AWS KMS ile Client-Side Encryption

Ben Kimim

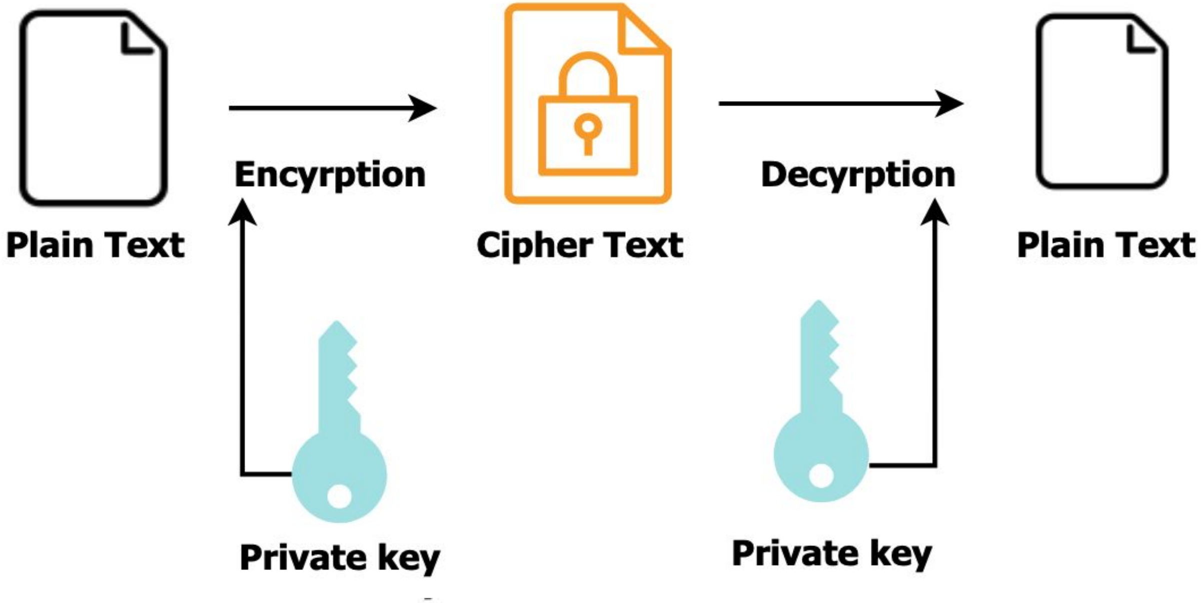
Emrullah ACAR
DevOps Engineer @VNGRS

Agenda

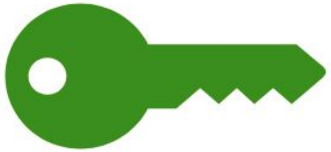
- Terminoloji
- Encryption Temelleri
- AWS Key Management Service Nedir?
- AWS KMS Key hiyerarşisi
- Demo (KMS Data Key Generate, KMS Encryption)
- AWS Encryption SDK nedir?
- AWS ESDK Encryption & Decryption
- Demo (AWS ESDK Encryption & Decrpytion)

Terminoloji

- Server-Side Encryption
- Client-Side Encryption
- Data key
- Master key
- Symmetric key
- Asymmetric key

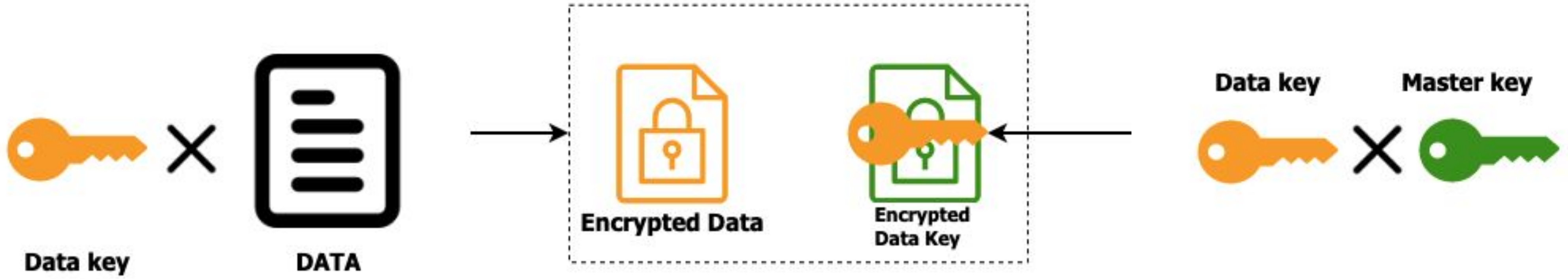


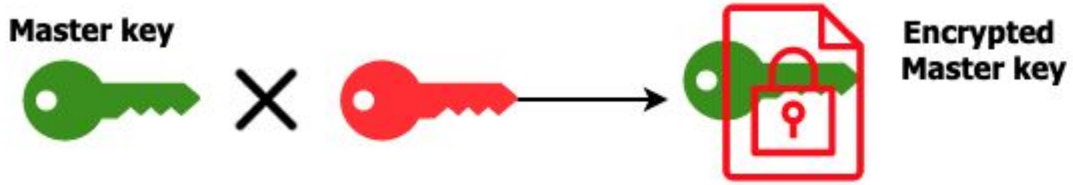
Data key



Master key

Encryption Temelleri



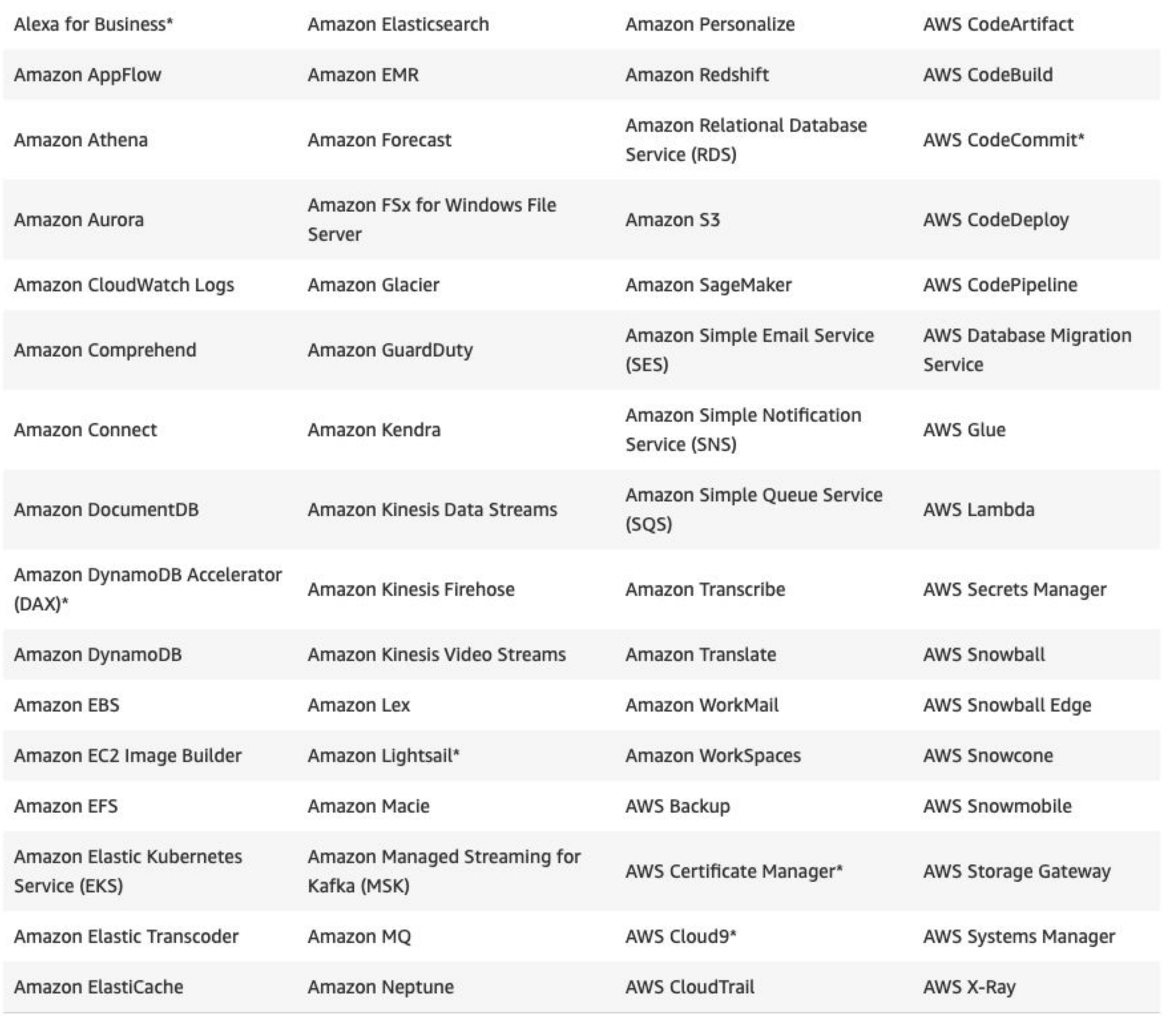


AWS Key Management Service

Customer Master Keylerimizi üretmemizi ve kontrol etmemizi sağlayan managed servis.

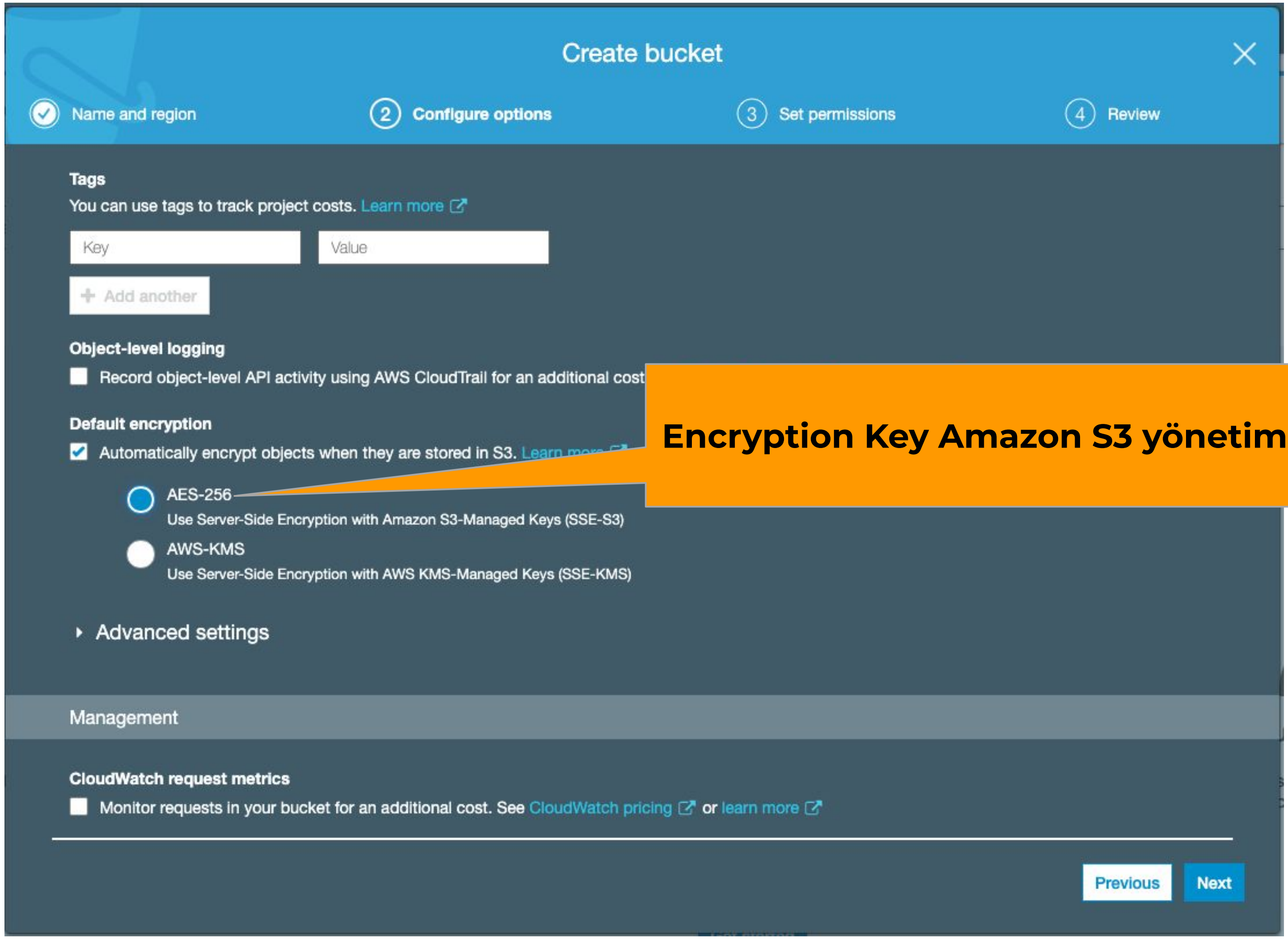
- Verilerimizi şifrelemek icin gerekli keylerimizi yönetmemizi sağlar
- High available
- Key lifecycle
- IAM Role’ler ile Yönetilebilir
- Bir çok AWS Server-side encryption servisleri ile entegre
- Cloudtrail ile Key kullanım yönetimi

AWS KMS ile Entegre Servisler



Alexa for Business*	Amazon Elasticsearch	Amazon Personalize	AWS CodeArtifact
Amazon AppFlow	Amazon EMR	Amazon Redshift	AWS CodeBuild
Amazon Athena	Amazon Forecast	Amazon Relational Database Service (RDS)	AWS CodeCommit*
Amazon Aurora	Amazon FSx for Windows File Server	Amazon S3	AWS CodeDeploy
Amazon CloudWatch Logs	Amazon Glacier	Amazon SageMaker	AWS CodePipeline
Amazon Comprehend	Amazon GuardDuty	Amazon Simple Email Service (SES)	AWS Database Migration Service
Amazon Connect	Amazon Kendra	Amazon Simple Notification Service (SNS)	AWS Glue
Amazon DocumentDB	Amazon Kinesis Data Streams	Amazon Simple Queue Service (SQS)	AWS Lambda
Amazon DynamoDB Accelerator (DAX)*	Amazon Kinesis Firehose	Amazon Transcribe	AWS Secrets Manager
Amazon DynamoDB	Amazon Kinesis Video Streams	Amazon Translate	AWS Snowball
Amazon EBS	Amazon Lex	Amazon WorkMail	AWS Snowball Edge
Amazon EC2 Image Builder	Amazon Lightsail*	Amazon WorkSpaces	AWS Snowcone
Amazon EFS	Amazon Macie	AWS Backup	AWS Snowmobile
Amazon Elastic Kubernetes Service (EKS)	Amazon Managed Streaming for Kafka (MSK)	AWS Certificate Manager*	AWS Storage Gateway
Amazon Elastic Transcoder	Amazon MQ	AWS Cloud9*	AWS Systems Manager
Amazon ElastiCache	Amazon Neptune	AWS CloudTrail	AWS X-Ray

Örneğin AWS S3 - KMS Integration



Tags

You can use tags to track project costs. Learn more

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost

Default encryption

☑ Automatically encrypt objects when they are stored in S3. Learn more

● AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

○ AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

▸ Advanced settings

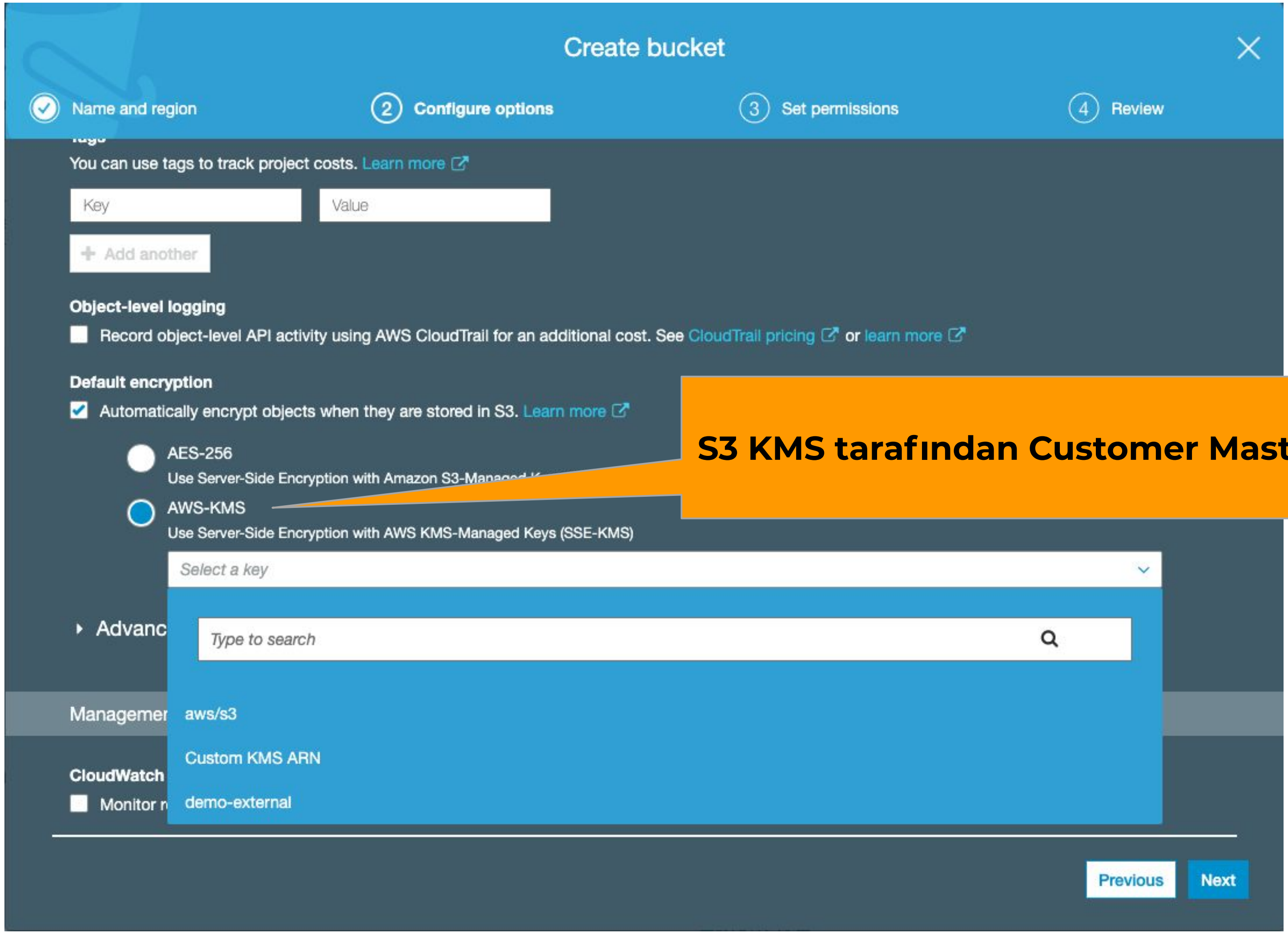
Management

CloudWatch request metrics

□ Monitor requests in your bucket for an additional cost. See CloudWatch pricing or learn more

Encryption Key Amazon S3 yönetimindedir

Örneğin AWS S3 - KMS Integration



Create bucket

✓ Name and region ② Configure options ③ Set permissions ④ Review

You can use tags to track project costs. Learn more

Key | Value

+ Add another

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

☑ Automatically encrypt objects when they are stored in S3. Learn more

○ AES-256
Use Server-Side Encryption with Amazon S3-Managed K

● AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Select a key

Type to search

- aws/s3
- Custom KMS ARN
- demo-external

▸ Advanc

Managemen

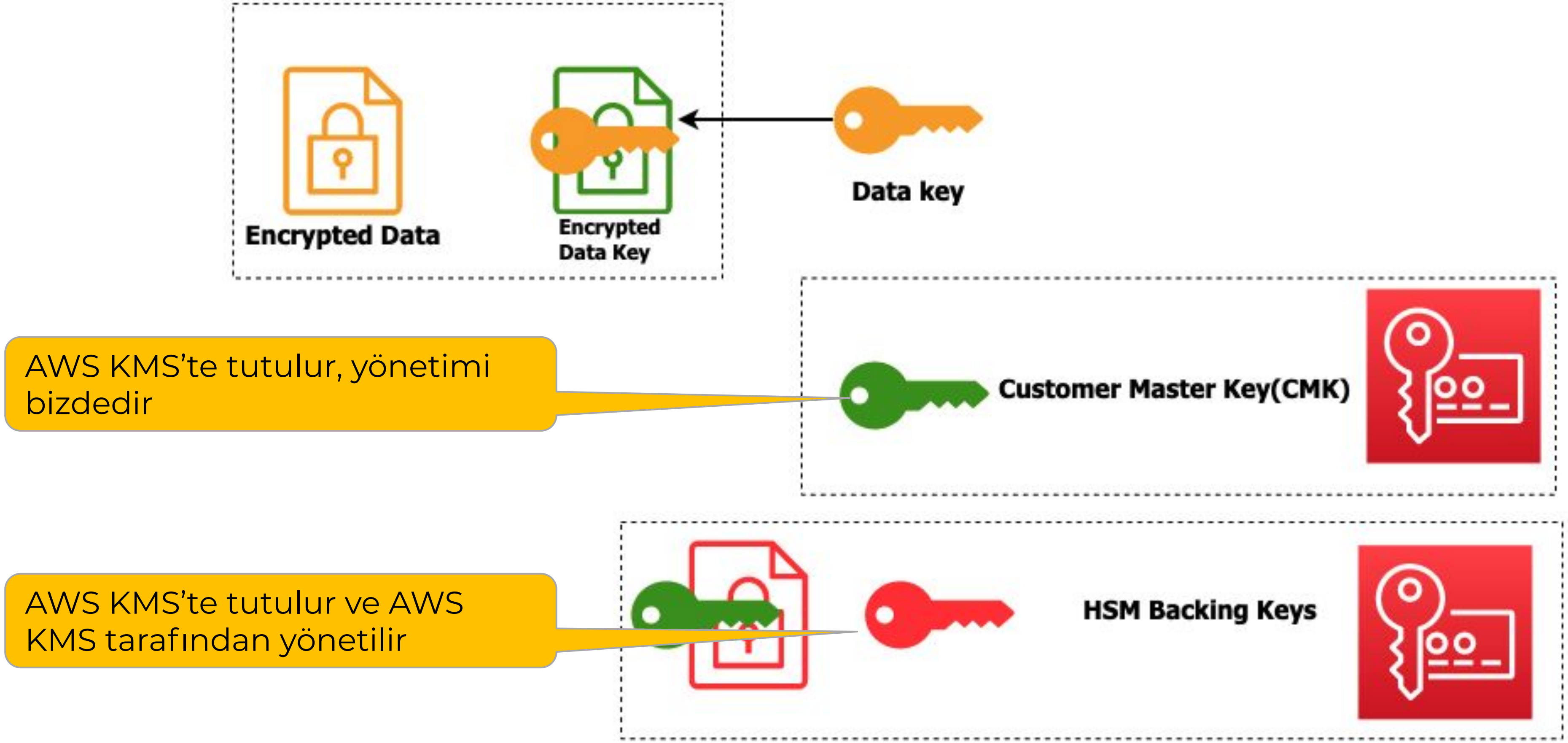
CloudWatch

□ Monitor r

Previous | Next

S3 KMS tarafından Customer Master Key'i kullanır

AWS KMS Key Hiyerarşisi



AWS KMS’te tutulur, yönetimi bizdedir

AWS KMS’te tutulur ve AWS KMS tarafından yönetilir

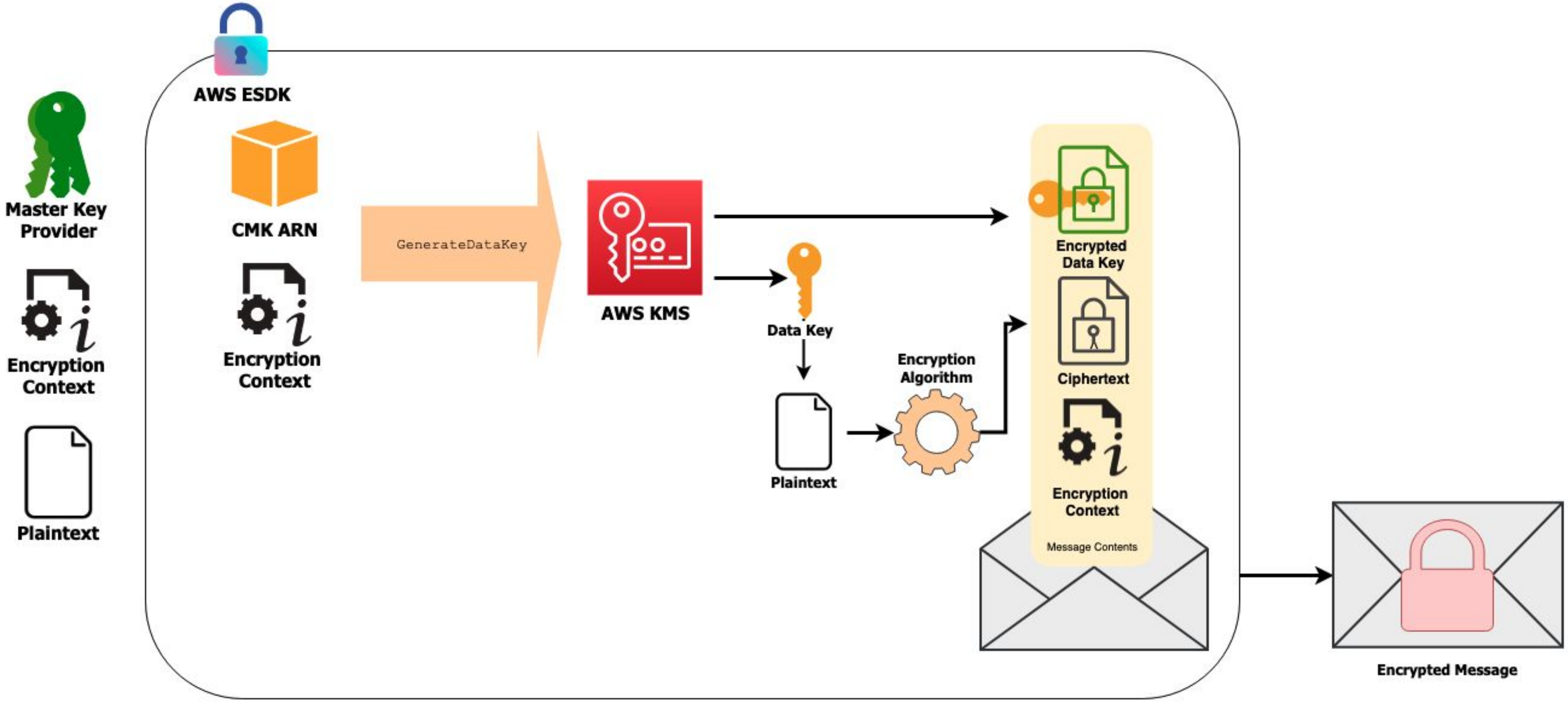
AWS KMS Demo

github.com/gokboru/aws-community-day-demo

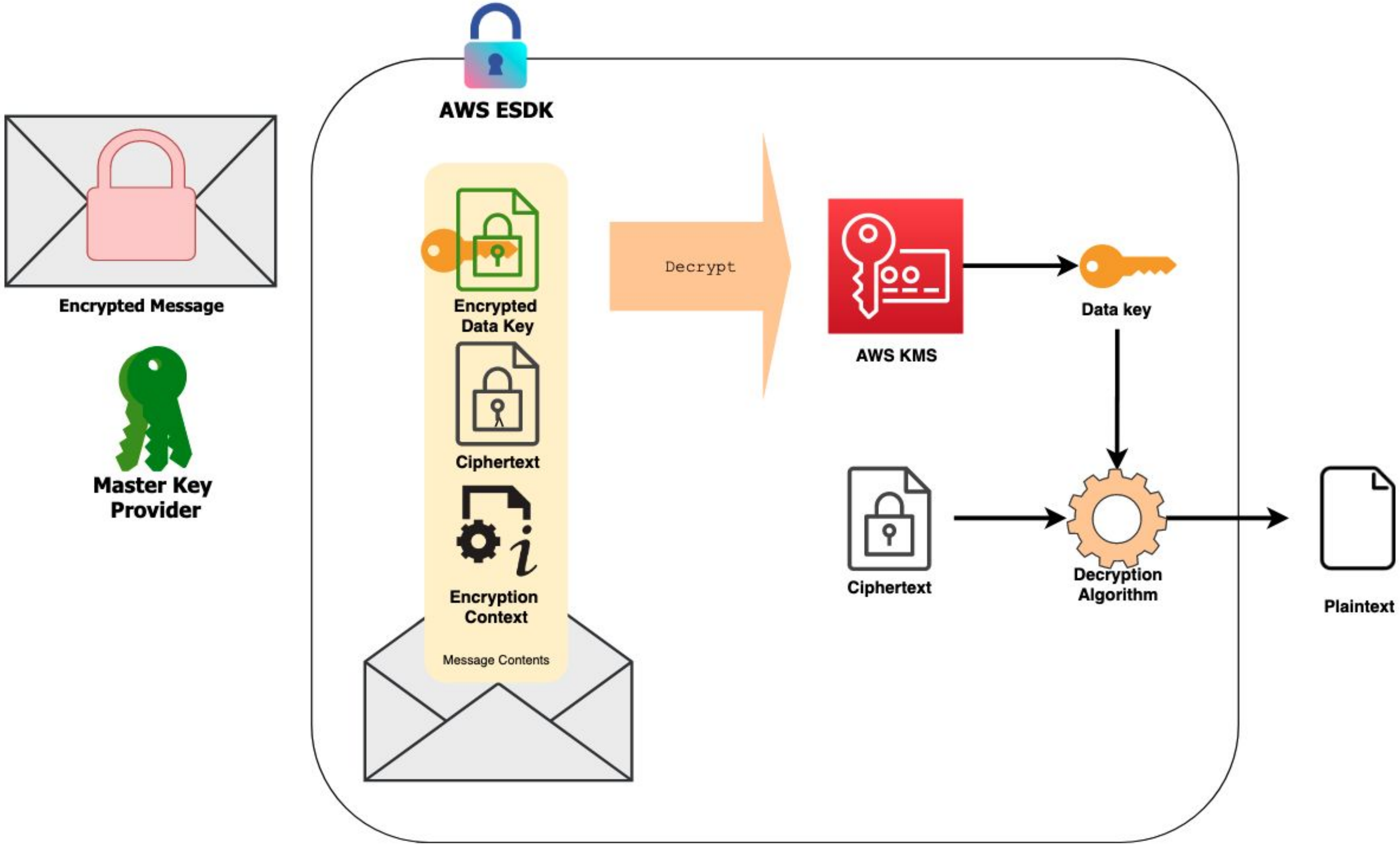
AWS Encryption SDK Nedir?

- Best Practice’lere uygun Encrypt - Decrypt yapmamıza yardımcı Client-Side Encryption Kütüphanesi
- Açık kaynak, Apache 2.0
- Çoklu dil desteği
  - AWS Encryption SDK for Python
  - AWS Encryption SDK for Java
  - AWS Encryption SDK for C
  - AWS Encryption SDK for Javascript and Node.js
  - AWS Encryption SDK for Command Line Interface
- Çoklu Master Key ve Data Key Caching

AWS Encryption SDK ile Encrypting



AWS Encryption SDK ile Decrypting



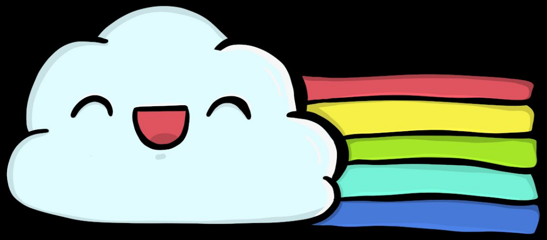
AWS Encryption SDK Github

github.com/aws/aws-encryption-sdk-python

AWS Encryption SDK Demo

github.com/gokboru/aws-community-day-demo

SORU & CEVAP



KEEP
CALM
IT WORKS
ON ALL
MACHINES

VNGRS | cloud