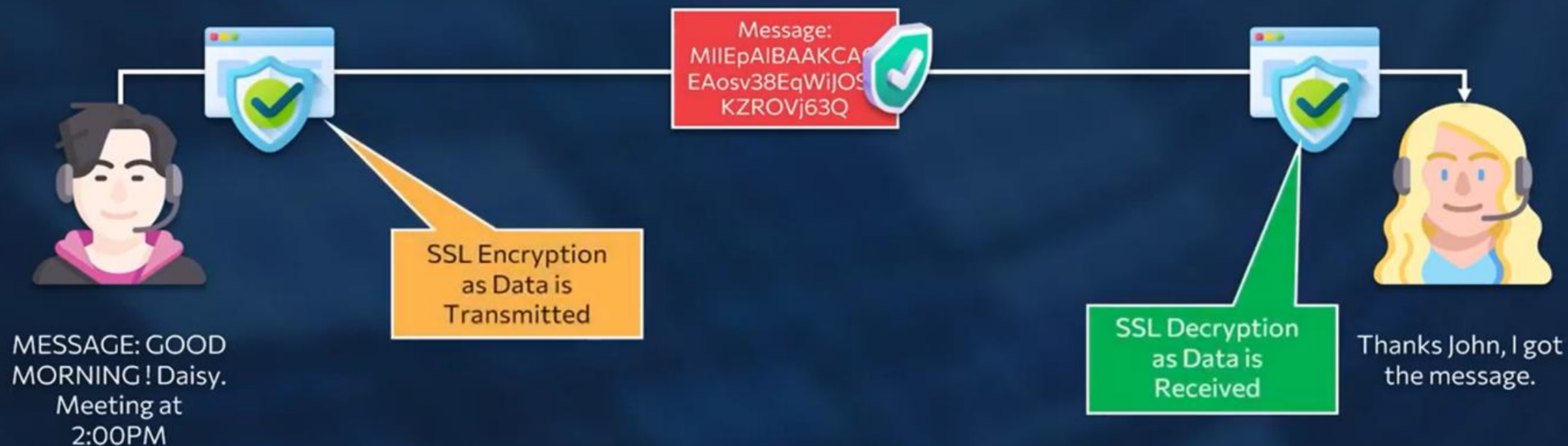


**Encryption at
Rest**



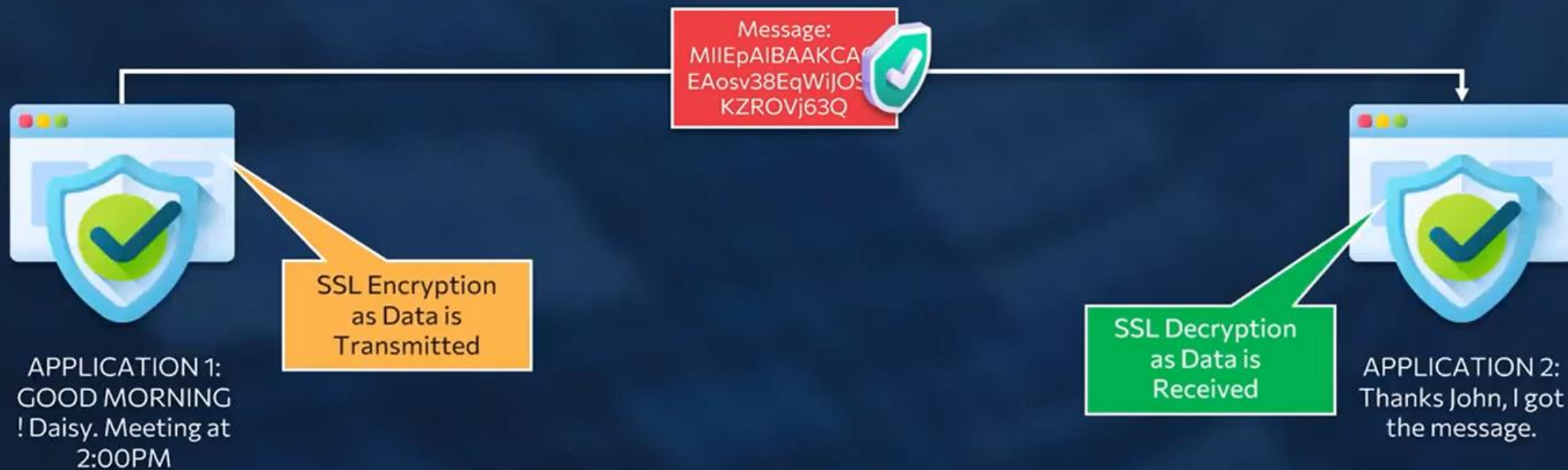


Encryption in Flight



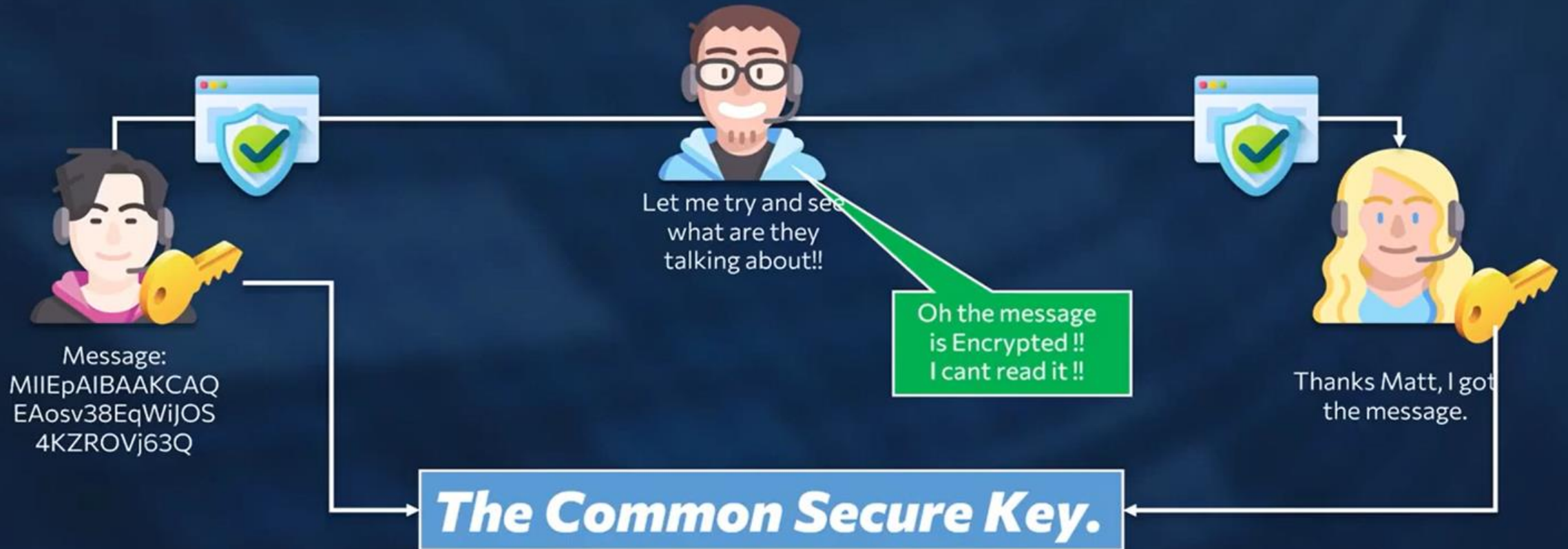


Encryption in Flight





Encryption at Rest





AWS Key Management Store

Easily create and control the keys used to encrypt or digitally sign your data

Create and manage cryptographic keys and control their use across a wide range of AWS services:

- Uses hardware security modules (HSM) that have been validated under FIPS 140-2.
- Integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
- AWS Free Tier includes 20,000 free AWS Key Management Service requests each month.

Centralized Key Management

1

Centralized control over the lifecycle and permissions of your keys. Import keys from your own key management infrastructure, or use keys stored in your AWS CloudHSM cluster. Automatic rotation of master keys generated in AWS KMS once per year

AWS Service Integration

2

AWS KMS integrates with AWS services to encrypt data at rest. To protect data at rest, integrated AWS services use envelope encryption, where a data key is used to encrypt data, and is itself encrypted under a CMK stored in AWS KMS.

Custom Key Store

3

Create your own key store using HSMs that you control. Each custom key store is backed by an AWS CloudHSM cluster. CMKs stored in a custom key store are managed by you like any other CMK and can be used with any AWS service that integrates with AWS KMS.

Hands on to create the KMS:

1. Login using root user / IAM user with admin access
2. Search for Key Management Service
3. Click on create key, and then follow the slides for further configurations

[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 key used for encrypting and decrypting data or generating and verifying HMAC codes.

**Asymmetric**

A public and private key pair used for encrypting and decrypting data or signing and verifying messages.

Key usage [Help me choose](#)

**Encrypt and decrypt**

Use the key only to encrypt and decrypt data.

**Generate and verify MAC**

Use the key only to generate and verify hash-based message authentication codes (HMAC).

► Advanced options

[Cancel](#)[Next](#)

[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

Pradeep-Key1

Description - optional

You can change the description at any time.

Description

Pradeep-Key1

Tags - optional

You can use tags to categorise and identify your KMS keys 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



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](#)

Define key administrative permissions

Key administrators (1/9)

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 type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	Admin	/	User
<input checked="" type="checkbox"/>	pradeep	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
<input type="checkbox"/>	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
<input type="checkbox"/>	AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
<input type="checkbox"/>	IAM-Role-Datasync	/	Role
<input type="checkbox"/>	S3EC2-Role	/	Role

Key deletion

☐ Allow key administrators to delete this key.

Cancel

Previous

Next



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](#)

Define key usage permissions

Key users (1/9)

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

< 1 >

<input type="checkbox"/>	Name ▾	Path ▾	Type ▾
<input type="checkbox"/>	Admin	/	User
<input checked="" type="checkbox"/>	pradeep	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
<input type="checkbox"/>	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
<input type="checkbox"/>	AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
<input type="checkbox"/>	IAM-Role-Datasync	/	Role
<input type="checkbox"/>	S3EC2-Role	/	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



Step 2

[Add labels](#)

Step 3

[Define key administrative permissions](#)

Step 4

Define key usage permissions

Step 5

[Review](#)

Key users (1/9)

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

<1>

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	Admin	/	User
<input checked="" type="checkbox"/>	pradeep	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
<input type="checkbox"/>	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
<input type="checkbox"/>	AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
<input type="checkbox"/>	IAM-Role-Datasync	/	Role
<input type="checkbox"/>	S3EC2-Role	/	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



Alias and description

Alias	Description
Pradeep-Key1	Pradeep-Key1

Tags

Key	Value
No data No tags to display	

Key policy

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

```
34     "Resource": "*",
35   },
36   {
37     "Sid": "Allow use of the key",
38     "Effect": "Allow",
39     "Principal": {
40       "AWS": "arn:aws:iam::233000744127:user/pradeep"
41     },
42     "Action": [
43       "kms:Encrypt",
44       "kms:Decrypt",
45       "kms:ReEncrypt*",
46       "kms:GenerateDataKey*",
47       "kms:DescribeKey"
```


[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

Regionality
Single-region key

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

Alias and description

Alias
Pradeep-Key1

Description
Pradeep-Key1

Tags

Key

Value

No data
No tags to display

← → ↻ ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys

aws Services [Alt+S]

Key Management Service (KMS)

Success
Your AWS KMS key was created with alias Pradeep-Key1 and key ID 67f4e02e-6cff-4a34-b909-668d4dcbf568. View key

KMS > Customer-managed keys

Customer-managed keys (2)

Filter keys by properties or tags

<input type="checkbox"/>	Aliases	Key ID	Status	Key type	Key spec	Key usage
<input type="checkbox"/>	Financial_Doc	2c731e1c-103e-48a3-82a7-f...	Pending deletion	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt
<input type="checkbox"/>	Pradeep-Key1	67f4e02e-6cff-4a34-b909-66...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

Can observe the Keys generated in the KMS dashboard – Customer-managed keys.

Can use the key to encrypt for the S3 service.

S3 Bucket Creation (can follow the previous session slides)

Should enable Key for the Bucket or for the file uploaded in the bucket, by edit the encryption option.

Key	Value
No tags associated with this resource.	

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket. [Edit](#)

Encryption type [Info](#)
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#) [↗](#)

Enabled

Intelligent-Tiering Archive configurations (0)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](#) [↗](#)

[View details](#) [Edit](#) [Delete](#) [Create configuration](#)

[Find Intelligent-Tiering Archive configurations](#)

Name	Status	Scope	Days until transition to Archive Access tier	Days until transition to Deep Archive Access tier
No archive configurations				

Choosing of KMS Keys

aws

Services

Search

[Alt+S]

Global

pradeepkum

Amazon S3

Buckets

pradeep-falms

Edit default encryption

Edit default encryption

Info

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type

Info

☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)

☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the **Storage** tab of the [Amazon S3 pricing page](#).

AWS KMS key

Info

☒ Choose from your AWS KMS keys

☐ Enter AWS KMS key ARN

Available AWS KMS keys

Choose AWS KMS key

Create a KMS key

Q

arn:aws:kms:ap-south-1:233000744127:key/2c731e1c-103e-48a3-82a7-fe74442c0e49
Financial_Doc

arn:aws:kms:ap-south-1:233000744127:key/67f4e02e-6cff-4a34-b909-668d4dcbf568
Pradeep-Key1

arn:aws:kms:ap-south-1:233000744127:alias/aws/s3
aws/s3

has the necessary AWS KMS permissions. [Learn more](#)

Cancel

Save changes

Choosing of SSE_KMS for S3



[Amazon S3](#) > [Buckets](#) > [bucket-pradeep-7alias](#) > Edit default encryption

Edit default encryption [Info](#)

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the **Storage** tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

Cancel

Save changes

Final output of s3 of User

Services

Search

[Alt+S]

Global

pradeepkuma

Amazon S3 > Buckets > bucket-pradeep-7alias

bucket-pradeep-7alias

Info

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

Objects (1)

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 explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

< 1 >

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<div>Attendance_Summary_Matrix_2023_24_ENG_SOE_DSU_B_Tech_CSE_Semester_5_CSE_5_05_08_2023_To_13_10_2023_F.xls</div>	xls	October 19, 2023, 16:24:49 (UTC+05:30)	114.1 KB	Standard

Try to view the key from a IAM user(developer)

Key Management Service (KMS)

AWS managed keys

Customer-managed keys

Custom key stores

AWS CloudHSM key stores

External key stores

ListAliases request failed

AccessDeniedException - User: am:aws:iam::233000744127:user/Admin is not authorized to perform: kms:ListAliases on resource: * because no identity-based policy allows the kms:ListAliases action

KMS > AWS managed keys

AWS managed keys (0)

Filter keys by properties or tags

< 1 >

⚙

Aliases

Key ID

Status

Loading keys

Customer managed keys | Key

ap-south-1.console.aws.amazon.com/kms/home?region=ap-south-1#/kms/keys

Search [Alt+S]

Mumbai

pradeepkun

Key Management Service (KMS)

AWS managed keys

Customer-managed keys

Custom key stores

AWS CloudHSM key stores

External key stores

KMS > Customer-managed keys

Customer-managed keys (2)

Key actions

Create key

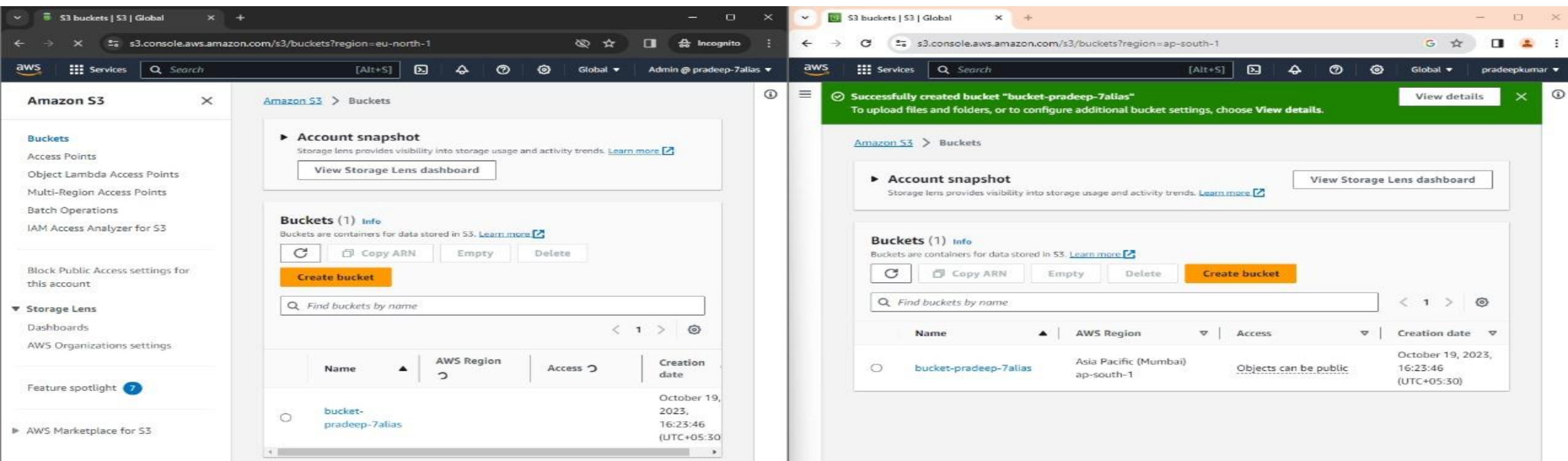
Filter keys by properties or tags

< 1 >

⚙

<input type="checkbox"/>	Aliases	Key ID	Status	Key type
<input type="checkbox"/>	Financial...	2c731e1c...	Pending d...	Symmetric
<input type="checkbox"/>	Pradeep...	67f4e02e...	Enabled	Symmetric

Output of Admin



After creating the bucket, try to login in 2 different IAM user account, check for the viewing of the bucket.

- The files can be viewed by the user of IAM provided Keys access and other can't view the encrypted file

Thank you...