
AWS
re:Invent

SEC201

Do you need an AWS KMS custom key store?

Tracy Pierce

Sr. Consultant – Security

AWS Professional Services

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

What is AWS Key Management Service (AWS KMS) custom key store?

- How does it work?
- Do you *really* need it?

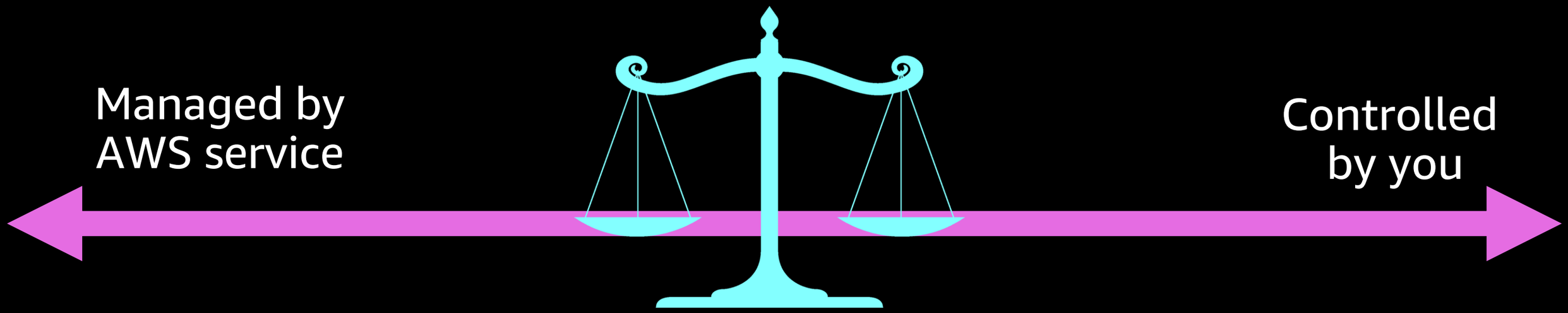


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

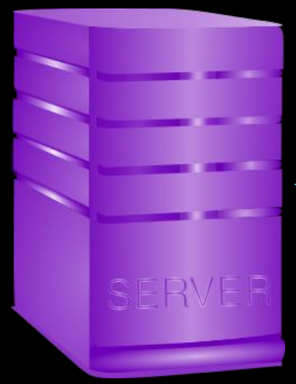
Cryptography: what, how and why



Hardware security module



AWS KMS



Your applications



Your on-prem HSM (BYOK)

Imported to KMS

AWS KMS

Native KMS

Shared FIPS 140-2 Level 2 HSM

Authentication

Authorization

Logging

AWS services



AWS CloudHSM

KMS custom key store

Single-tenant HSMs in your VPC under your control

Now with added asymmetric keys

- RSA and EC keys
- Signing for public key infrastructure (PKI), code, document, timestamp and more
- Encryption for key exchange, proof of knowledge and more
- Supported via AWS Command Line Interface (AWS CLI) today
- Keys generated and stored in FIPS-validated shared HSMs

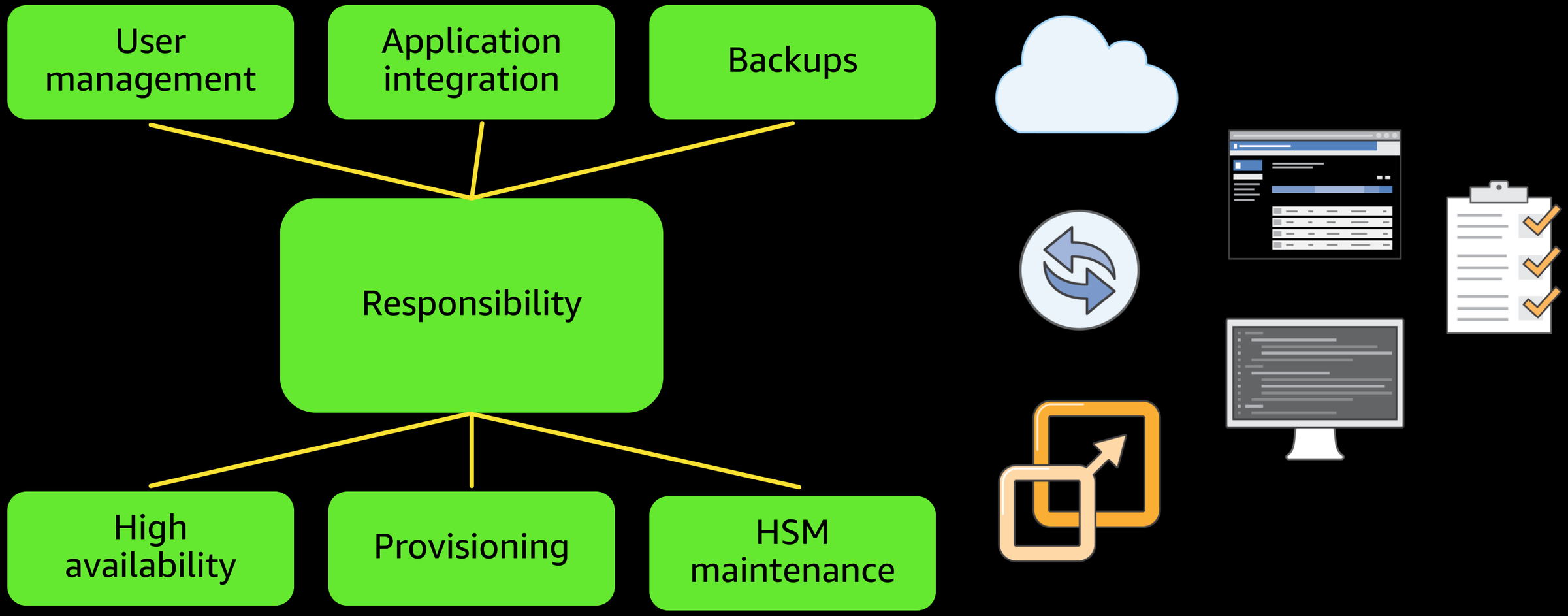
I want to have direct access to an FIPS 140-2 Level 3 HSM that I control



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CloudHSM simplifies management tasks



AWS KMS and CloudHSM

	AWS KMS	CloudHSM
Scope	AES-256 and RSA encrypt; RSA and ECC sign	Most general-purpose HSM functions (encrypt, sign /verify, derive, hash, wrap)
Secrets / keys stored in –	Shared FIPS-validated HSM	Single-tenant FIPS-validated HSM in customer VPC
HSM controlled by –	AWS	Customer
Key access by –	AWS Identity and Access Management / resource policies	Customer-defined credentials
Integrated with AWS services –	Yes	No
Secret / key operations implemented with –	AWS CLI / SDK or Encryption SDK	Customer-built application
Scalability managed by –	AWS	Customer
Keys managed by –	AWS	Customer
Rotation executed by –	AWS [not for BYOK and CKS]	Customer

AWS KMS custom key store: best of two worlds

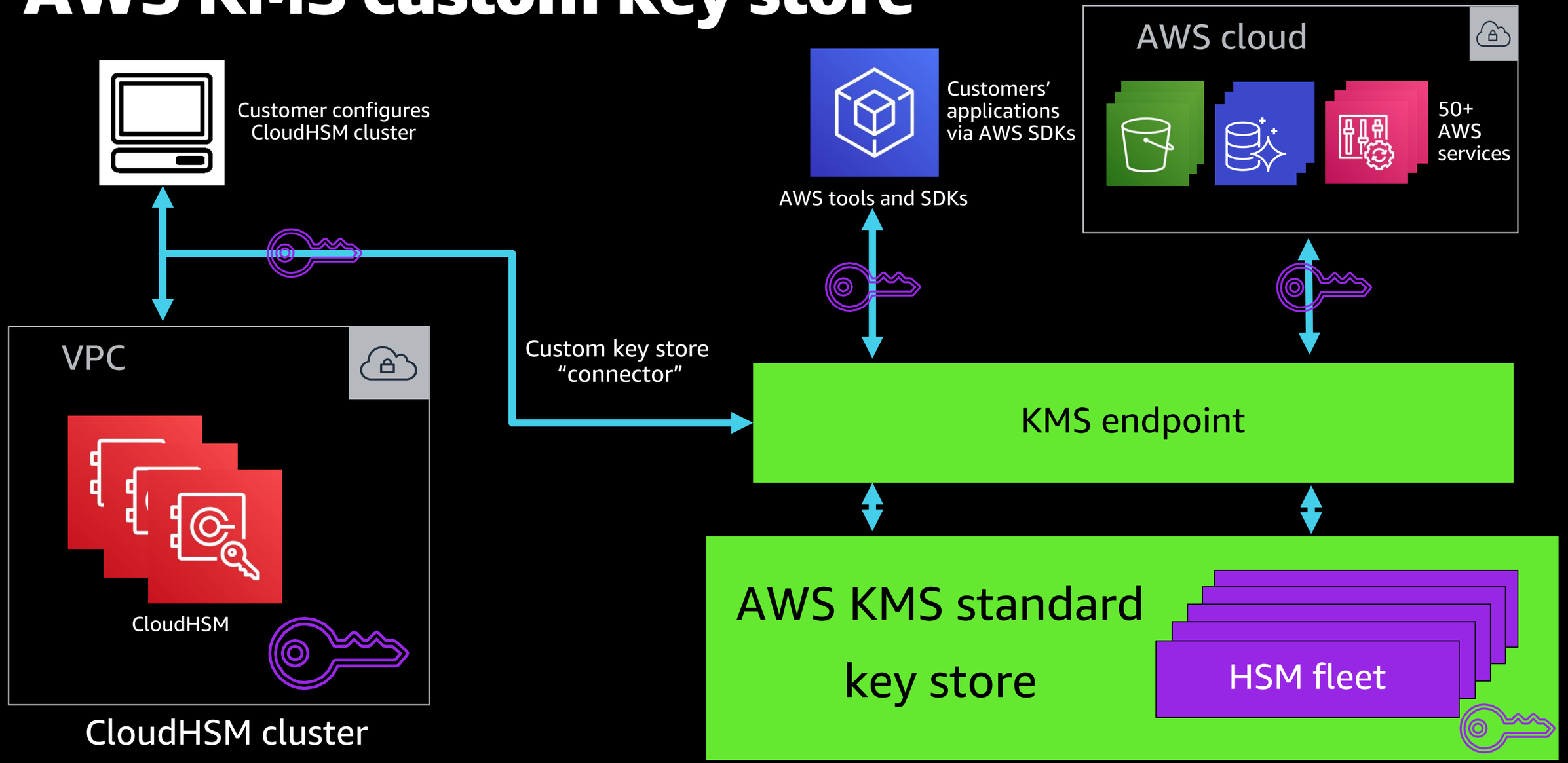
	AWS KMS	KMS custom key store (CloudHSM)
Where keys are generated	HSMs controlled by AWS	HSMs controlled by you
Where keys are stored	HSMs controlled by AWS	HSMs controlled by you
Where keys are used	HSMs controlled by AWS	HSMs controlled by you
How to control key use	JSON key policies you define	JSON key policies you define
Responsibility for performance / scale	AWS	You
Integration with AWS services?	Yes	Yes
Pricing model	$1/key + usage	$1/key + usage; hourly charge for each HSM

So what is AWS KMS custom key store?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS KMS custom key store

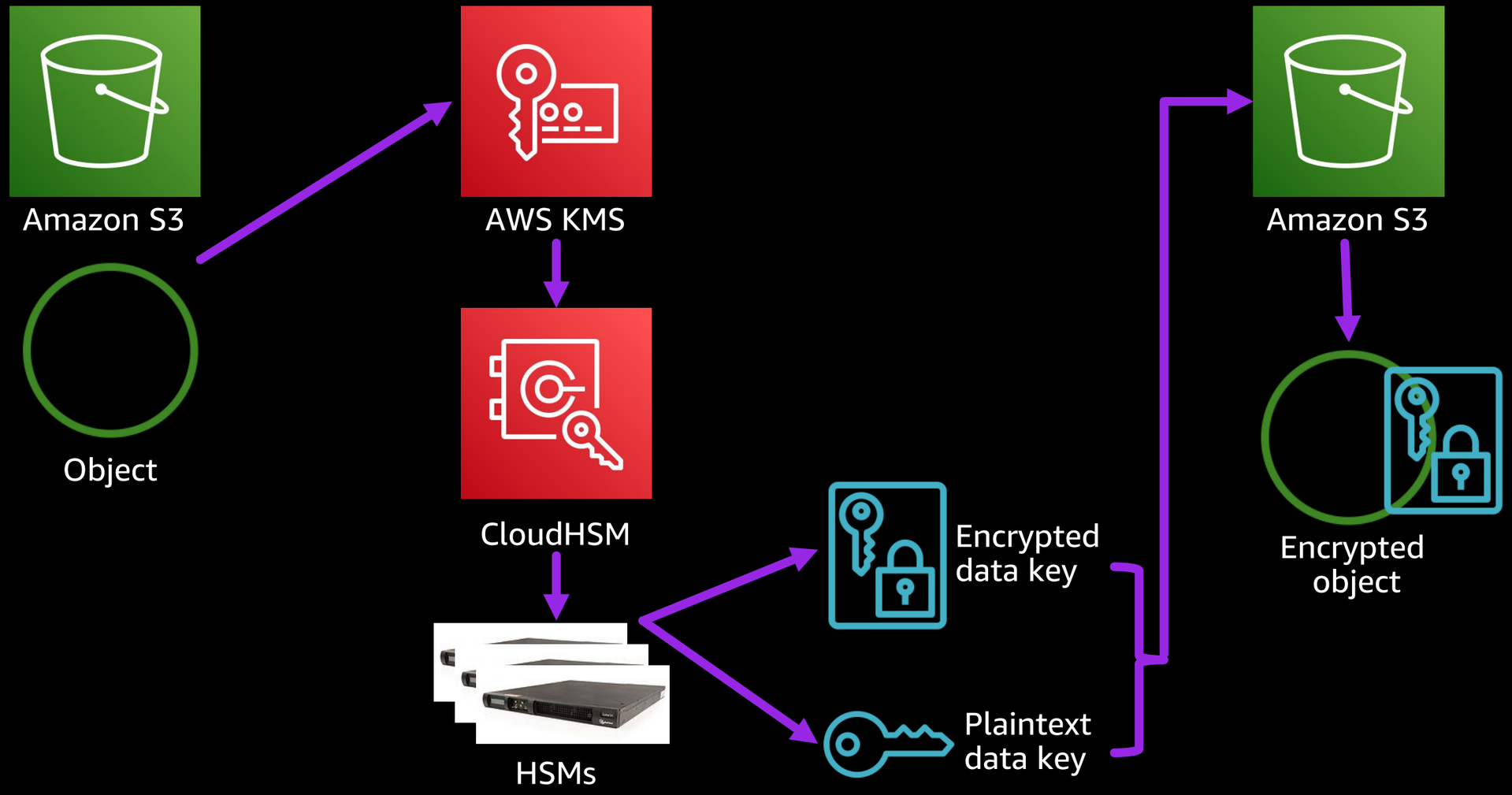


How does this thing work?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encrypting an Amazon Simple Storage Service (Amazon S3) object using SSE-KMS



Wait, do you *REALLY* need it?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Ask yourself these questions:

- Do you have compliance or regulatory requirements for FIPS 140-2 Level 3?
- Why *won't* AWS KMS work?
- Do you really want to pay that much money?
- Did you just succumb to "oh shiny" object syndrome?
- Do you really want to manage HSMs?
- Wouldn't you just rather let AWS handle all the hard stuff?
- Do you really want that cookie?



“You have *BRAINS* in your *HEAD*. You have *FEET* in your *SHOES*. You can *STEER YOURSELF* any direction you choose.”

Dr. Seuss

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.