Solutions Architect Professional

AWS Security

KMS Question 1

20 seconds

True or False.

You can export a CMK and use it in your own applications.

T. True

F. False

aws

KMS Question 1 - Answer

True or False.

You can export a CMK and use it in your own applications.

T. True

F. False

CMKs are created and used only within the service to help ensure their security, enable your policies to be consistently enforced, and provide a centralized log of their use

aws

KMS Question 2

20 seconds

True or False.

You can I bring your own keys to AWS KMS.

T. True

F. False

aws

KMS Question 2 - Answer

True or False.

You can I bring your own keys to AWS KMS.

T. True

F. False

You can import a copy of your key from your own key management infrastructure to AWS KMS and use it with any integrated AWS service or from within your own applications. You cannot import asymmetric CMKs into AWS KMS.

aws

KMS Question 3

20 seconds

What types of keys can you import to KMS?

A. 128-bit symmetric key

B. 256-bit symmetric key

C. 256-bit asymmetric key

D. 512-bit symmetric key

E. All of the above

aws

KMS Question 3

W
ir

You can import 256-bit symmetric keys.

C. 256-bit asymmetric key

D. 512-bit symmetric key

E. All of the above

aws

Shared Security Model

Shared Security Model: Infrastructure Services

Such as Amazon EC2, Amazon EBS, and Amazon VPC

Customer content

Platform & Applications Management

Operating System, Network & Firewall Configuration

Client-Side Data encryption & Data Integrity Authentication

Server-Side Encryption Fire System and/or Data

Network Traffic Protection Encryption / Integrity / Identity

Optional – Opaque data: 1's and 0's (in transit/at rest)

Customer IAM

Managed by

Customers

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

AWS IAM

Managed by

amazon web services

aws

All customers benefit from the same security

Certified by independent experts

- **SOC 1** (SSAE 16 & ISAE 3402) Type II
- **SOC 2 Type II** and public **SOC 3** report
- **ISO 27001**
- **ISO 9001**
- **PCI DSS Level 1** - Service Provider
- **ISO 27017** (security of the cloud)
- **ISO 27018** (personal data)

AWS Foundation Services

Compute | Storage | Database | Network

amazon web services

AWS Global Infrastructure

Availability Zones

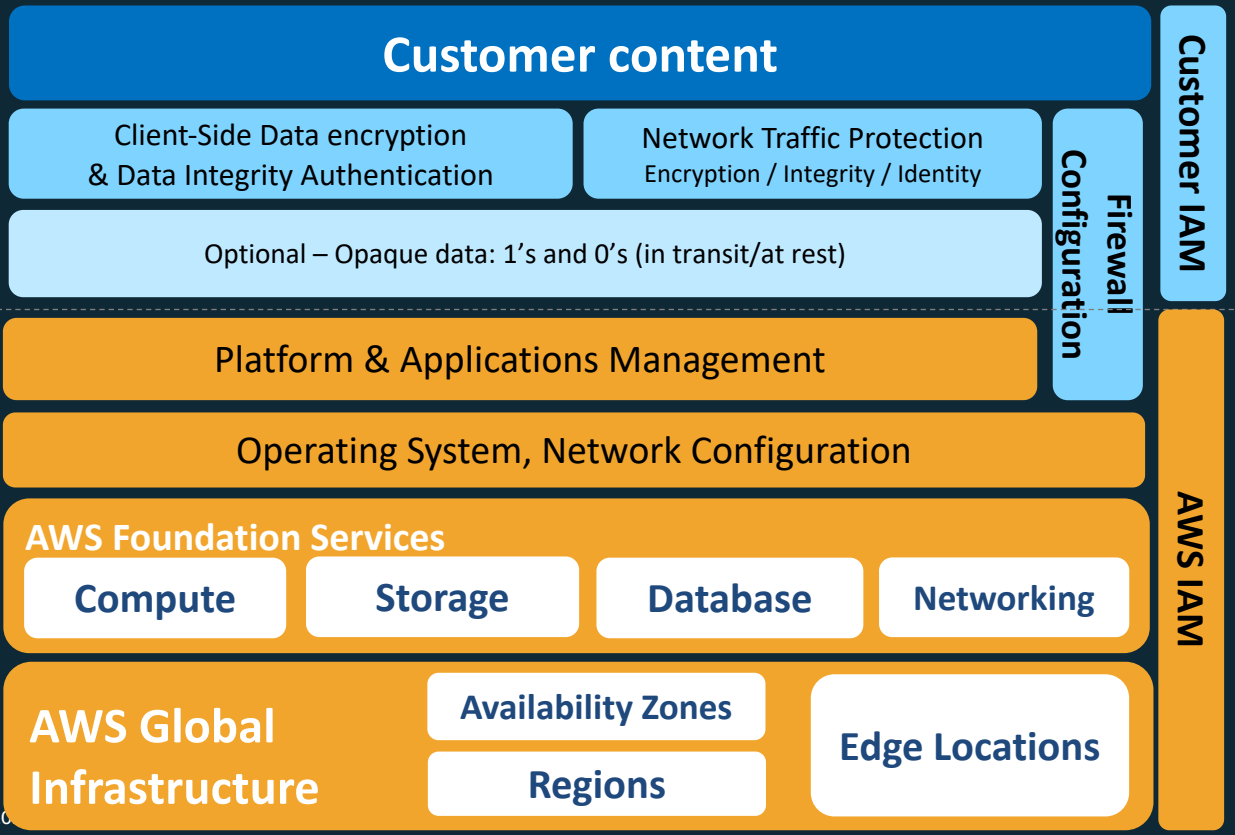
Regions

CloudFront edge locations

aws

Shared Security Model: Container Services

Such as Amazon RDS and Amazon EMR



Managed by

Customers

Managed by

amazon web services

aws

Shared Security Model: Abstracted Services

Such as Amazon S3 and Amazon DynamoDB

Managed by Customers

Customer content

Optional – Opaque Data: 1's and 0's
(in flight / at rest)

Client-Side Data Encryption
& Data Integrity Authentication

Data Protection by the Platform
Protection of Data at Rest

Network Traffic Protection by the Platform
Protection of Data at in Transit

Platform & Applications Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

Compute | **Storage** | **Database** | **Networking**

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

AWS IAM

Managed by

amazon web services

aws

Transport Security

Authenticating AWS to you and protecting confidentiality using TLS

- TLS can be used with every AWS API to protect data upload/download and configuration change

- You can provide your own certificates to be presented to your customers when using:
    - Elastic Load Balancing
    - Amazon CloudFront
    - Amazon API Gateway

AWS Certificate Manager (ACM)

- Provision trusted SSL/TLS certificates from AWS for use with AWS resources:
  - Elastic Load Balancing
  - Amazon CloudFront distributions
  - Amazon API Gateway
- AWS handles the muck
  - Key pair and CSR generation
  - Managed renewal and deployment
- Domain validation (DV) through email
- Available through AWS Management Console, AWS Command Line Interface (AWS CLI), or API

ACM-provided certificates

Domain names

- Single domain name: www.example.com
- Wildcard domain names: *.example.com
- Combination of wildcard and non-wildcard names
- Multiple domain names in the same certificate (up to 10)

ACM-provided certificates are **managed**

- Private keys are generated, protected, and managed
- ACM-provided certificates cannot be used on Amazon EC2 instances or on-premises servers
- Can be used with AWS services, such as Elastic Load Balancing and Amazon CloudFront

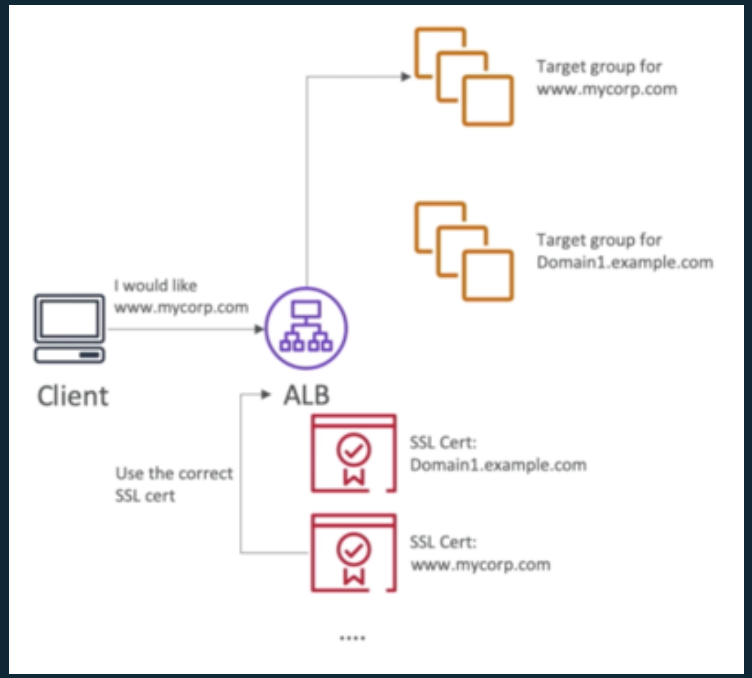
Algorithms

- RSA 2048/4096 and SHA-256/384

aws

SSL – Server Name Indication (SNI) and Smart Certificate Selection

- SNI solves the problem of loading multiple SSL certificates onto one web server (to serve multiple websites)
- It requires the client to indicate the hostname of the target server in the initial SSL handshake
- The server will find the correct certificate, or return the default one
- Only works for ALB & NLB, CloudFront
- Does not work with CLB



aws

Data-at-rest security

Basic definitions

Plaintext

Data Key

Encryption Algorithm

Ciphertext

aws

Encryption

Decryption

Options for using encryption in AWS

Client-side encryption

- You encrypt your data ***before*** data submitted to service
- You supply encryption keys OR use keys in your AWS account
- Available clients:
  - S3, EMR File System (EMRFS), DynamoDB, AWS Encryption SDK

Server-side encryption

- AWS encrypts data on your behalf ***after*** data is received by service
- 20+ integrated services including S3, Snowball, EBS, RDS, Amazon Redshift, WorkSpaces, Amazon Kinesis Firehose, CloudTrail

AWS Key Management Service (AWS KMS)

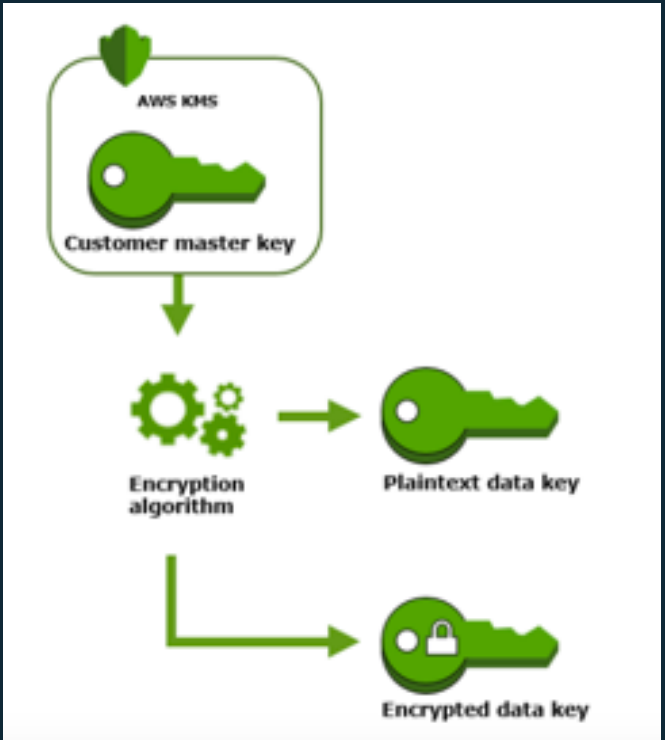
- Managed service that simplifies creation, control, rotation, deletion, and use of encryption keys in your applications
- Integrated with most of AWS services for server-side encryption
- Integrated with AWS service clients/SDKs
    - S3, EMRFS, DynamoDB, AWS Encryption SDK
- Integrated with CloudTrail to provide auditable logs of key usage for regulatory and compliance activities
- Available in all commercial regions except China

KMS Key facts

- Even though KMS is a global service but keys are regional that means you can't send keys outside the region in which they are created.
- How does AWS KMS protect the confidentiality and integrity of your keys? KMS uses FIPS 140-2 validated HSMs (Hardware Security Modules).
- Whether you are writing your own application or using other AWS services, you can control who can access your master keys and gain access to your data.
- When you are importing keys in KMS make sure to maintain a copy of those keys so that you can re-import them anytime.

aws

How does KMS encrypt your data?

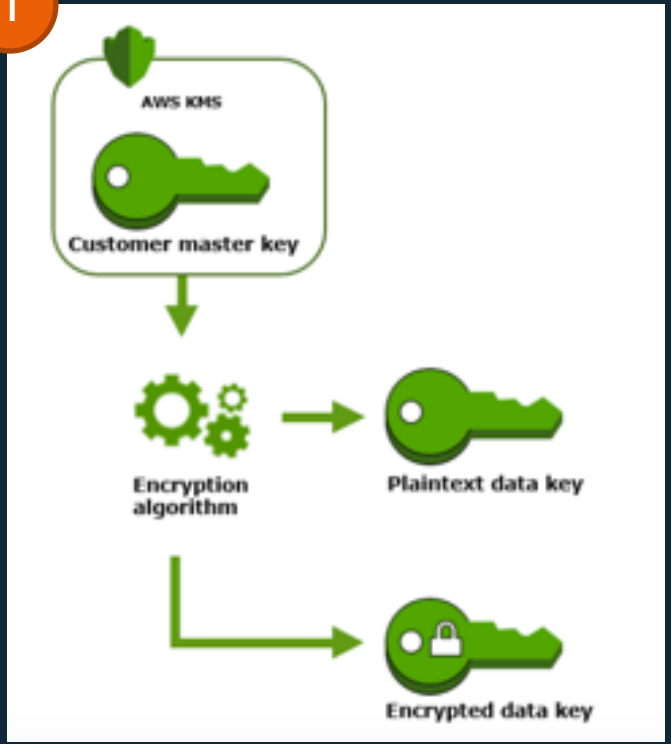


- Actually, It doesn't…
  - The primary resource of KMS is a Customer Master Key (CMK)
- The CMK can encrypt or decrypt data up to 4096 bytes.
- Why is this 4096 byte limit not a problem?
  - The CMK is used to generate Data Keys that do all the encryption outside of KMS
- CMKs never leave the HSM

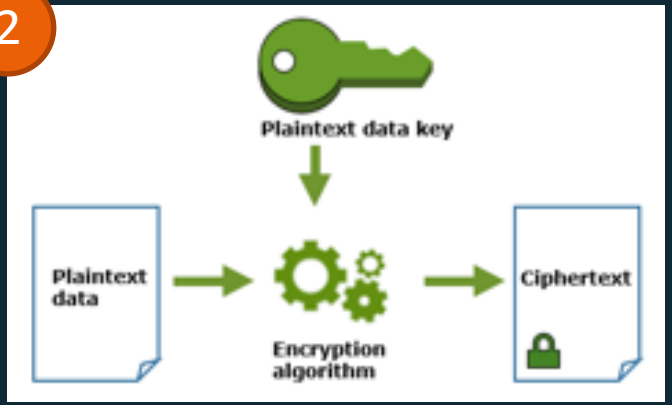
aws

How does KMS encrypt your data?

1



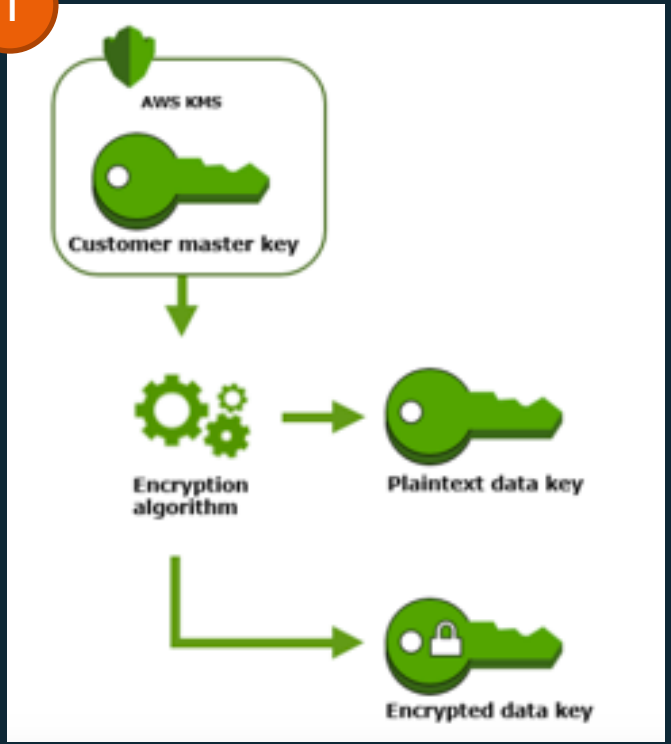
2



aws

How does KMS encrypt your data?

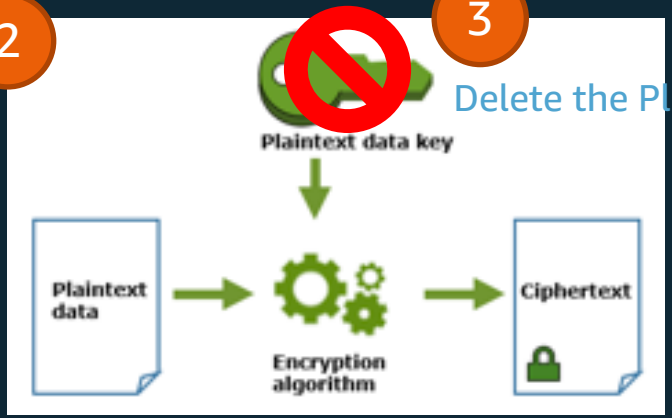
1



2

3

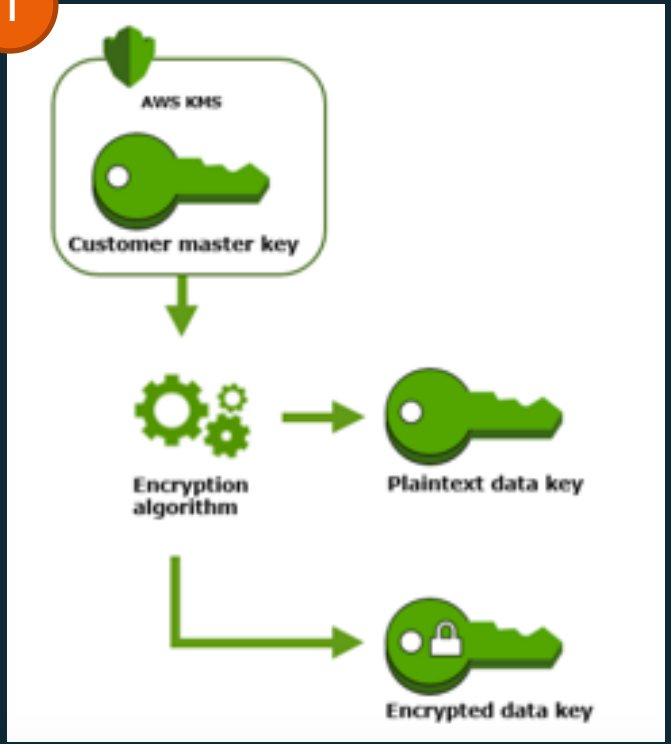
Delete the Plaintext key



aws

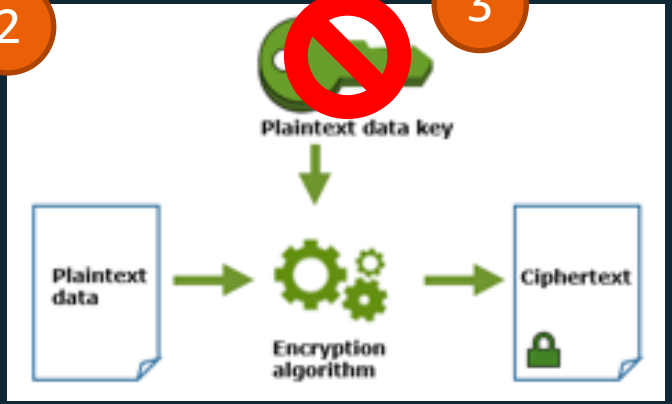
How does KMS encrypt your data?

1



2

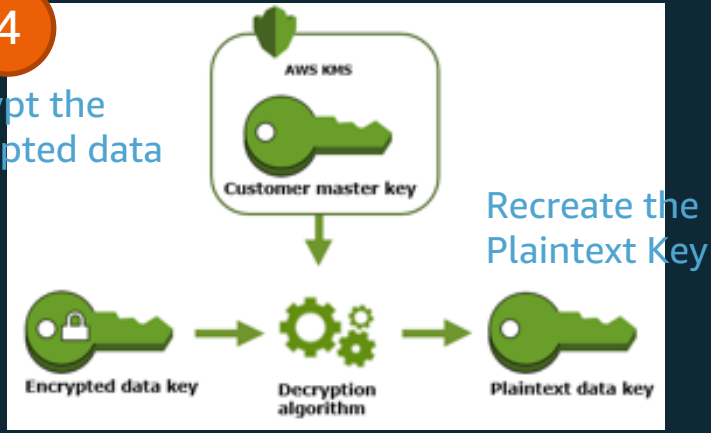
3



4

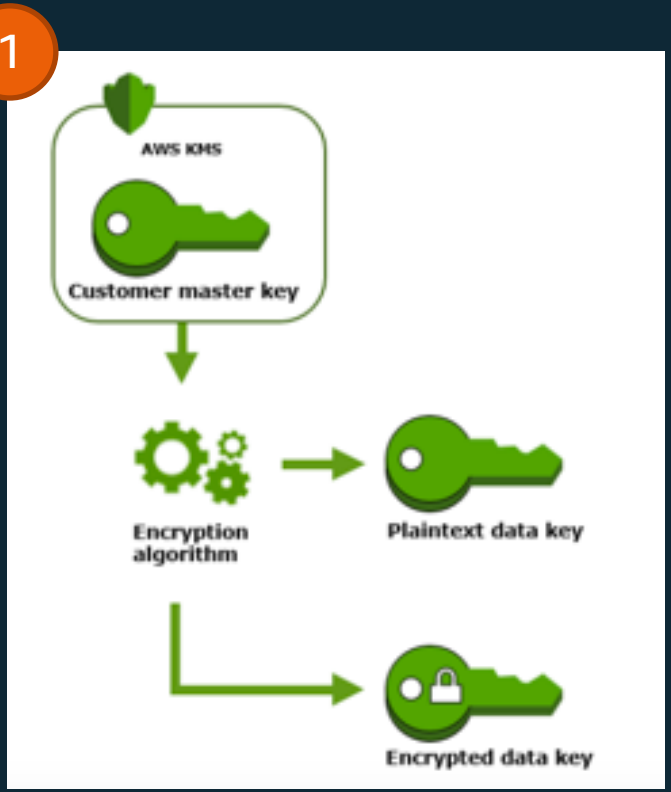
Decrypt the encrypted data key

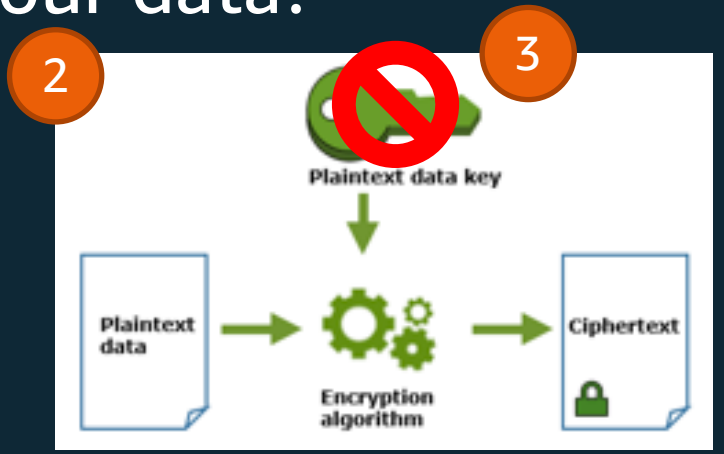
Recreate the Plaintext Key

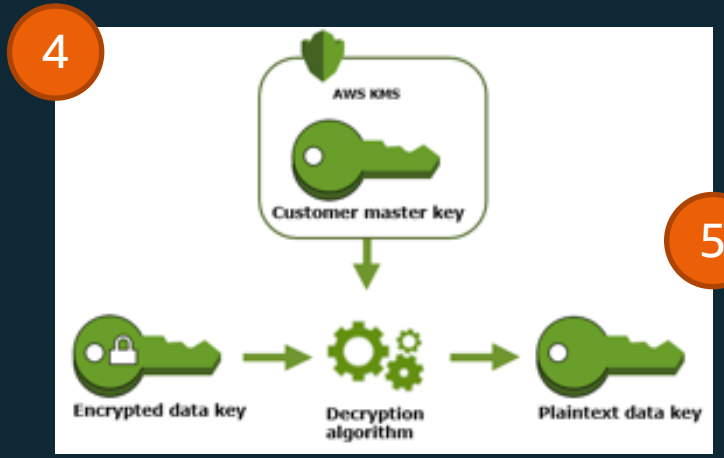


aws

How does KMS encrypt your data?





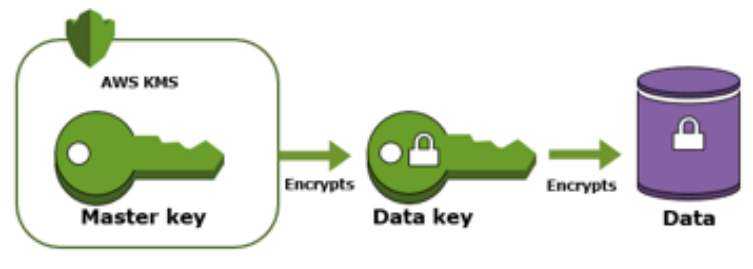


Use this key to decrypt your data

5

Then delete plaintext key

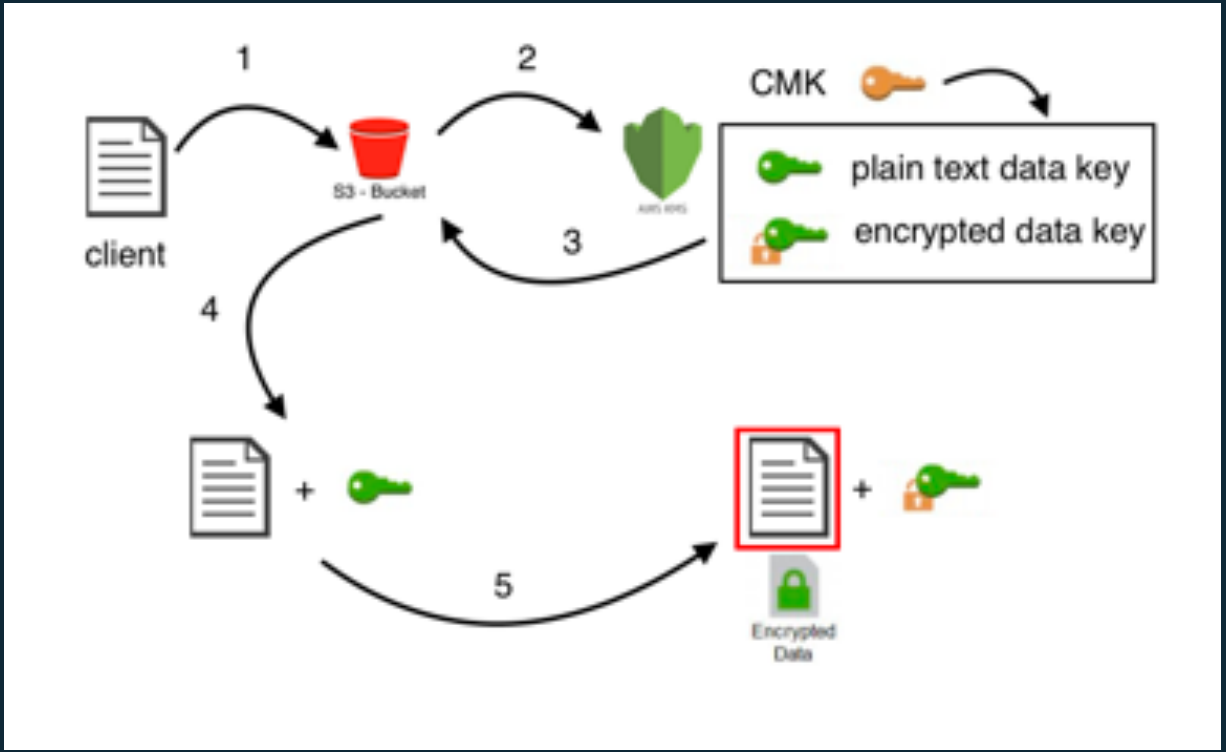
Envelope Encryption



Benefits

1. You can store the encrypted data key alongside the encrypted data
2. Low risk of exposing CMK
3. Role separation. Even if you have access to the encrypted data key and encrypted data, you can't decrypt it unless you have appropriate KMS permissions.
4. Centralized audit trail

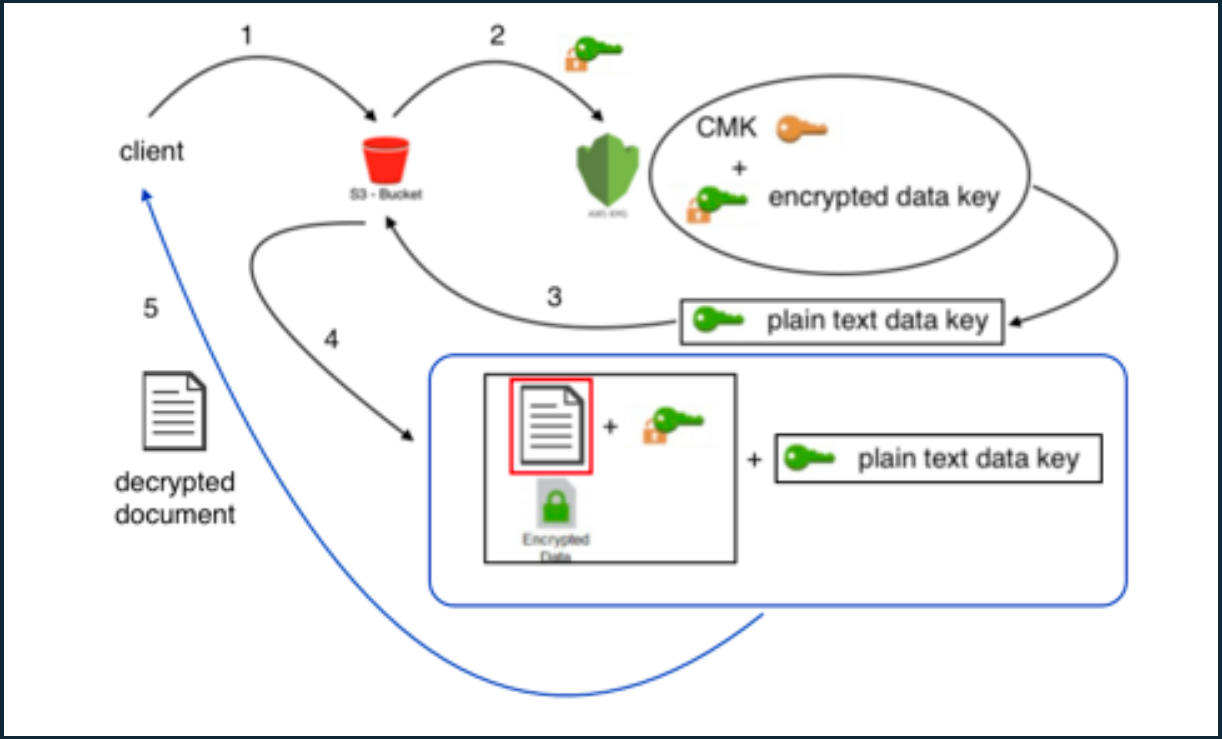
S3 SSE-KMS



1. User uploads text to bucket
2. S3 calls KMS
3. KMS uses the CMK to generate data keys and passes them both back to S3
4. S3 uses the Plaintext data key to encrypt the data
5. S3 stores the encrypted data and the encrypted data key

aws

S3 SSE-KMS



1. User want to get encrypted data
2. S3 knows the request needs to be decrypted
3. KMS uses the CMK and the encrypted data key to generate a plaintext data key
4. S3 uses the plaintext data key to decrypt the data
5. S3 returns the decrypted data to the user

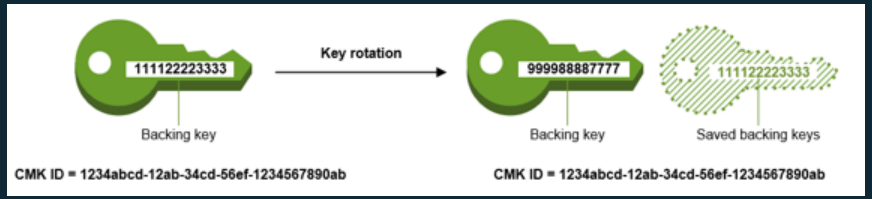
aws

Bring your own key

By default when you create a CMK, KMS generates the key material. You may also chose to import your own key material.

Automatic Key Rotation

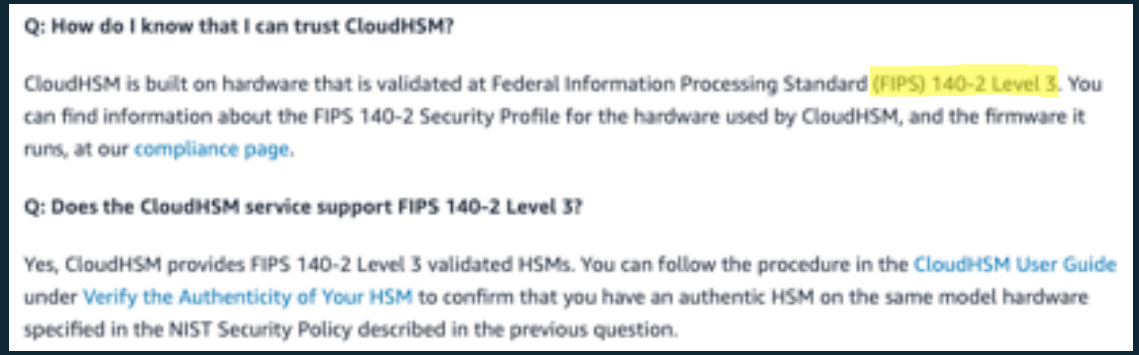
- Automatically generates new cryptographic material for the CMK every year.
- KMS also saves the old cryptographic material in perpetuity so it can be used to decrypt data that it encrypted.
- Key rotation only changes the *backing key*



- Can't change rotation for AWS managed CMKs – automatic rotation every 3 years

AWS CloudHSM

Available in all AWS regions



Q: How do I know that I can trust CloudHSM?

CloudHSM is built on hardware that is validated at Federal Information Processing Standard (FIPS) 140-2 Level 3. You can find information about the FIPS 140-2 Security Profile for the hardware used by CloudHSM, and the firmware it runs, at our compliance page.

Q: Does the CloudHSM service support FIPS 140-2 Level 3?

Yes, CloudHSM provides FIPS 140-2 Level 3 validated HSMs. You can follow the procedure in the CloudHSM User Guide under Verify the Authenticity of Your HSM to confirm that you have an authentic HSM on the same model hardware specified in the NIST Security Policy described in the previous question.

Compliance

- Included in AWS PCI DSS and SOC compliance packages
- FIPS 140-2 level 3 (maintained by Gemalto SafeNet)

Typical use cases

- Use with Amazon Redshift and RDS for Oracle
- Integrate with third-party software (Oracle, Microsoft SQL Server, Apache, SafeNet)
- Build your own custom applications

aws

Comparing CloudHSM with KMS

CloudHSM (Your own)

- Dedicated access to one or more HSM devices that comply with government standards (for example, FIPS 140-2 Level 3, Common Criteria)
- You control all access to your keys and the application software that uses them
- Supported applications:
  - Your custom software
  - Third-party software
  - AWS services: Amazon Redshift, RDS for Oracle
- Can do Asymmetric encryption also

KMS (Shared)

- Highly available and durable key storage, management, and auditable service
- Allows you to import keys
- Easily encrypt your data across AWS services and within your own applications based on policies you define
- Supported applications:
  - Your custom software built with AWS SDKs/CLI
  - AWS services (S3, EBS, RDS, Amazon Aurora, Amazon Redshift, WorkMail, WorkSpaces, CloudTrail, Elastic Transcoder)
- FIPS 140-2 Level 2

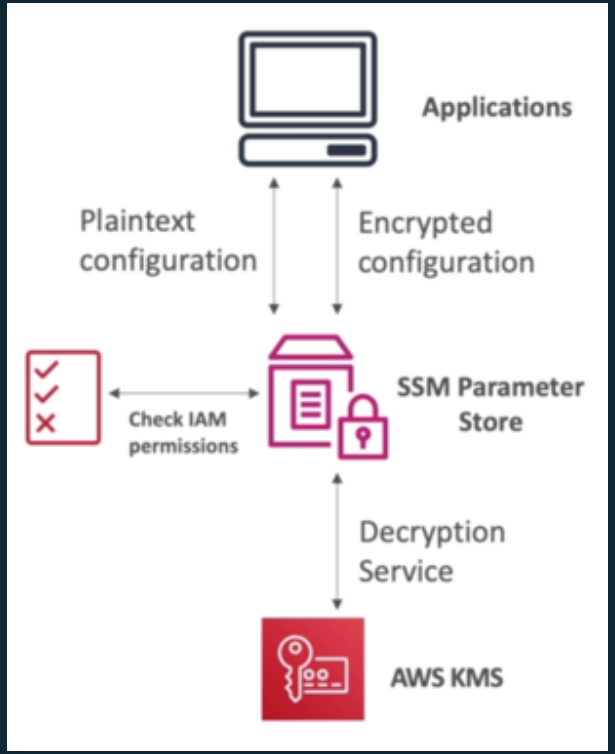
aws

AWS Parameter Store

AWS Parameter Store

- Secure storage for configuration and secrets
- Optional seamless encryption using KMS
- Serverless, scalable, durable, easy SKD, free
- Version tracking of configurations / secrets
- Configuration management using path & IAM
- Notifications with CloudWatch Events
- Integration with CloudFormation

- Can retrieve secrets from Secrets Manager using the SSM Parameter store API



Parameter Store Hierarchy

- /my-department/
    - my-app/
        - dev/
            - db-url
            - db-password
    - other-app/
- /other-department/
- /aws/reference/secretsmanager/secret_ID_in_Secrets_Manager
- /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

AWS Secrets Manager

AWS Secrets Manager

- Meant for storing secrets
- Capability to force rotation of secrets
- Automate generation of secrets on rotation (uses Lambda)
- Integration with Amazon RDS (MySQL, PostgreSQL, Aurora)
- Secrets are encrypted using KMS

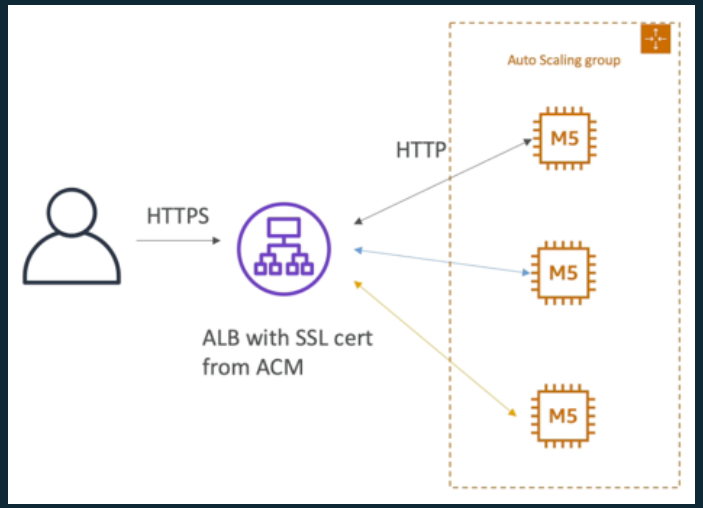
RDS Security

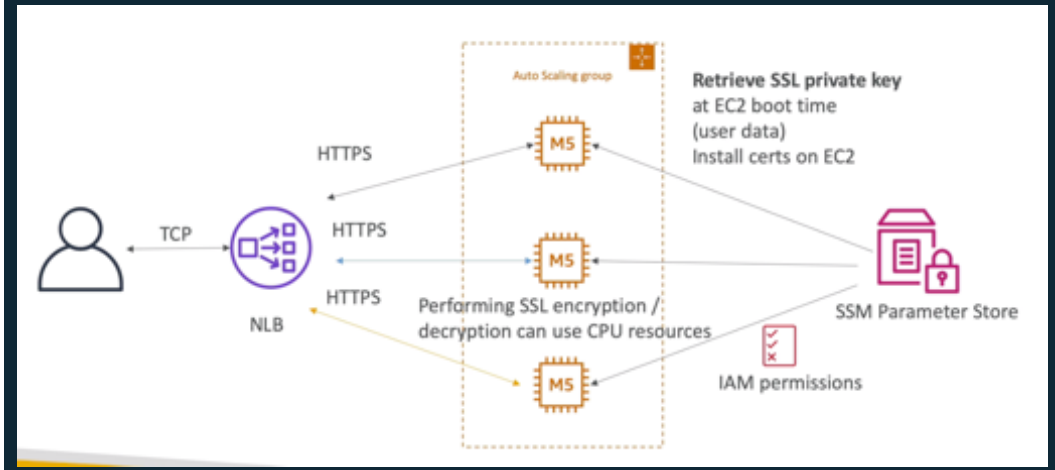
RDS Security

- KMS encryption at rest for underlying EBS volumes / snapshots
- Transparent Data Encryption (TDE) for Oracle and SQL Server
- SSL encryption to RDS is possible for all DB (in-flight)
- IAM authentication for MySQL and PostgreSQL
- Authorization still happens within RDS (not in IAM)
- Can copy an un-encrypted RDS snapshot into an encrypted one
- CloudTrail cannot be used to track queries made within RDS

SSL on ELB

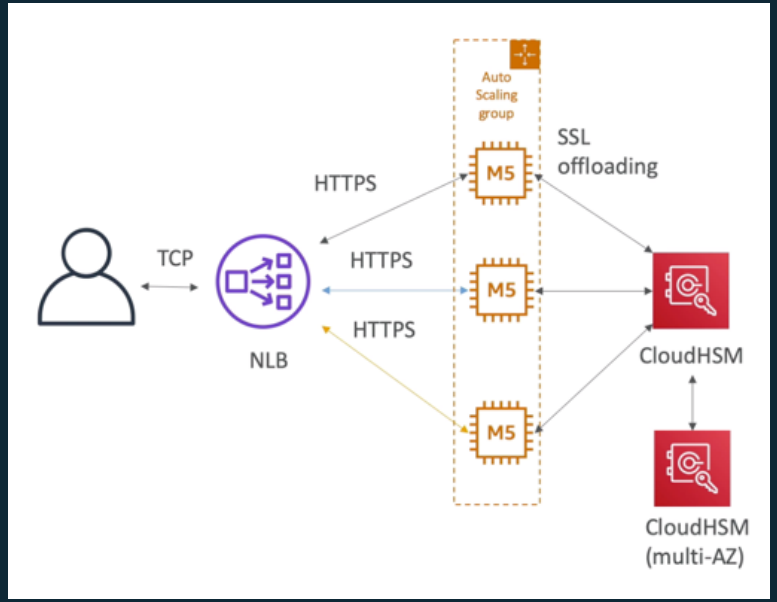
SSL on ELB





CloudHSM – SSL Offloading

- You can offload SSL to CloudHSM (SSL Acceleration)
- Supported by NGINX & Apache Web Servers
- Extra security: the SSL private key never leaves the HSM device
- Must set up a cryptographic user (CU) on the CloudHSM device)



S3 Security

S3 Encryption

- SSE-S3 – default
- SSE-KMS – uses KMS
- SSE-C – Uses your own encryption keys
- Client-side – DIY

- Glacier: All data is AES-256 encrypted, key is under AWS control

S3 Bucket Policies

- Use S3 bucket policy to:
  - Grant public access to the bucket
  - Force objects to be encrypted at upload
  - Grant access to another account (Cross-account)
- Optional Conditions on:
  - [Source IP] Public IP or Elastic IP (not on private IP)
  - [Source VPC]
  - [Source VPC Endpoint]
  - CloudFront Origin Identity
  - MFA