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

AWS KMS

Pythoholic

AWS KMS

Lets talk about,

Encryption

Message: Good Morning. Meeting is at 2:00PM

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

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

Message: Good Afternoon. Meeting is at 4:00PM

Thanks John, I will be there for the meeting at 4:00 PM

Pythoholic

Designed by Pythoholic, Road to AWS Certified Solutions Architect SAA-C02

AWS KMS

Pythoholic

AWS KMS

Lets talk about,

Encryption

Message:
MIIEpAIBAAKCA
EAosv38EqWiJOS
KZROVj63Q

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

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

Message:
MIIEpAIBAAKCA
EAosv38EqWiJOS
KZROVj63Q

Thanks John, I got the message.

The Common Secure Key.

Pythoholic

Designed by Pythoholic, Road to AWS Certified Solutions Architect SAA-C02

Lets talk about,

Encryption

Cipher Text

Message:
MIIEpAIBAAKCA
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:
MIIEpAIBAAKCA
EAosv38EqWiJOS
KZROVj63Q

Thanks John, I got the message.

The Common Secure Key.

AWS KMS

Pythoholic

AWS KMS

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.

Pythoholic

AWS KMS

Pythoholic

AWS KMS

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.

Pythoholic

Designed by Pythoholic, Road to AWS Certified Solutions Architect SAA-C02

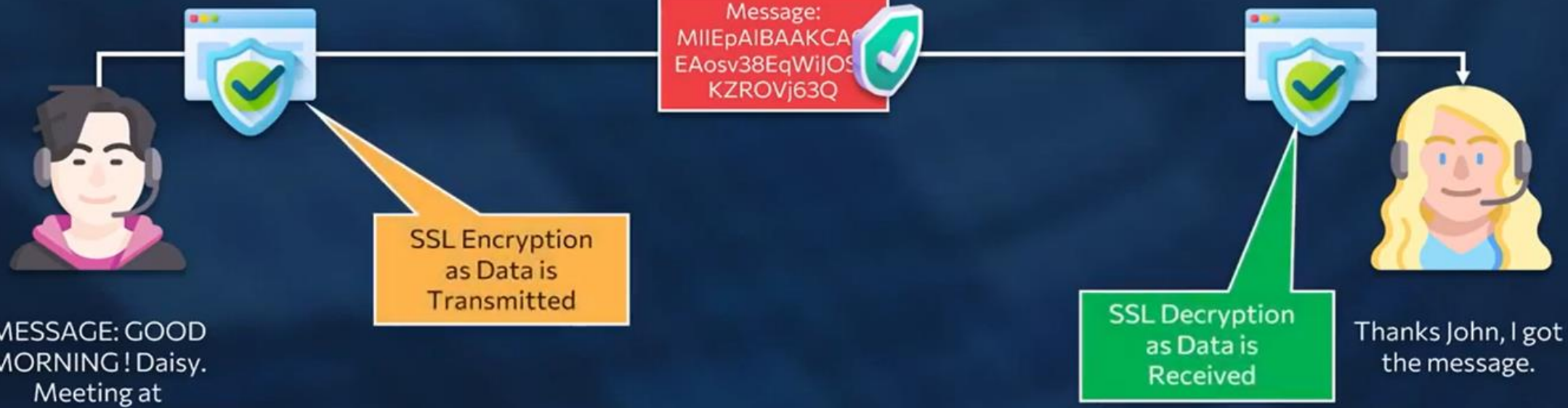
Security and Encryption

Encryption of DATA

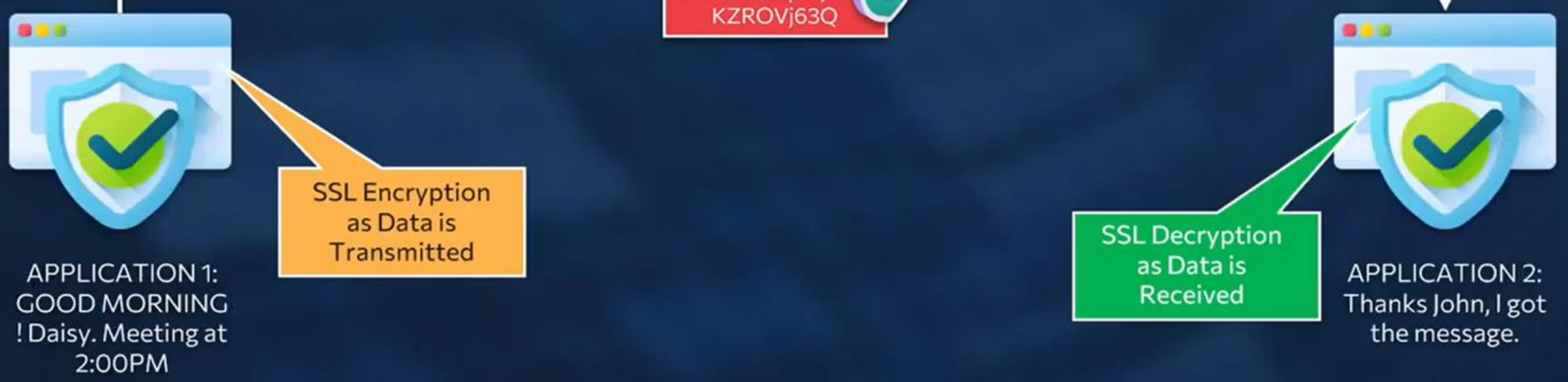
Encryption in Flight

Encryption at Rest

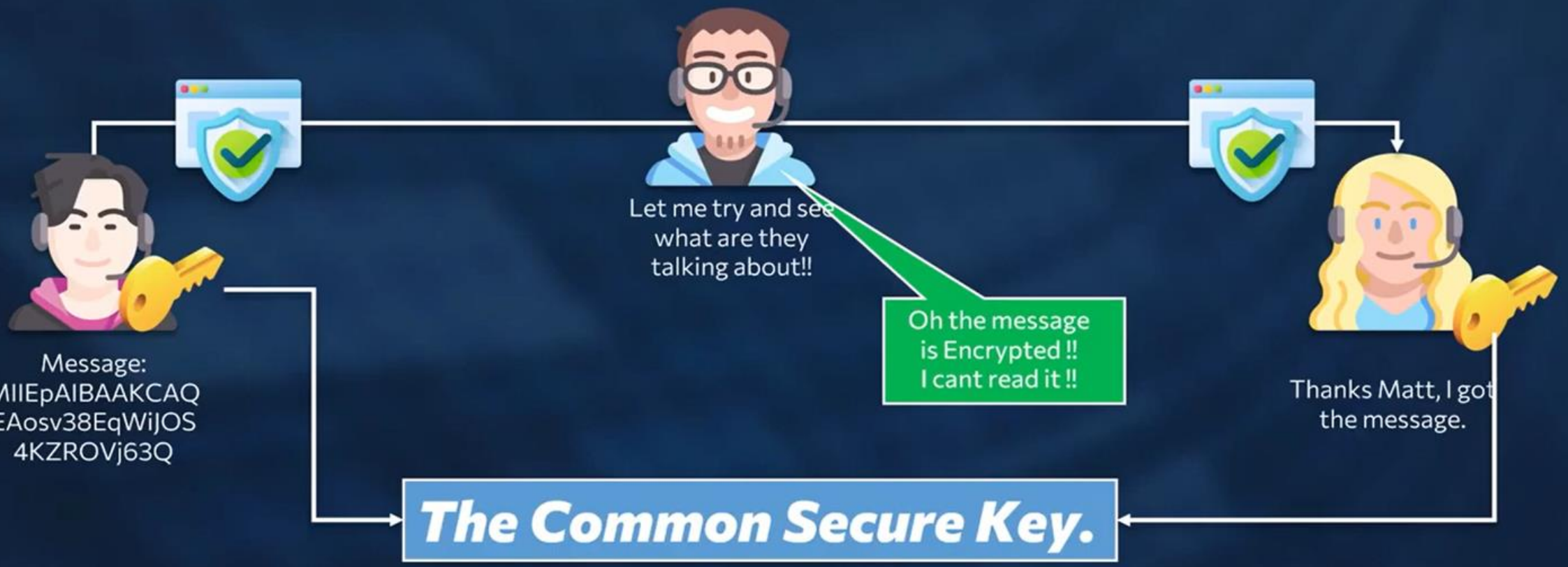
Encryption in Flight



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

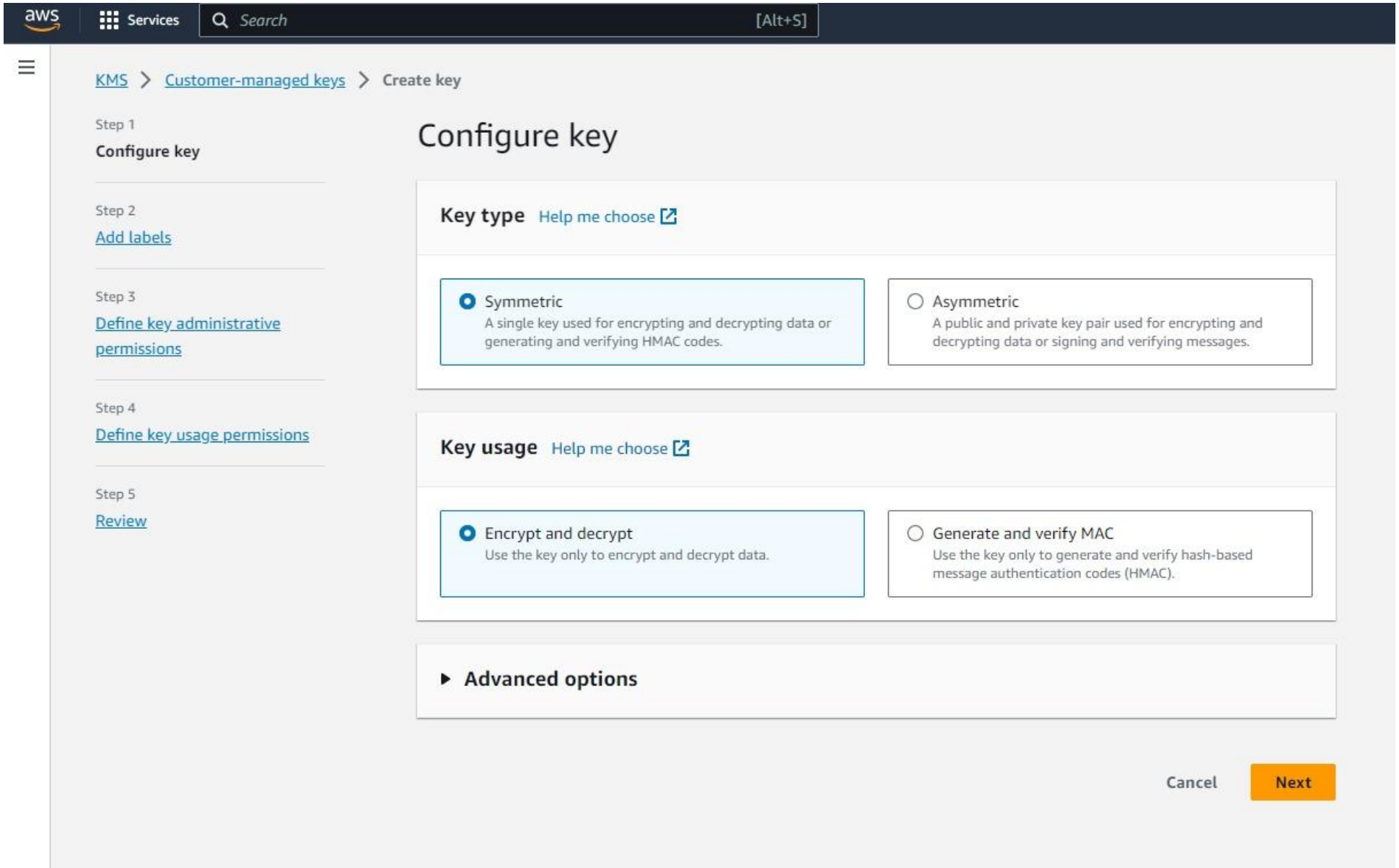
2. AWS KMS integrates with AWS services to encrypt data at rest. To protect data at rest, integrated AWS services use envelope encryption, where a data key is used to encrypt data, and is itself encrypted under a CMK stored in AWS KMS.

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 the follow the slides for further configurations


aws
Services
Search
[Alt+S]
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

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.

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

Name	Path	Type
Admin	/	User
pradeep	/	User
AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
IAM-Role-Datasync	/	Role
S3EC2-Role	/	Role

Key deletion

Allow key administrators to delete this key.

Cancel | Previous | Next

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

Name	Path	Type
Admin	/	User
pradeep	/	User
AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
IAM-Role-Datasync	/	Role
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

	Name	Path	Type
☐	Admin	/	User
☑	pradeep	/	User
☐	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling....	Role
☐	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
☐	AWSServiceRoleForGlobalAcce...	/aws-service-role/globalaccele...	Role
☐	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
☐	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role
☐	IAM-Role-Datasync	/	Role
☐	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.

```
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::233000744127:user/pradeep"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
```

Cancel | Previous | Finish

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	Key spec	Key usage
Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

Origin	Regionality
AWS KMS	Single-region key

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

Alias and description

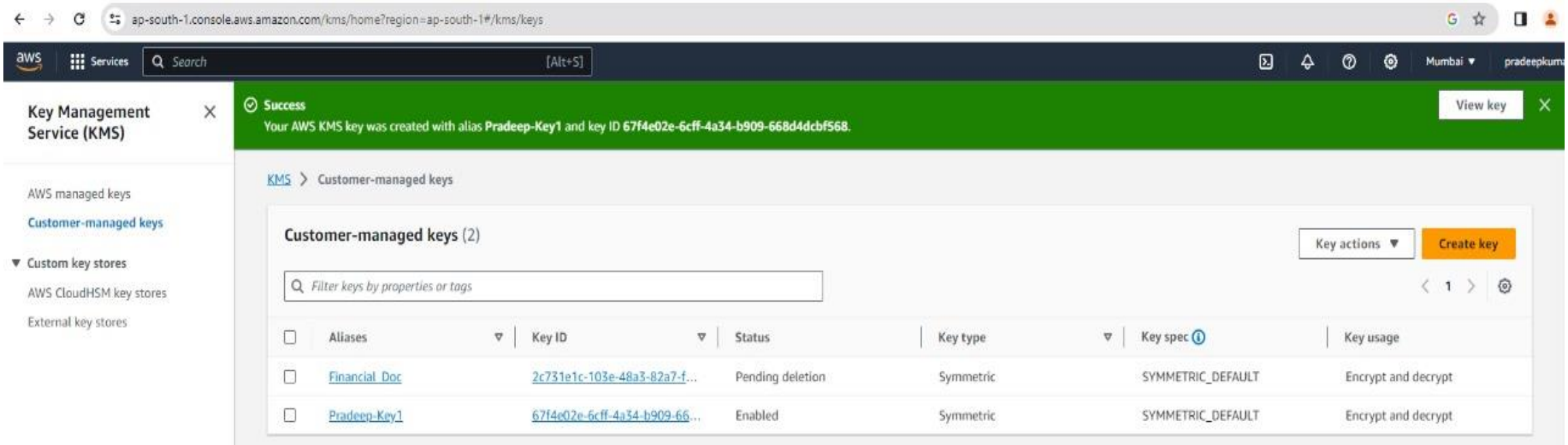
Alias	Description
Pradeep-Key1	Pradeep-Key1

Tags

Key	Value

No data

No tags to display

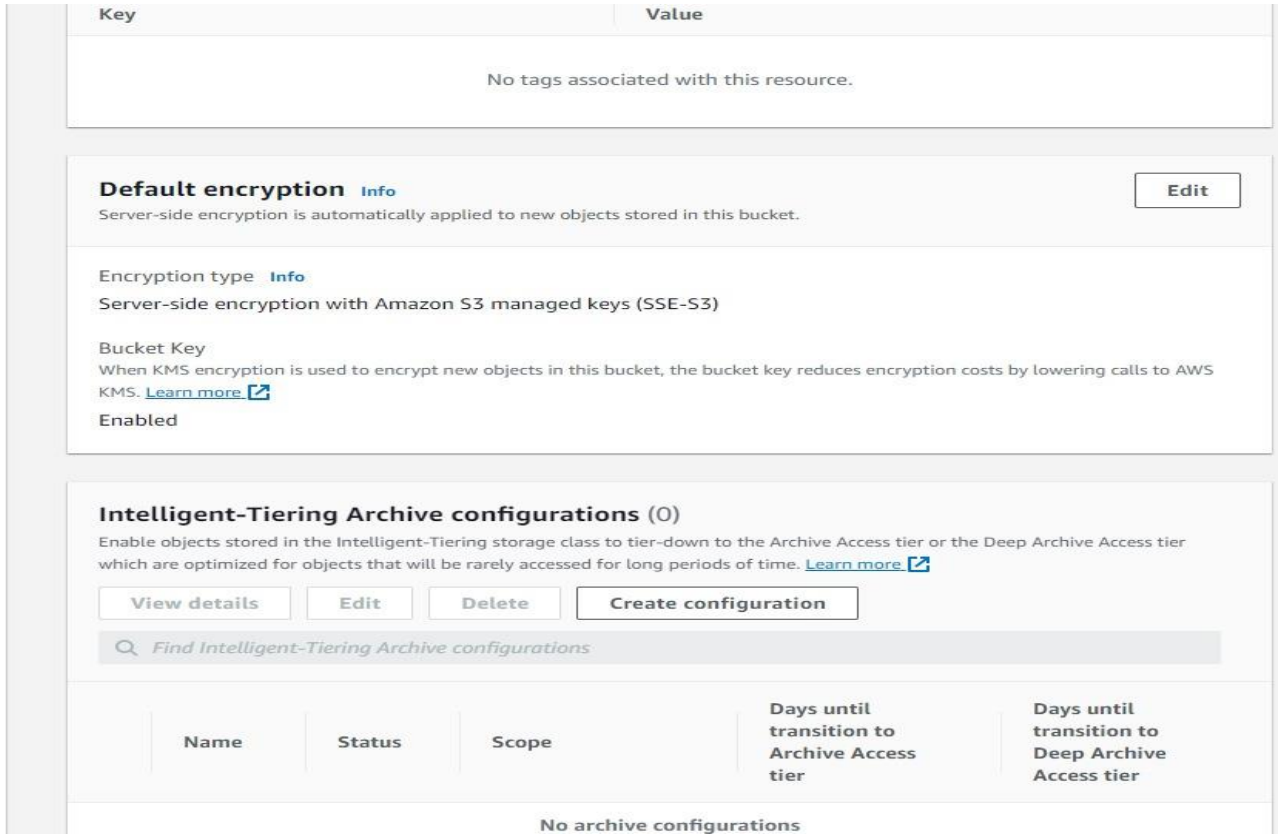


Can observe the Keys generated in the KMS dashboard – Customer-managed keys.

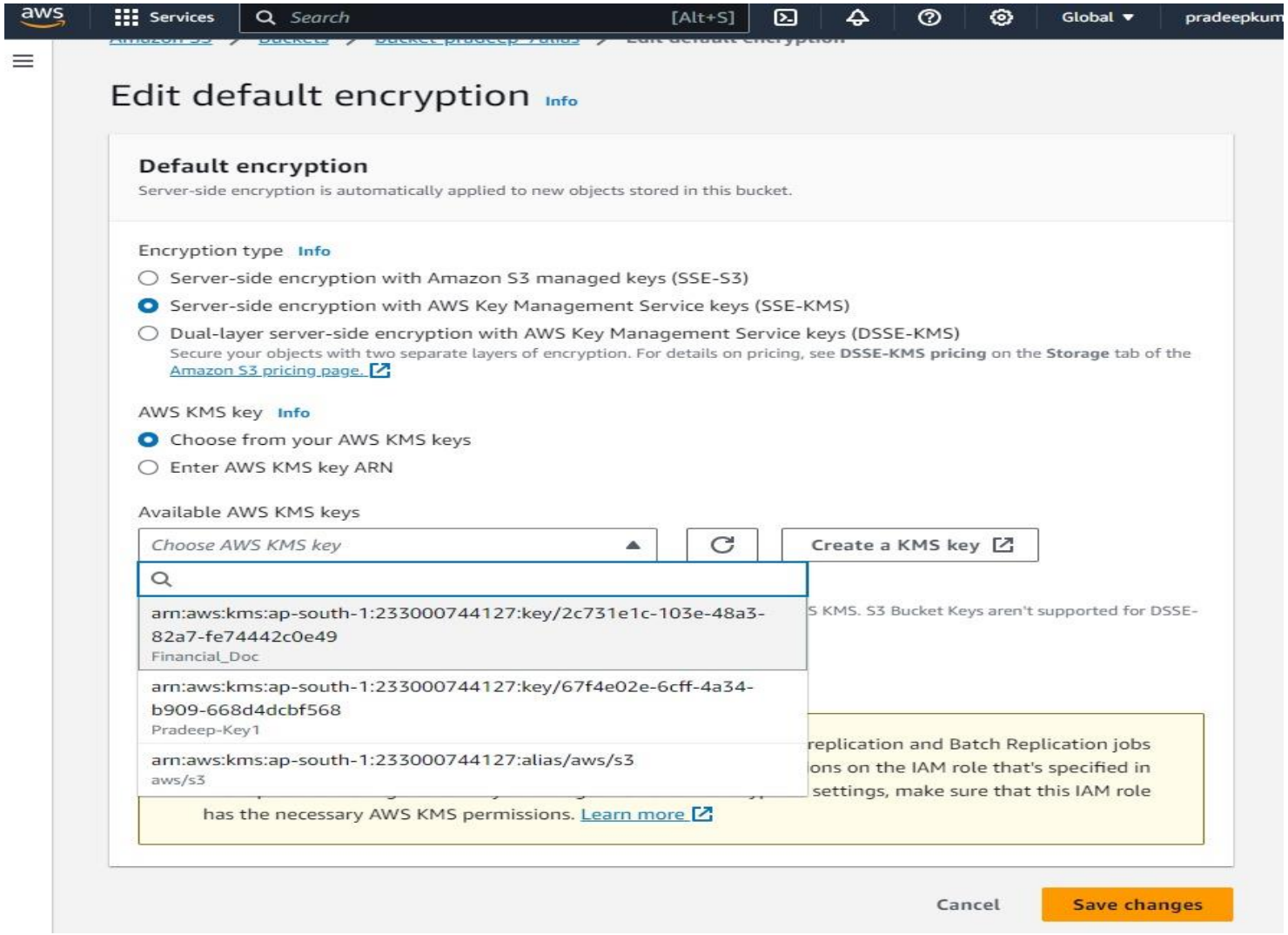
Can use the key to encrypt for the S3 service.

S3 Bucket Creation (can follow the previous session slides)

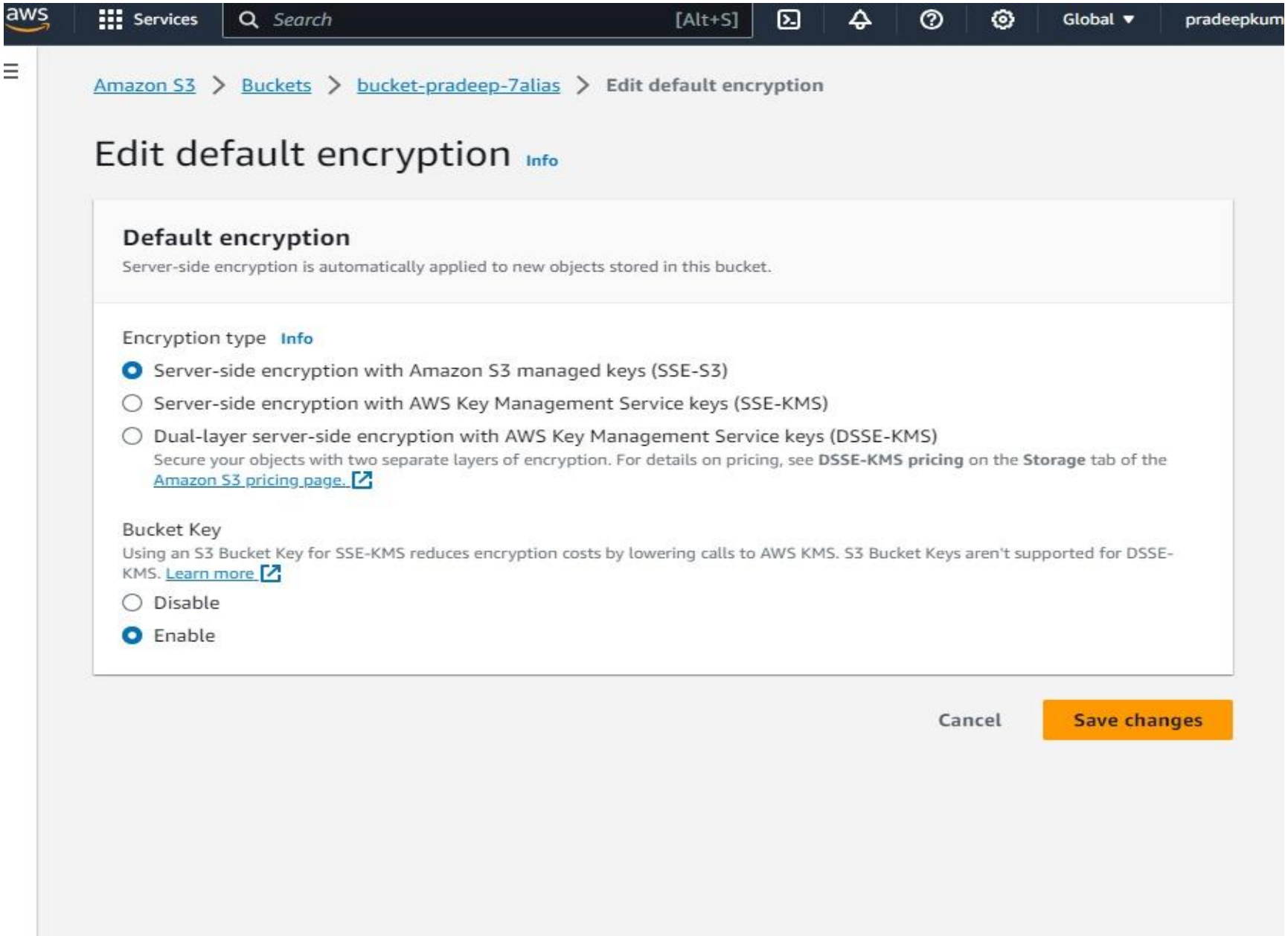
Should enable Key for the Bucket or for the file uploaded in the bucket, by edit the encryption option.



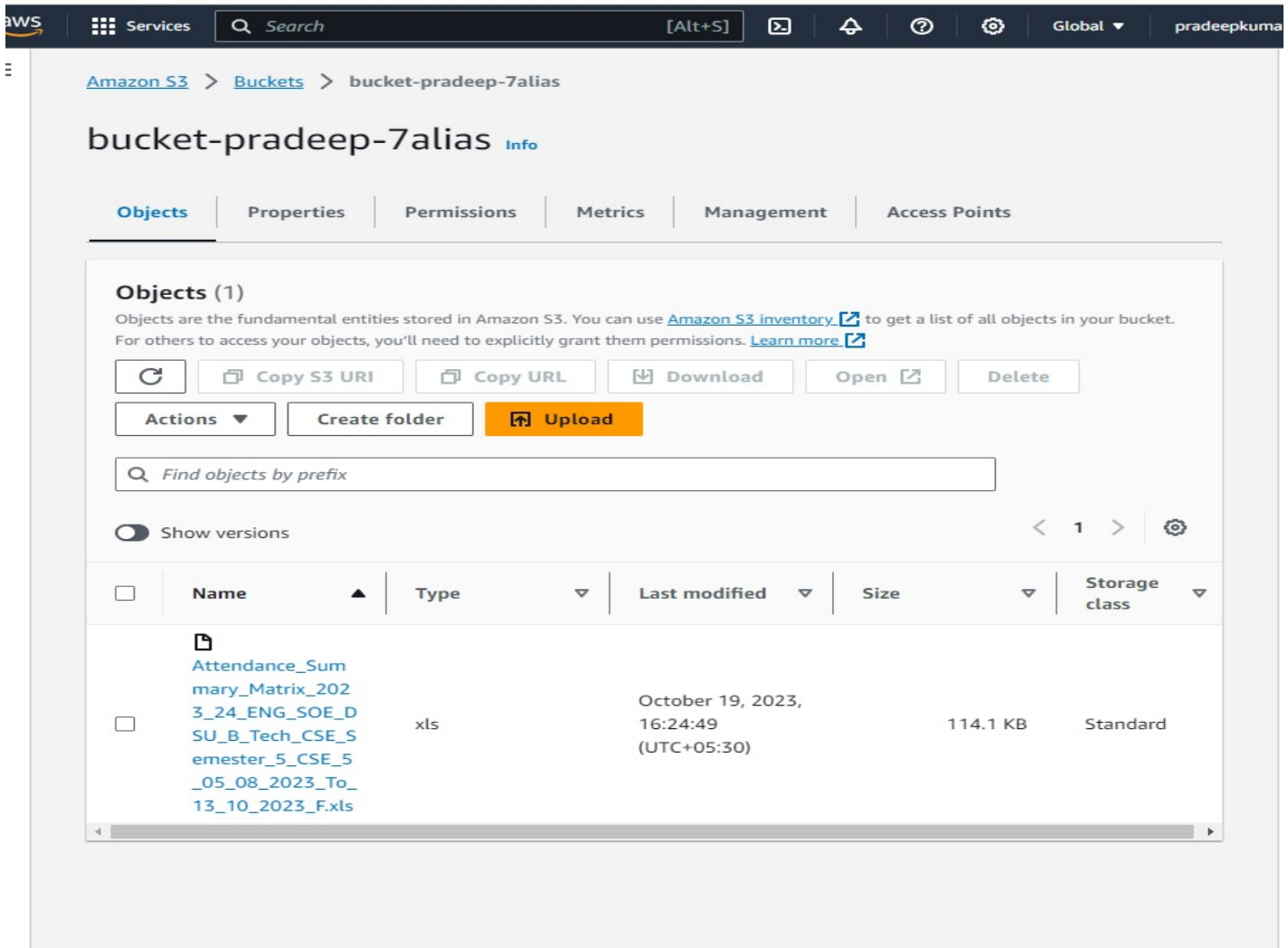
Choosing of KMS Keys



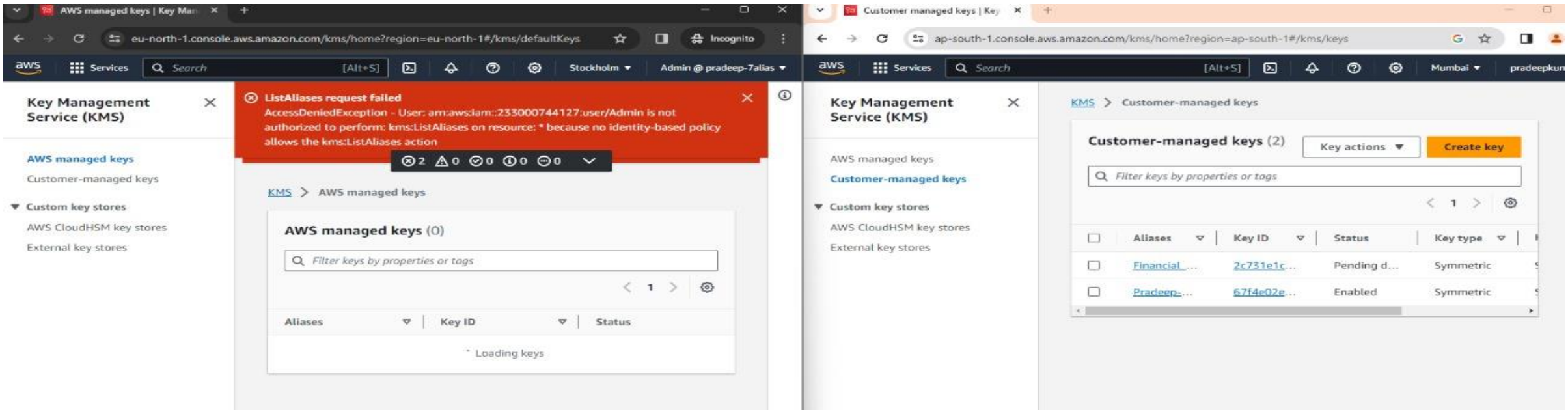
Choosing of SSE_KMS for S3



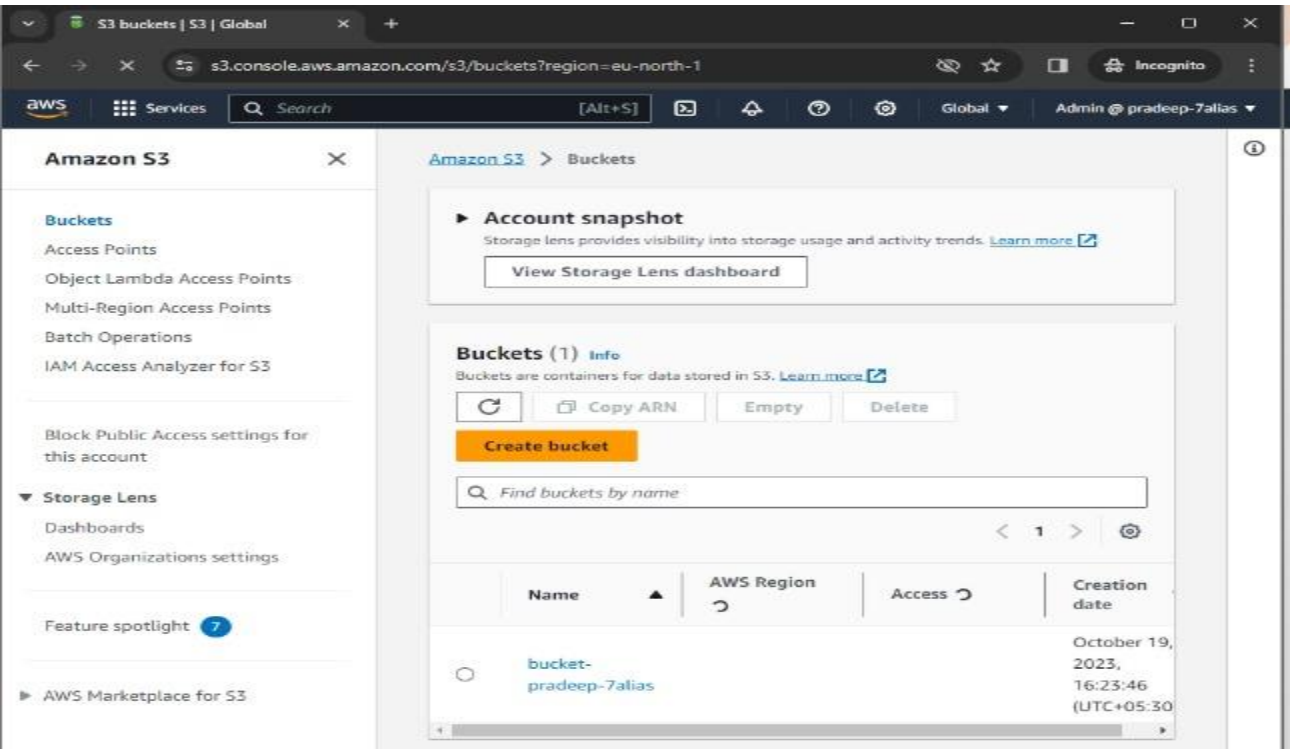
Final output of s3 of User

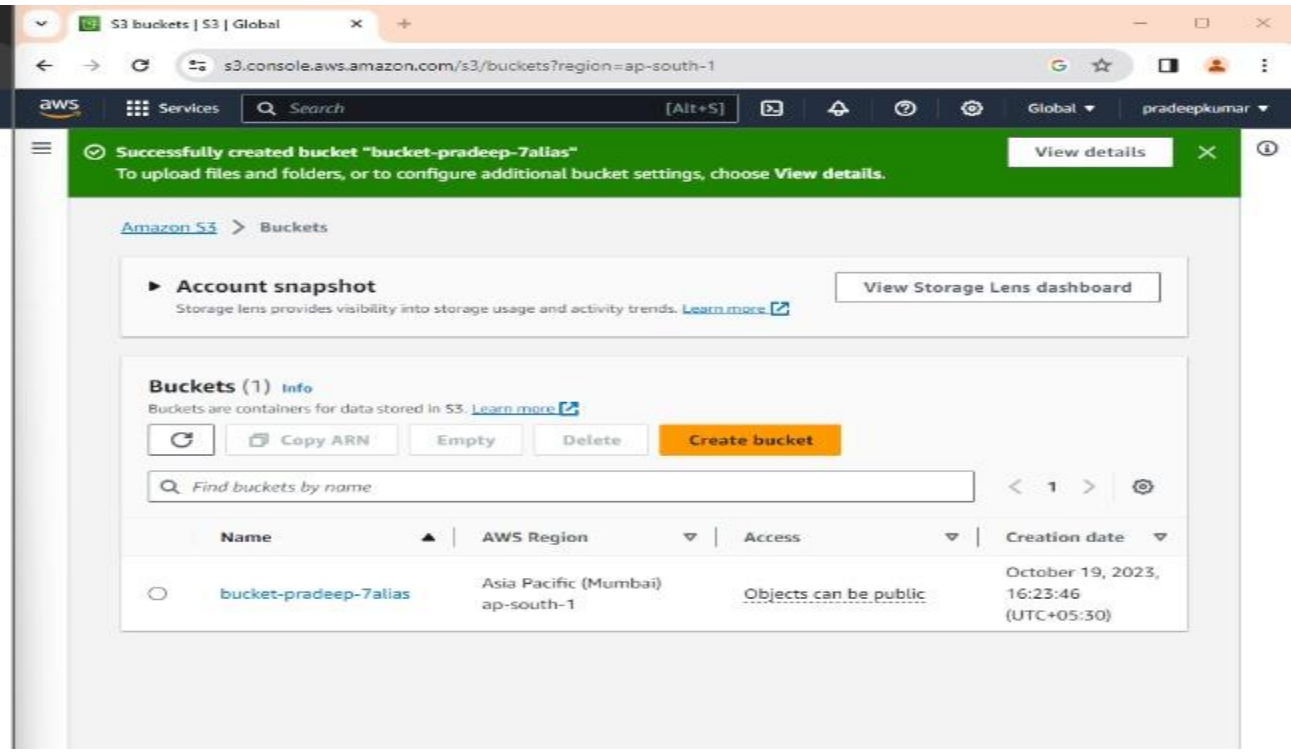


Try to view the key from a IAM user(developer)



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…