Enable

✓ Versioning can be done

- Versions cannot be deleted
- Versions can only be suspended

S3 optimization

default

- single blob of data
  single stream upload
  ↓
  if stream fail
  then all has to be
  restarted

- Single put data
  - slower speed with single speed.
  - unreliable

Multipart upload
min is 100MB
single put data is not worth.

parts can be fail & be restarted again
- transfer rate can be improved
  like IDM for upload

Accelerated transfer
uses S3 Edge Location
default is switchoff

- cannot contain period
- DNS compatible

Need to use new endpoint received from AWS Accelerator to get benefit of transfer Accelerator

Encryption Approaches

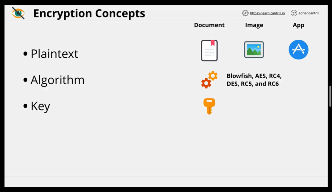
Encryption at rest

- ~~used when only one party is ther~~

- Encryption in-transit when multiple systems are involved

- plaintext - can be image document App.

- Algorithm - Blowfish, RC6



Encryption Concepts

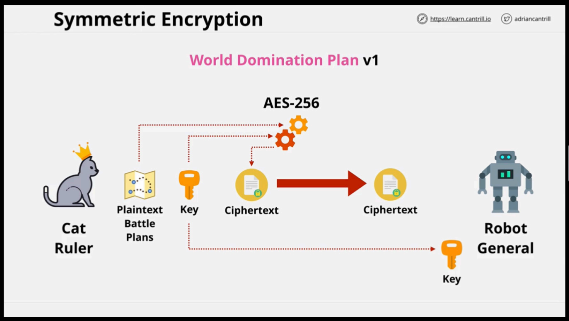
https://learn.cantrill.io adriancantrill

- Plaintext
- Algorithm
- Key

Different types of key

- Symmetric Encryption
  - Same key is used for Encryption & Decryption of data

good for Local file encryption or encryption on Laptop, local disk



Symmetric Encryption

https://learn.cantrill.io adriancantrill

World Domination Plan v1

Asymmetric Encryption

Both side needs public & private key.

- only private key can decrypt the data.
- pub is only is used to decrypt the data.

Mainly used for

- SSH, SSL

Signing

using private key we can sign in the document & we can verify identity. using public key

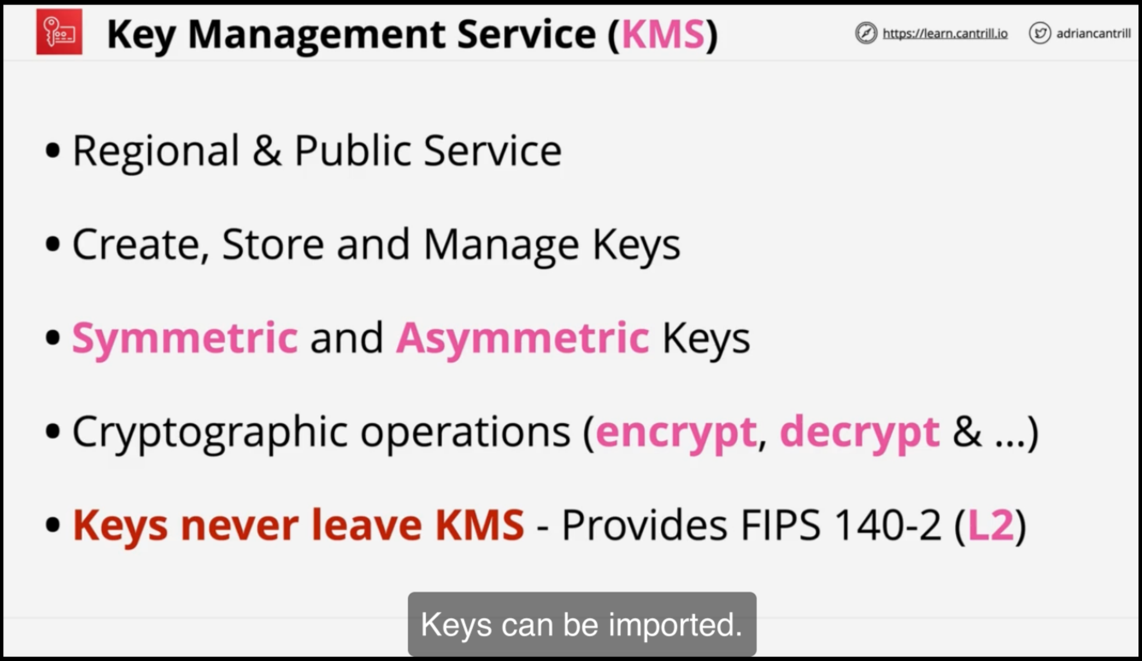
KMS

key managment service.

- regional & public service

Every region is isolated

- Used for create, store & Manage keys.



Key Management Service (KMS)

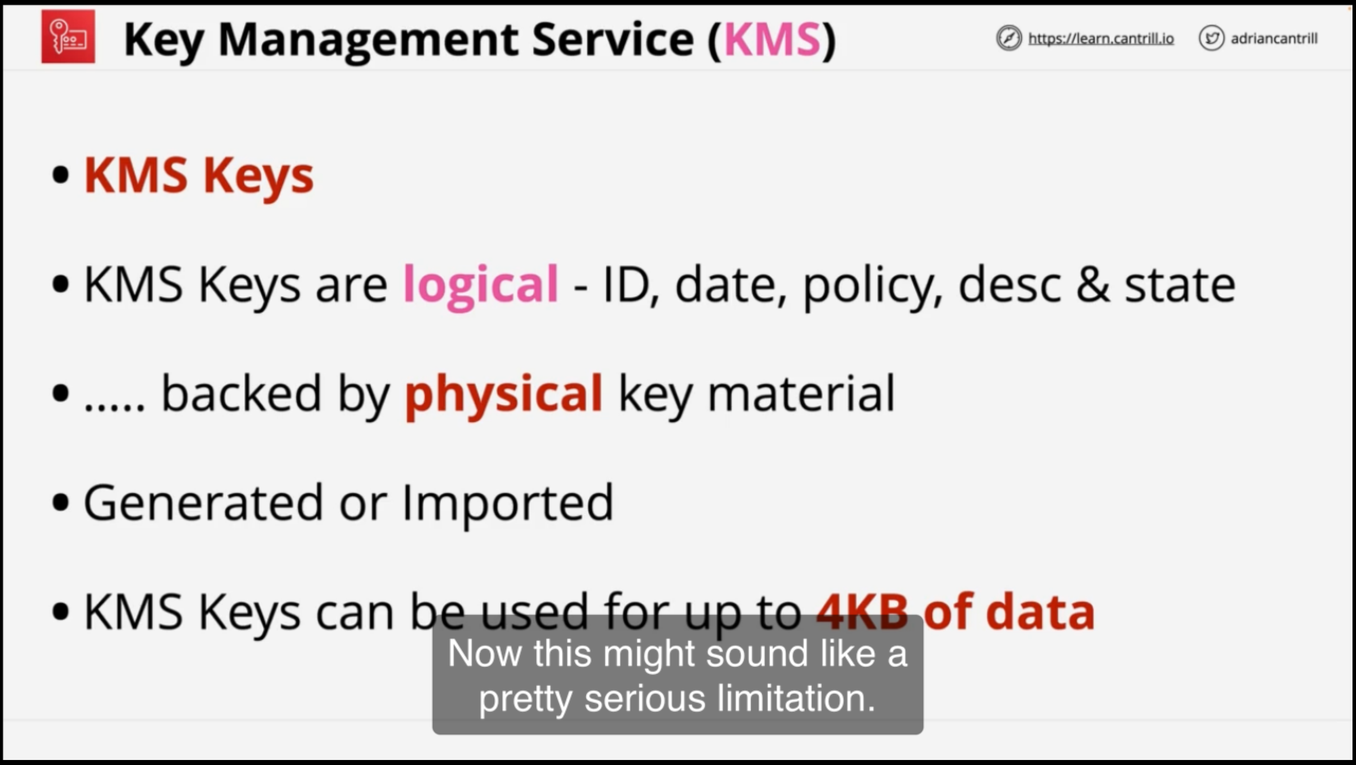
https://learn.cantrill.io adriancantrill

- Regional & Public Service
- Create, Store and Manage Keys
- **Symmetric** and **Asymmetric** Keys
- Cryptographic operations (**encrypt**, **decrypt** & ...)
- **Keys never leave KMS** - Provides FIPS 140-2 (**L2**)

Keys can be imported.

keys are locked inside the KMS - Held inside

It provides FIPS 140-2 (L2)

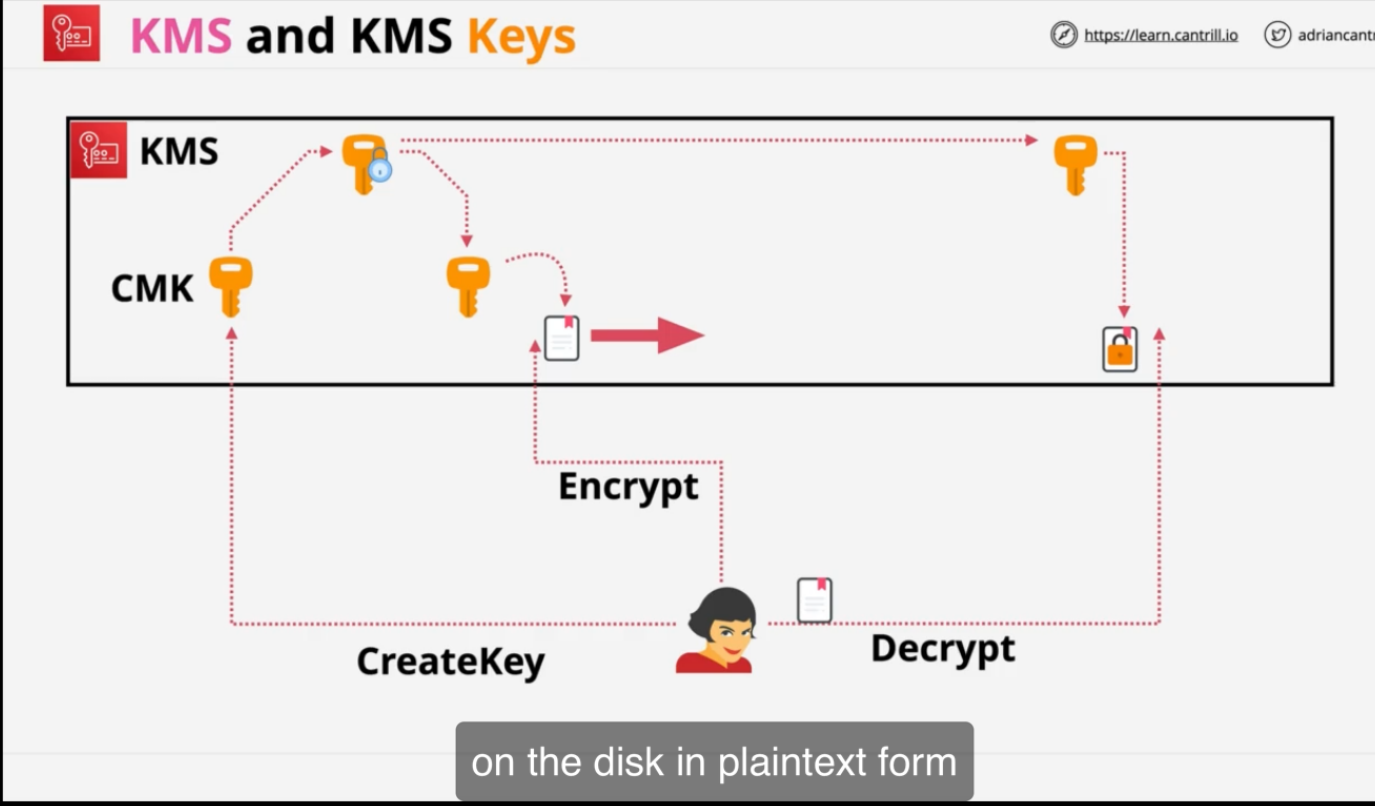


Key Management Service (KMS)

https://learn.cantrill.io adriancantrill

- **KMS Keys**
- KMS Keys are **logical** - ID, date, policy, desc & state
- ..... backed by **physical** key material
- Generated or Imported
- KMS Keys can be used for up to **4KB of data**

Now this might sound like a pretty serious limitation.



KMS and KMS Keys

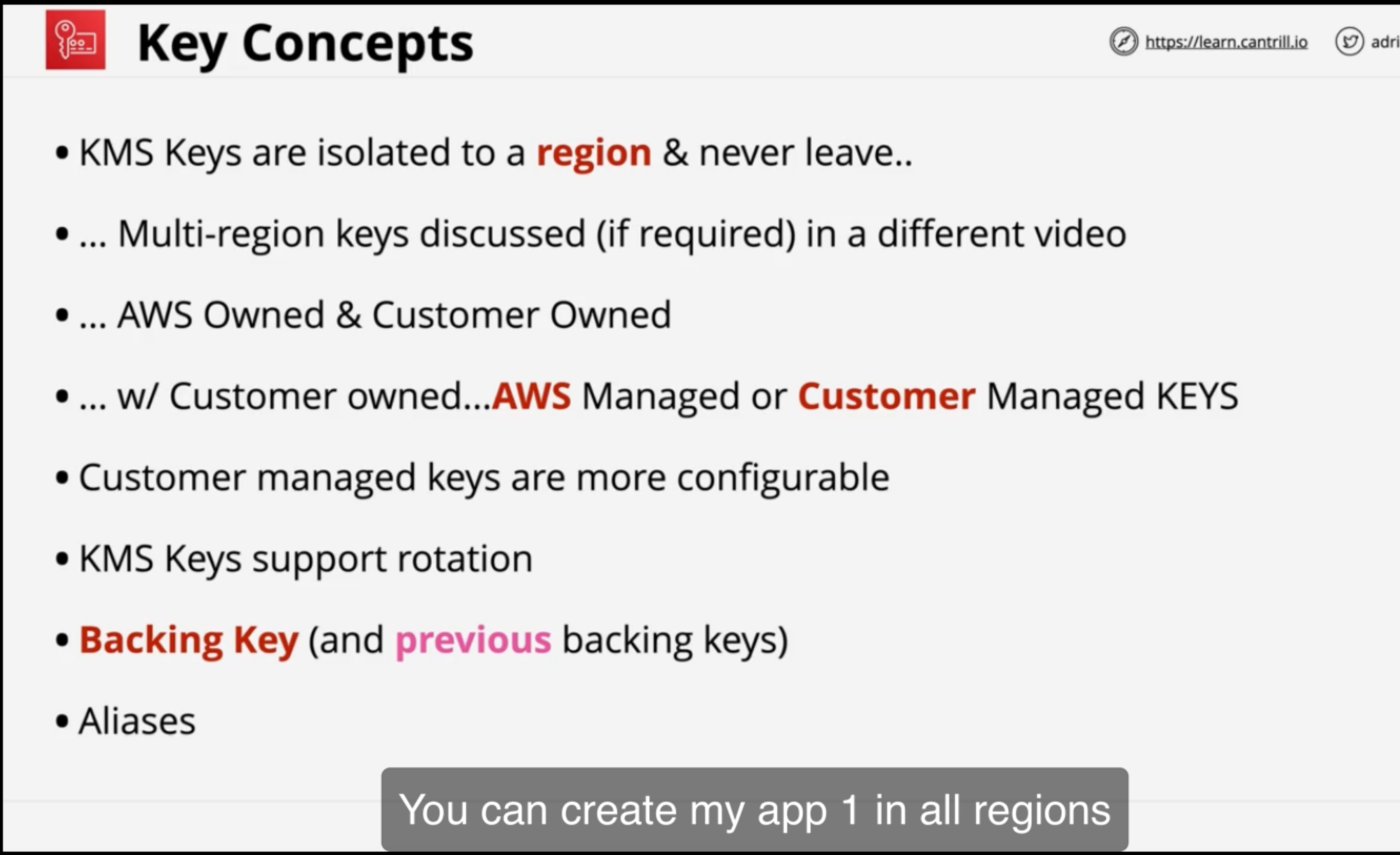
https://learn.cantrill.io adriancantr

on the disk in plaintext form

Data Encryption keys (DEK)

KMS doesn't do data Encryption on data which is larger than 4KB

you do or the service using kms.



Key Concepts

https://learn.cantrill.io adri

- KMS Keys are isolated to a **region** & never leave..
- ... Multi-region keys discussed (if required) in a different video
- ... AWS Owned & Customer Owned
- ... w/ Customer owned...**AWS** Managed or **Customer** Managed KEYS
- Customer managed keys are more configurable
- KMS Keys support rotation
- **Backing Key** (and **previous** backing keys)
- Aliases

You can create my app 1 in all regions

KMS Demo