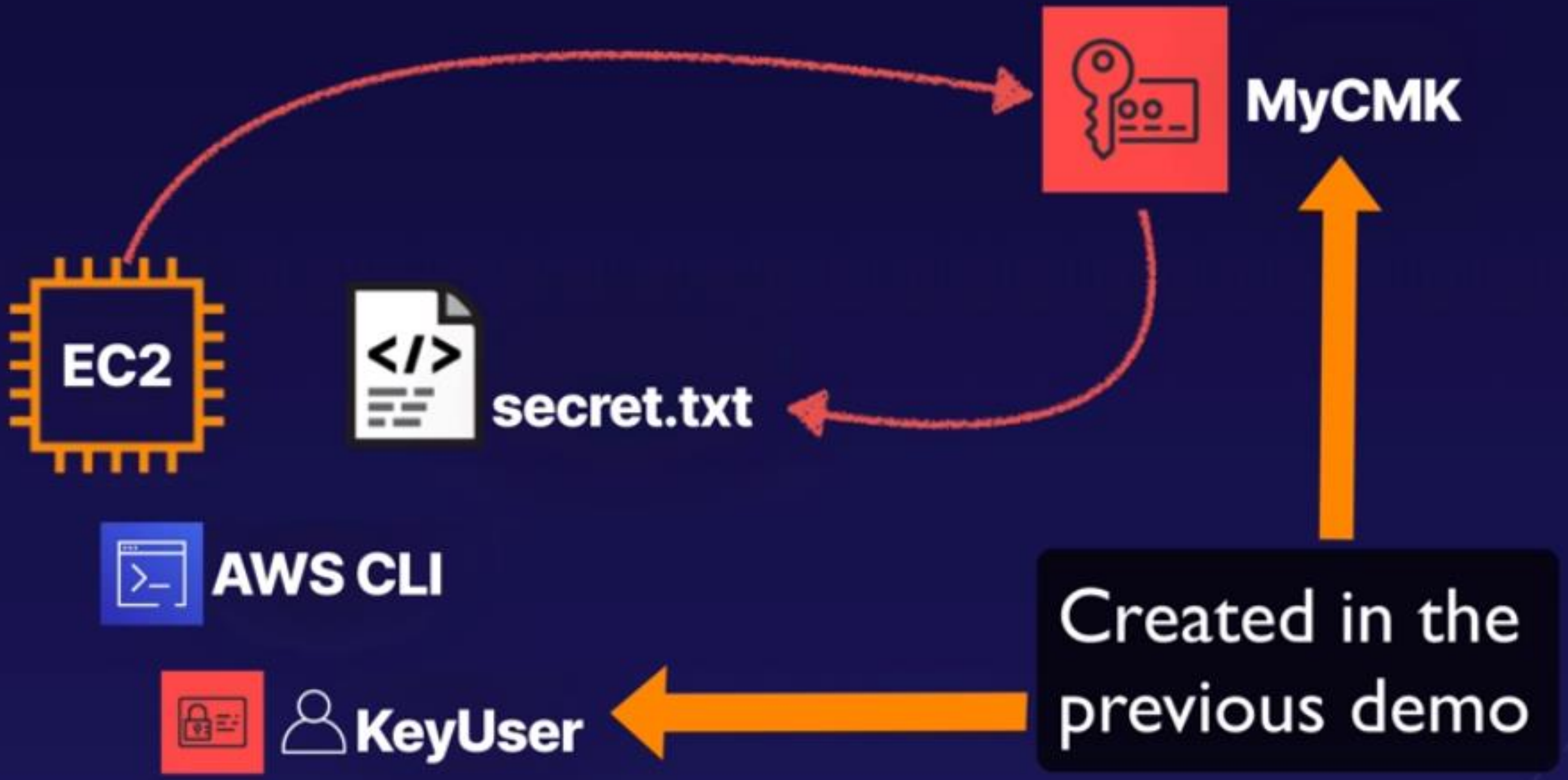
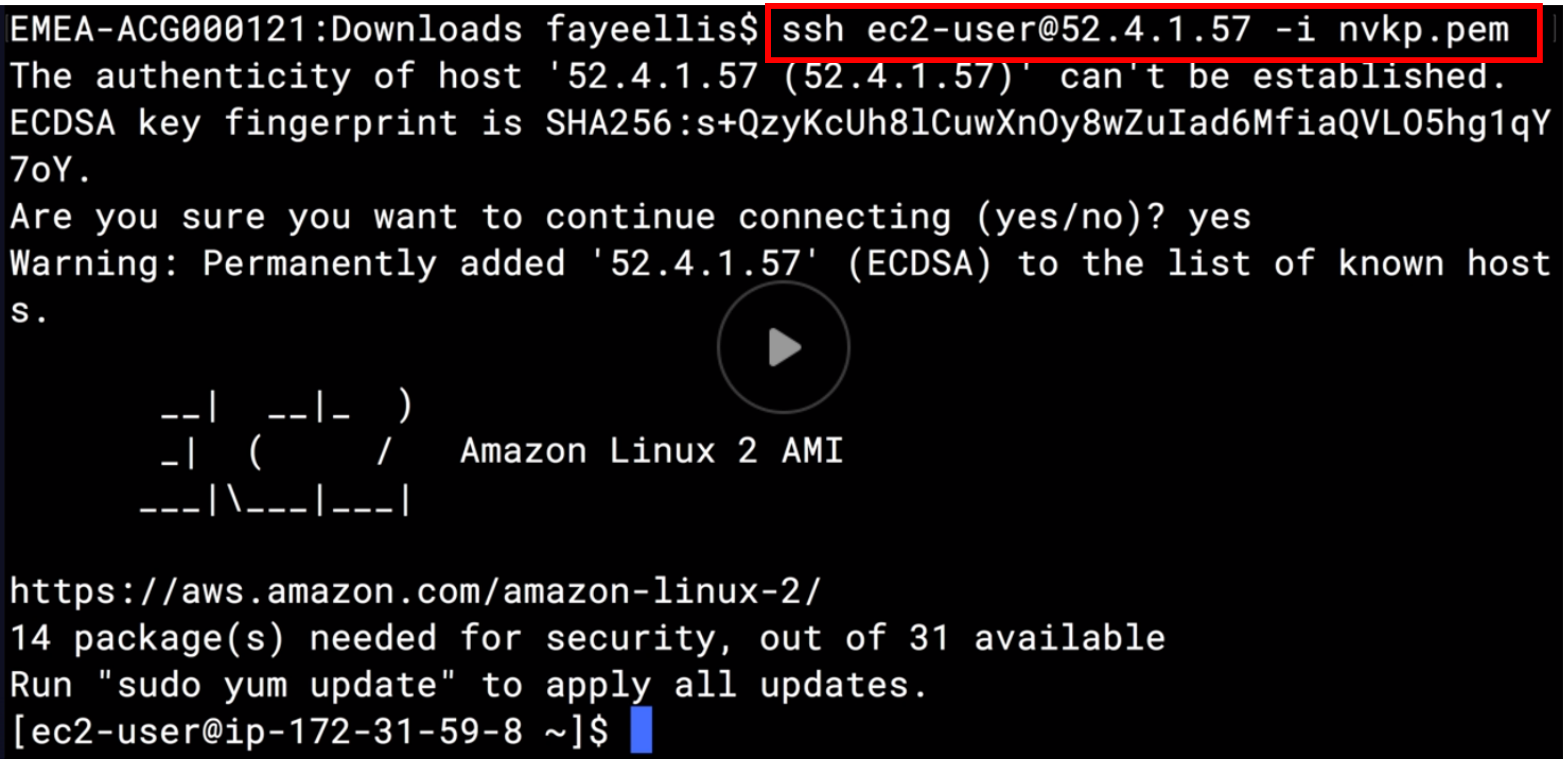
UNDERSTANDING KMS API CALLS - DEMO

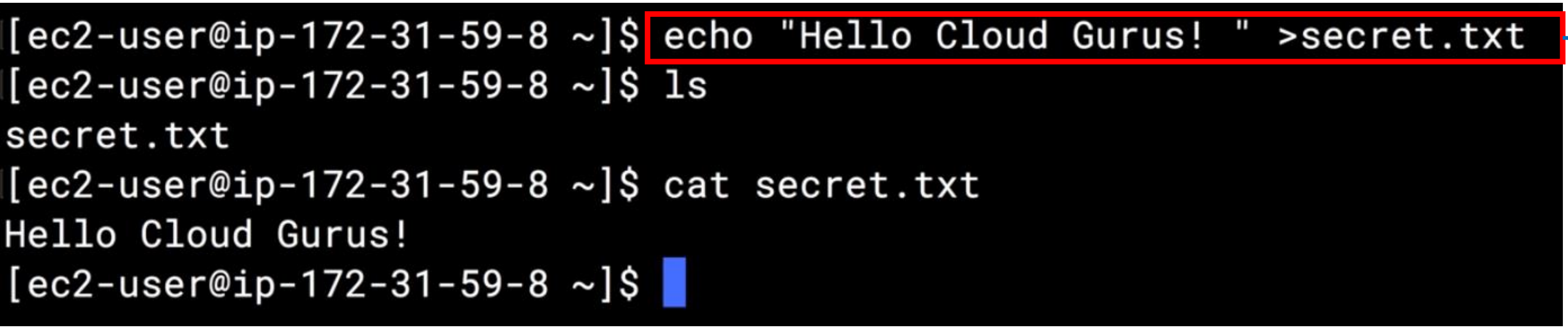
Architecture Overview



Create CMK
Launch instance in the same region where CMK is created

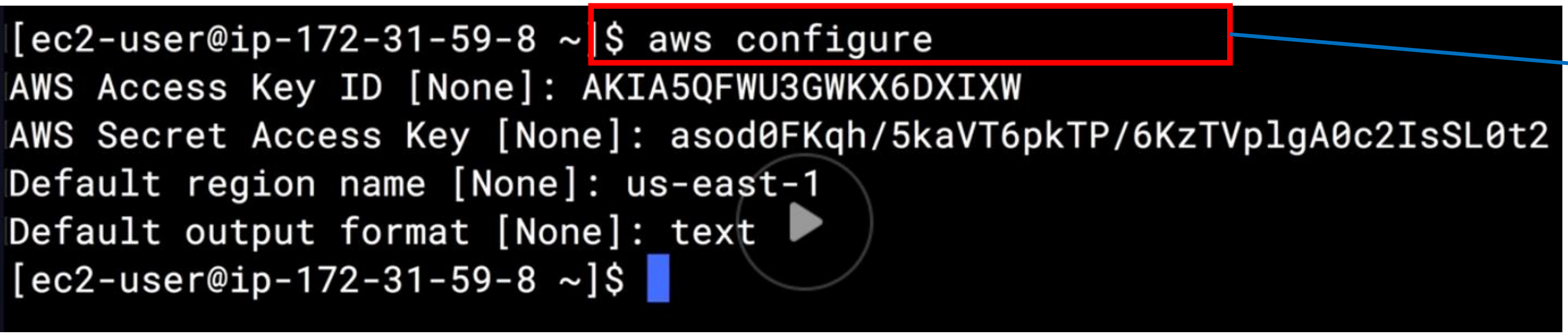


```
EMEA-ACG000121:Downloads fayeellis$ ssh ec2-user@52.4.1.57 -i nvkp.pem
The authenticity of host '52.4.1.57 (52.4.1.57)' can't be established.
ECDSA key fingerprint is SHA256:s+QzyKcUh8lCuwXnOy8wZuIad6MfiaQVLO5hg1qY
7oY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.4.1.57' (ECDSA) to the list of known host
s.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
14 package(s) needed for security, out of 31 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-59-8 ~]$ 
```



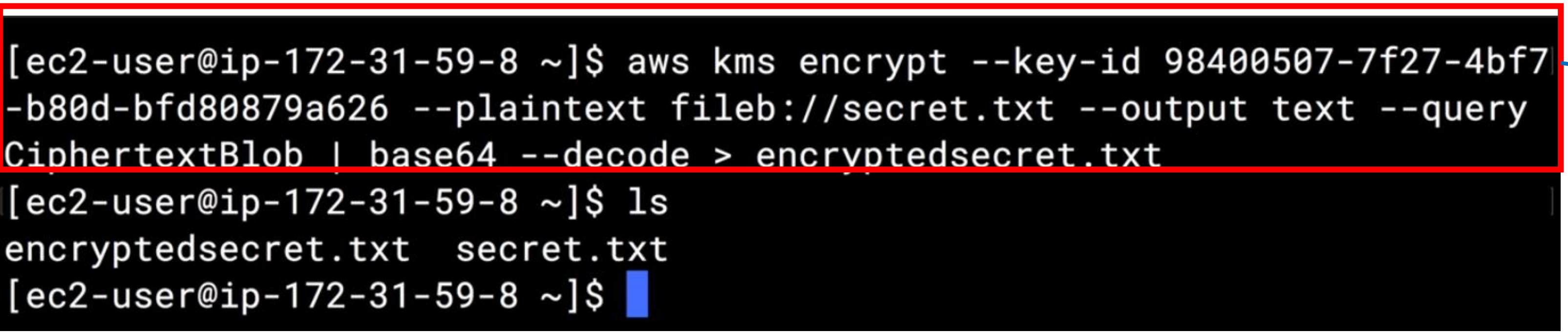
```
[ec2-user@ip-172-31-59-8 ~]$ echo "Hello Cloud Gurus! " >secret.txt
[ec2-user@ip-172-31-59-8 ~]$ ls
secret.txt
[ec2-user@ip-172-31-59-8 ~]$ cat secret.txt
Hello Cloud Gurus!
[ec2-user@ip-172-31-59-8 ~]$
```

Plain Text file that we are going to encrypt



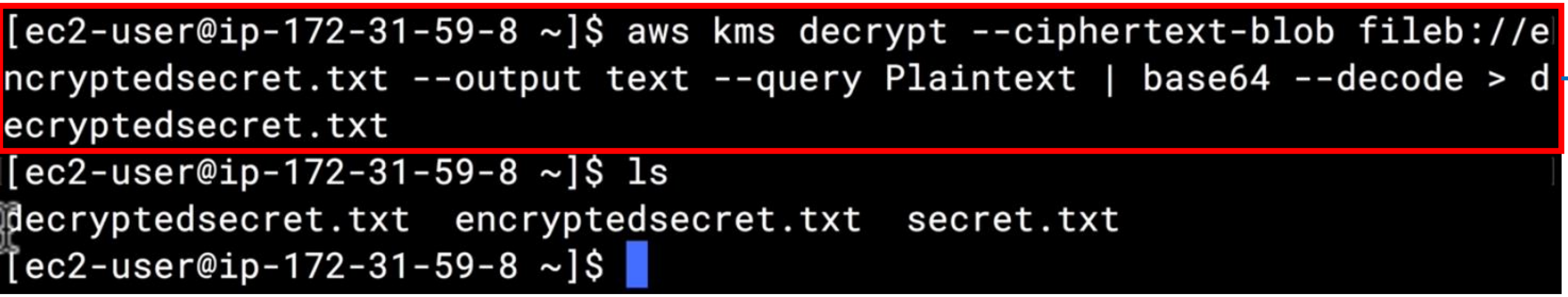
```
[ec2-user@ip-172-31-59-8 ~]$ aws configure
AWS Access Key ID [None]: AKIA5QFWU3GWKX6DXIXW
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: text
[ec2-user@ip-172-31-59-8 ~]$
```

Cofigure AWS CLI



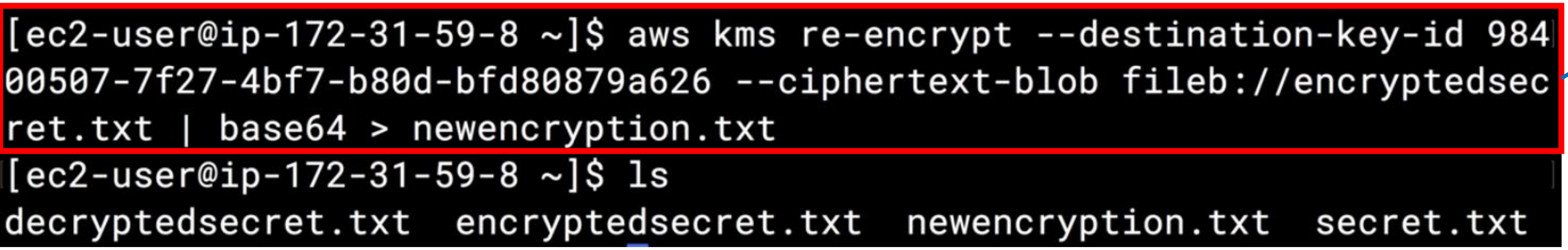
```
[ec2-user@ip-172-31-59-8 ~]$ aws kms encrypt --key-id 98400507-7f27-4bf7
-b80d-bfd80879a626 --plaintext fileb://secret.txt --output text --query
CiphertextBlob | base64 --decode > encryptedsecret.txt
[ec2-user@ip-172-31-59-8 ~]$ ls
encryptedsecret.txt  secret.txt
[ec2-user@ip-172-31-59-8 ~]$
```

Encrypt
Output – bytes format



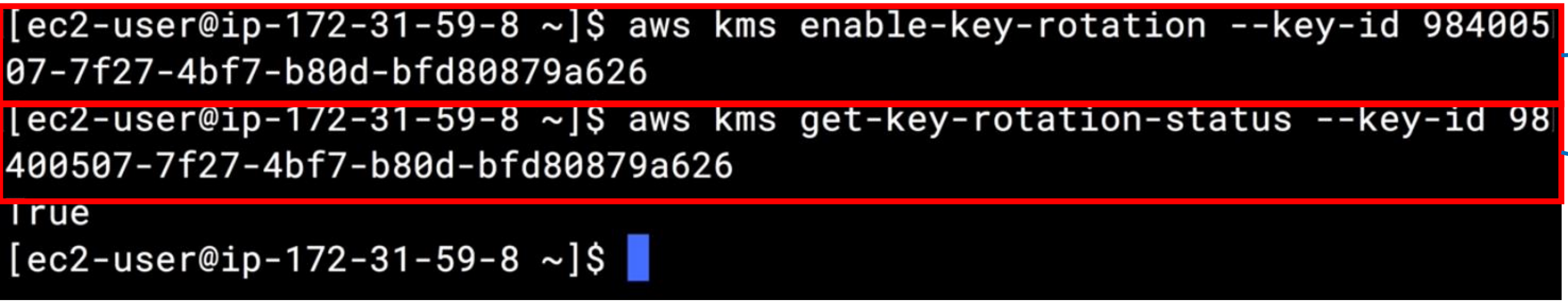
```
[ec2-user@ip-172-31-59-8 ~]$ aws kms decrypt --ciphertext-blob fileb://e
ncryptedsecret.txt --output text --query Plaintext | base64 --decode > d
ecryptedsecret.txt
[ec2-user@ip-172-31-59-8 ~]$ ls
decryptedsecret.txt  encryptedsecret.txt  secret.txt
[ec2-user@ip-172-31-59-8 ~]$ 
```

Decrypt file
Output file type – ASCII text



```
[ec2-user@ip-172-31-59-8 ~]$ aws kms re-encrypt --destination-key-id 984
00507-7f27-4bf7-b80d-bfd80879a626 --ciphertext-blob fileb://encryptedsec
ret.txt | base64 > newencryption.txt
[ec2-user@ip-172-31-59-8 ~]$ ls
decryptedsecret.txt  encryptedsecret.txt  newencryption.txt  secret.txt
```

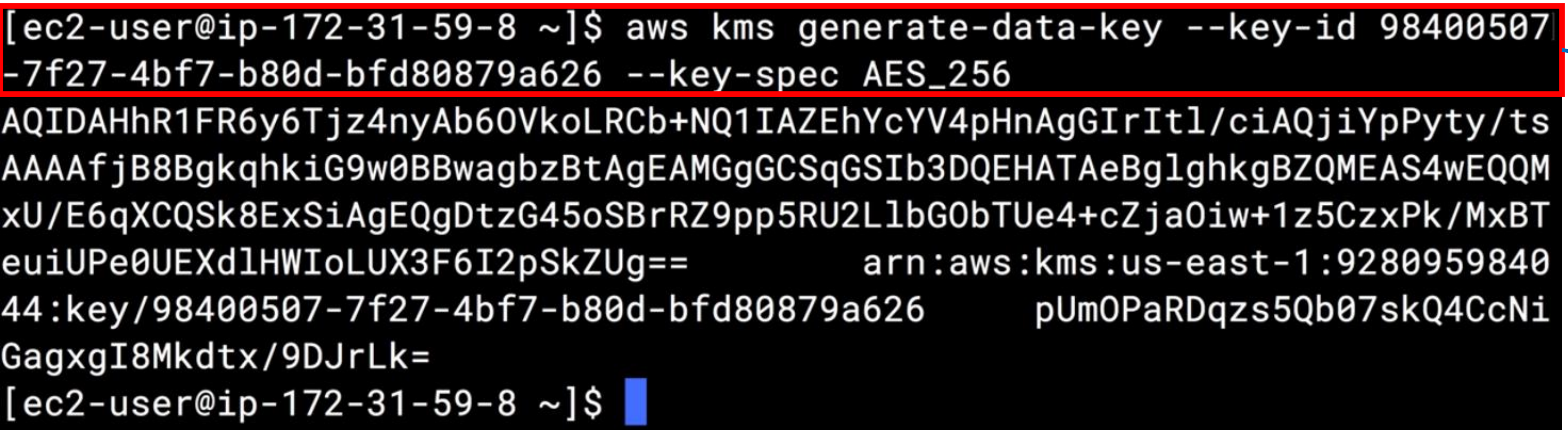
Re-encrypt takes the encrypted file and decrypt it without saving the plain text version anywhere. It decrypts and keep it in memory. Then it will re-encrypt it and save the newly encrypted file.
Useful when we want to encrypt something with different CMK.
We can re-crypt the encrypted file with different CMK id



```
[ec2-user@ip-172-31-59-8 ~]$ aws kms enable-key-rotation --key-id 984005
07-7f27-4bf7-b80d-bfd80879a626
[ec2-user@ip-172-31-59-8 ~]$ aws kms get-key-rotation-status --key-id 98
400507-7f27-4bf7-b80d-bfd80879a626
True
[ec2-user@ip-172-31-59-8 ~]$ 
```

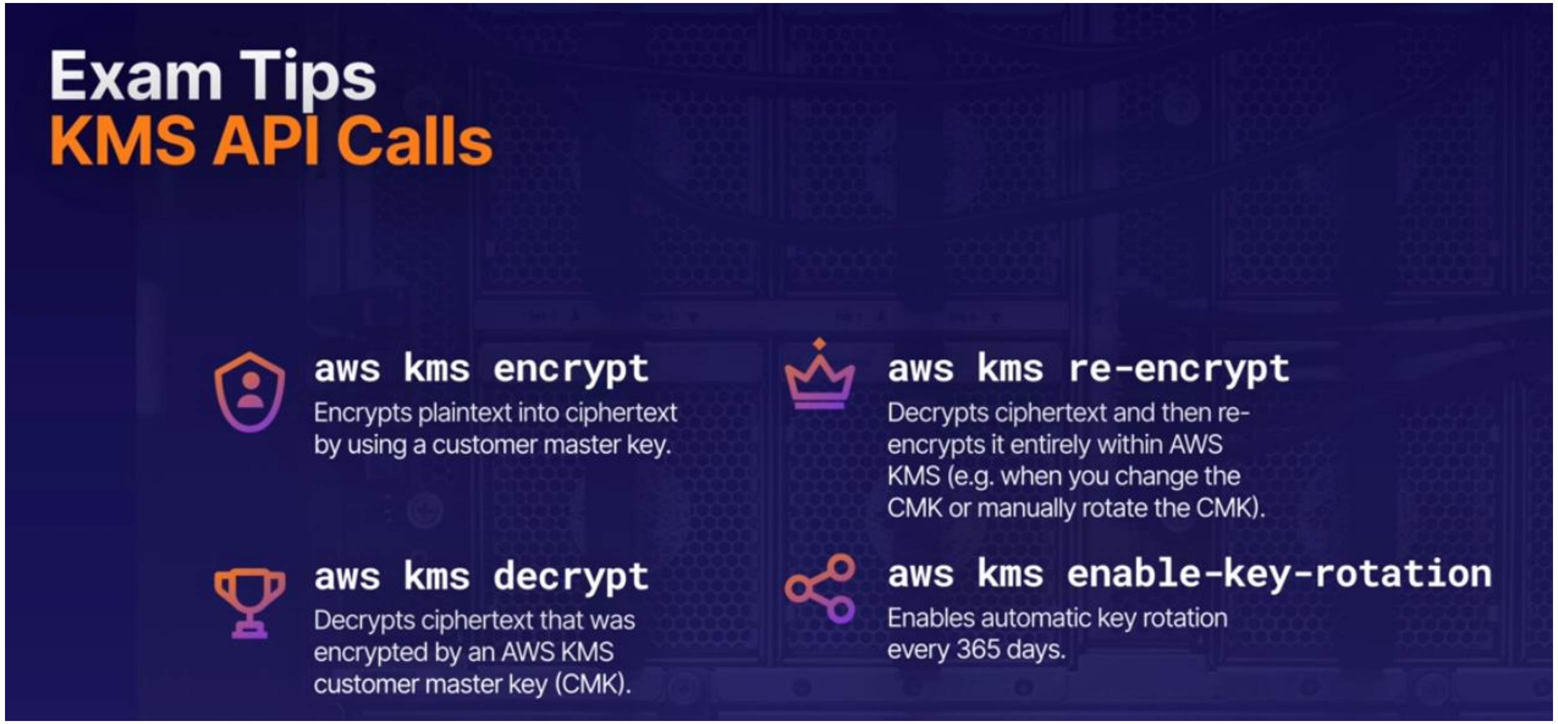
Rotate key on annual key basis

Key status



```
[ec2-user@ip-172-31-59-8 ~]$ aws kms generate-data-key --key-id 98400507
-7f27-4bf7-b80d-bfd80879a626 --key-spec AES_256
AQIDAHhR1FR6y6Tjz4nyAb6OVkoLRCb+NQ1IAZEhYcYV4pHnAgGIrItl/ciAQjiYpPyty/ts
AAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM
xU/E6qXCQSk8ExSiAgEQgDtzG45oSBrRZ9pp5RU2LlbGObTUe4+cZjaOiw+1z5CzxPk/MxBT
euiUPe0UEXdlHWIoLUX3F6I2pSkZUg==        arn:aws:kms:us-east-1:9280959840
44:key/98400507-7f27-4bf7-b80d-bfd80879a626     pUmOPaRDqzs5Qb07skQ4CcNi
GagxgI8Mkdtx/9DJrLk=
[ec2-user@ip-172-31-59-8 ~]$
```

Encryption and decryption on large amounts of data. It will give plain text version and cypher text version of the datakey



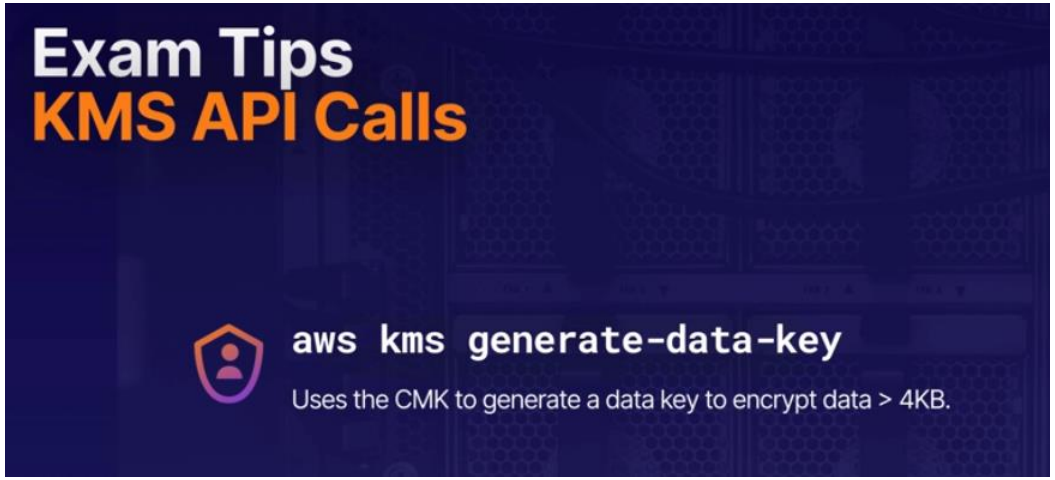
Exam Tips
KMS API Calls

`aws kms encrypt`
Encrypts plaintext into ciphertext by using a customer master key.

`aws kms re-encrypt`
Decrypts ciphertext and then re-encrypts it entirely within AWS KMS (e.g. when you change the CMK or manually rotate the CMK).

`aws kms decrypt`
Decrypts ciphertext that was encrypted by an AWS KMS customer master key (CMK).

`aws kms enable-key-rotation`
Enables automatic key rotation every 365 days.



Exam Tips
KMS API Calls

`aws kms generate-data-key`
Uses the CMK to generate a data key to encrypt data > 4KB.