
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC336

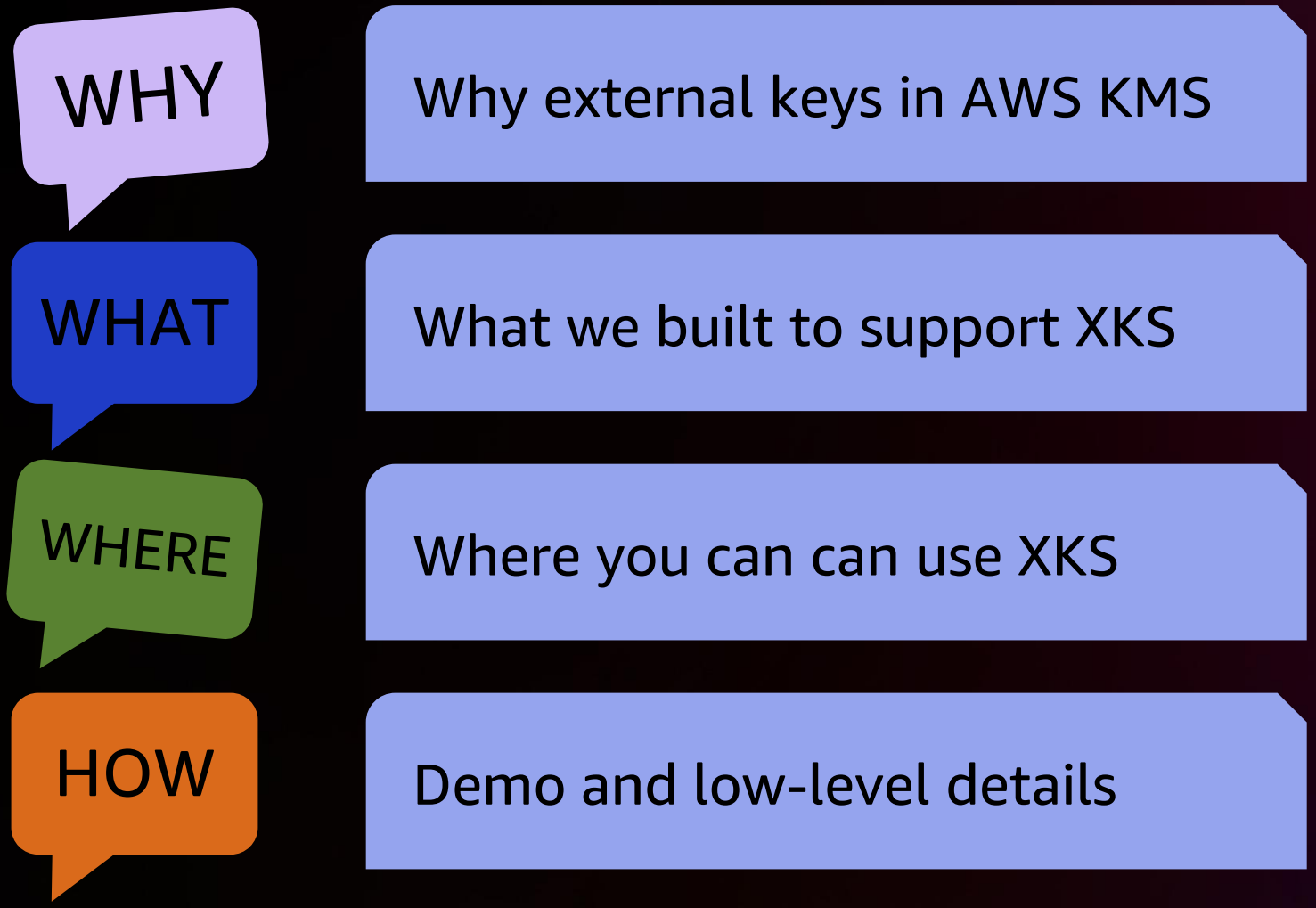
# Introducing AWS KMS external keys

Jeremy Stieglitz (he/him)
Principal Product Manager, KMS

Vipul Gupta (he/him)
Principal Engineer, KMS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS KMS external key store (XKS) launch




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# XKS executive summary

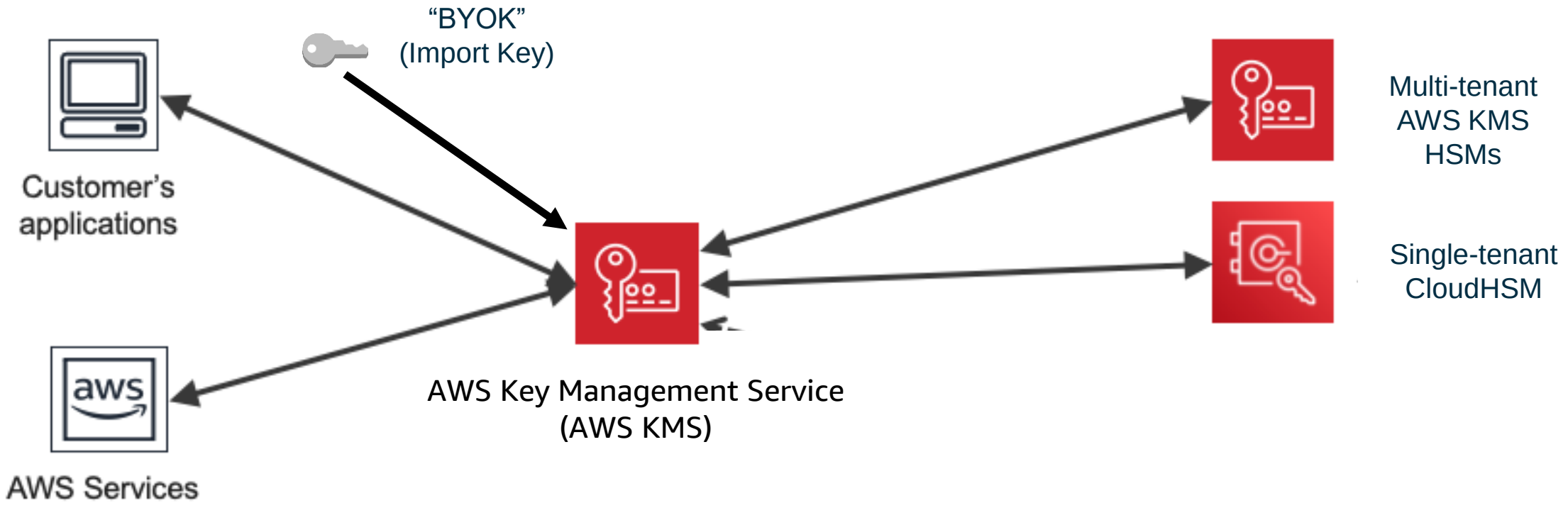
WHY

- *For customers who want to protect their data with encryption keys stored outside of the AWS Cloud*

- Extends existing AWS KMS custom key store feature beyond AWS CloudHSM (customer controlled, single-tenant HSM inside AWS datacenters) to keys in on-premises HSM

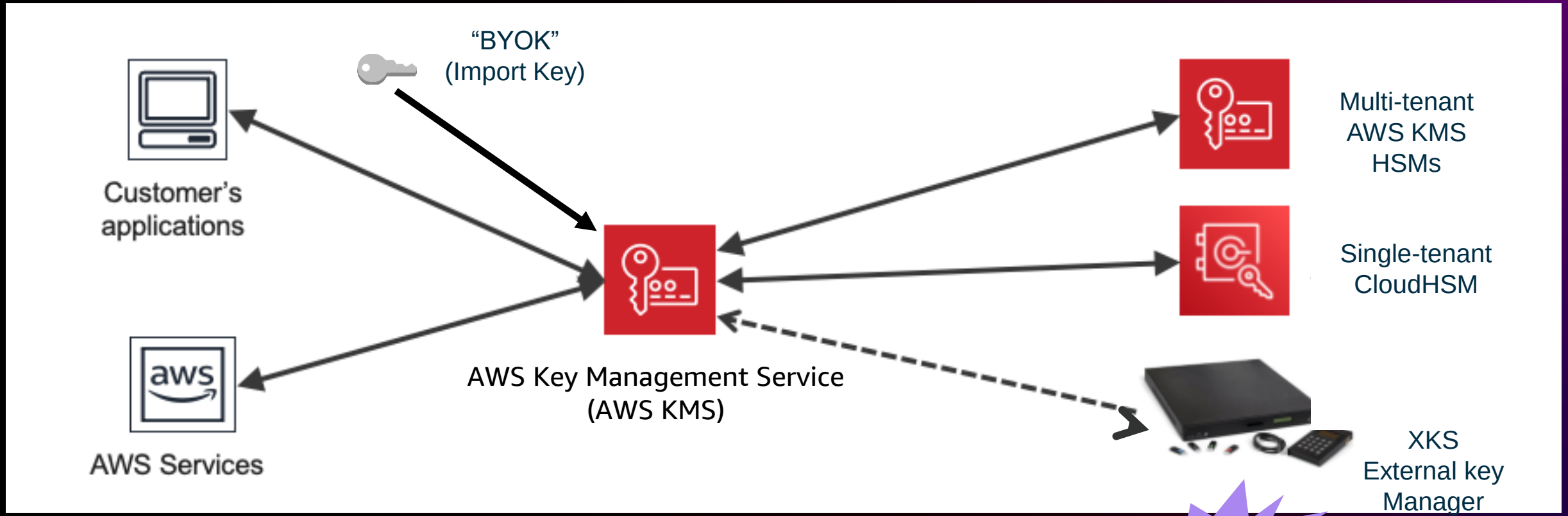
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Top-level design: AWS KMS today




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Top level design: AWS KMS new XKS option




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Technical highlights

- Full removal of root of trust from AWS KMS
  - All key material operated from customer's external key manager
  - External visibility and control over every key request
- Transparent to AWS services and client apps
- Flexibility on which keys you choose to store in external key manager
- No AWS KMS lifecycle management of keys kept in customer's HSMs {customer owns create, rotate, replicate, delete external keys}
- Serves as "kill switch": Turn off XKS & AWS data becomes unreadable

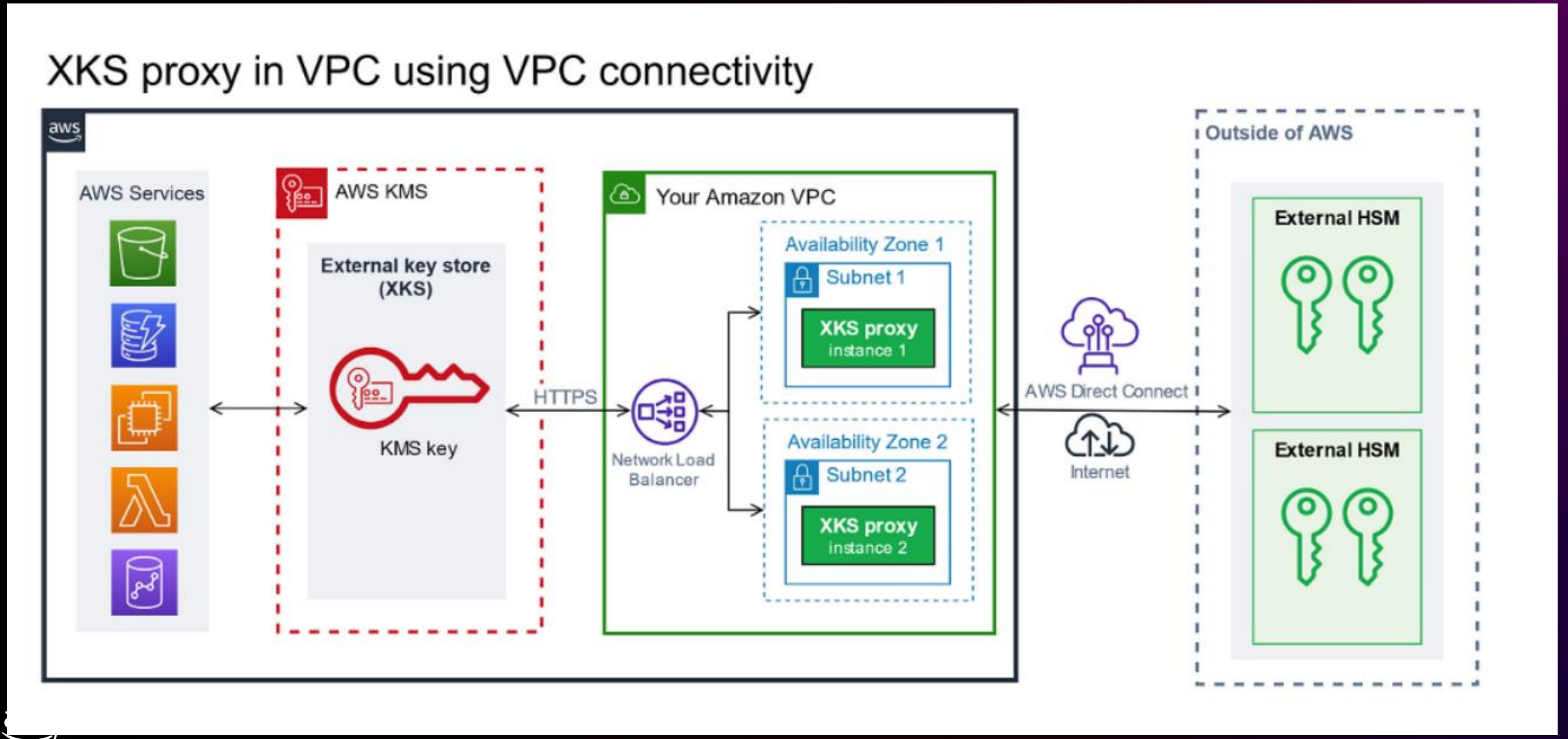
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Terminology

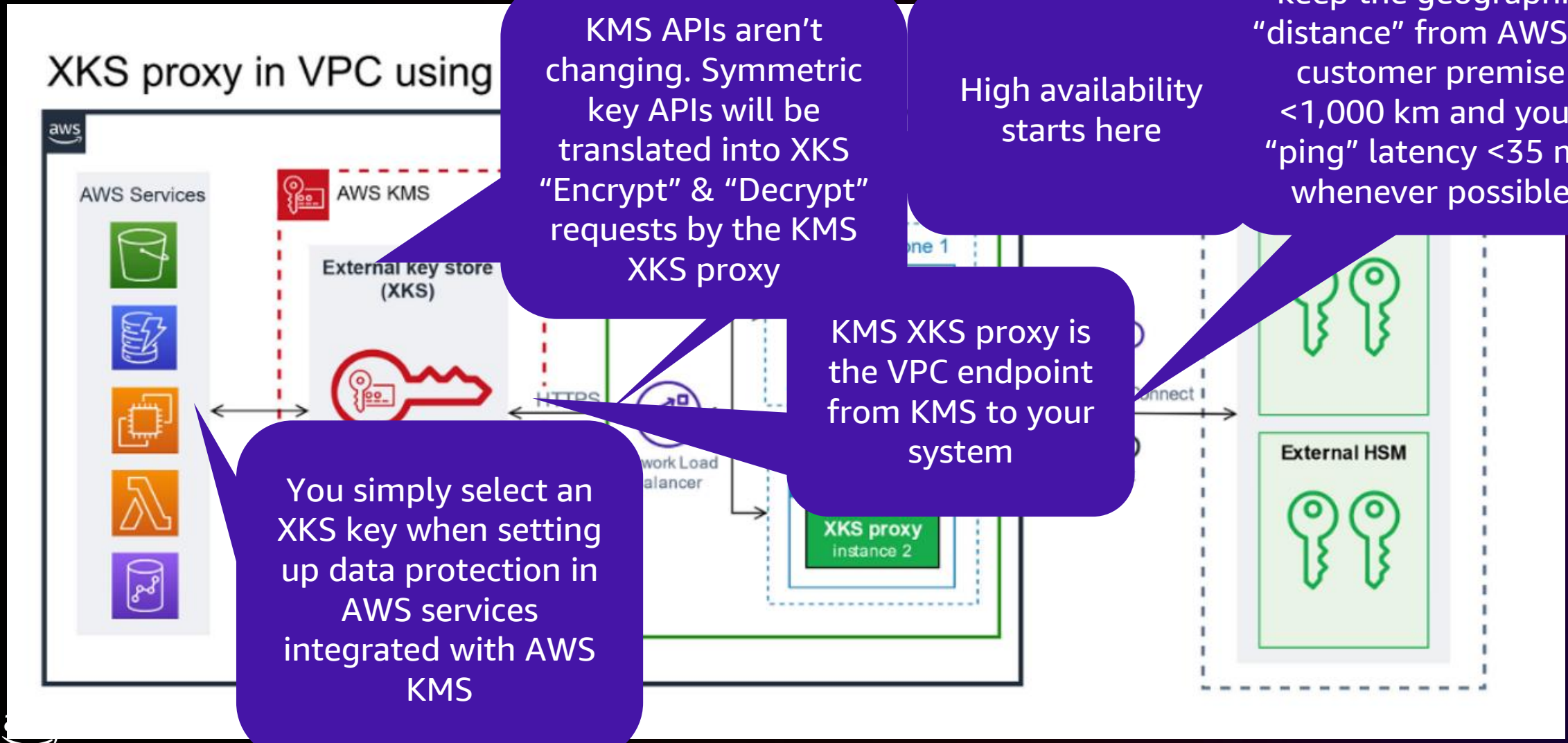
- **Custom Key Store**: logical construct within AWS KMS allows you to replace KMS HSMs with requests to an external key manager outside AWS KMS
    - **External Key Store (XKS)**: custom key store backed by an external key manager
    - **AWS CloudHSM key store**: custom key store backed by AWS CloudHSM
- **External Key Manager**: a hardware security module (HSM) or virtual HSM or any other key management system capable of generating keys and performing cryptographic operations. Supporting vendors such as Thales, Entrust, Atos, HashiCorp and Fortanix are developing XKS products
- **XKS proxy**: architectural component responsible for connecting and communicating AWS KMS requests to external key managers.

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# XKS detailed view



# XKS detailed view



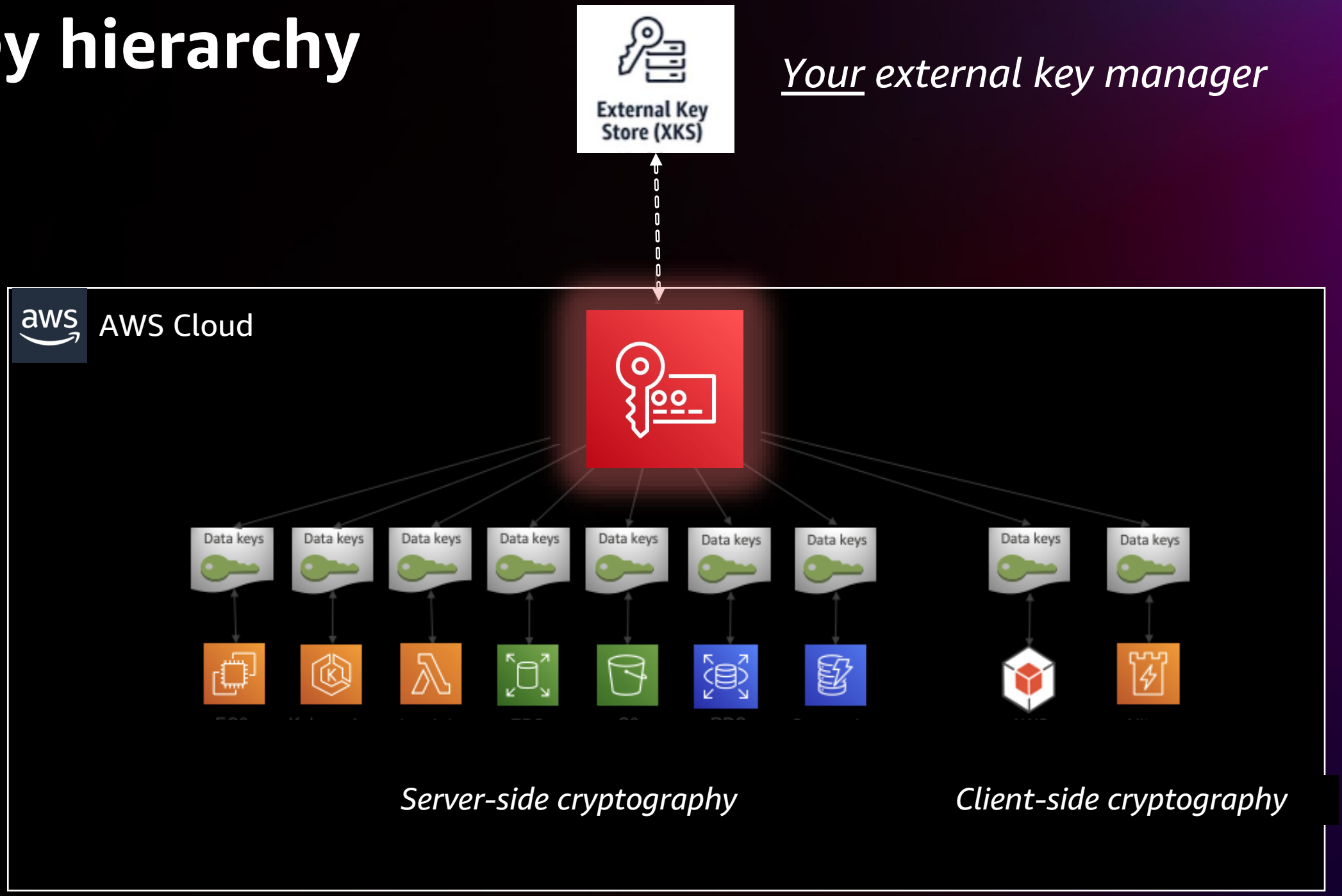
# XKS proxy APIs

| XKS API | Description | Calling KMS APIs |
|---|---|---|
| GetKeyMetadata | Gets metadata for a key in an external key manager | CreateKey |
| Encrypt | Encrypts input using a symmetric AES key in an external key manager | Encrypt, ReEncrypt, GenerateDataKey, GenerateDataKeyWithoutPlaintext |
| Decrypt | Decrypts input using a symmetric AES key in an external key manager | Decrypt, ReEncrypt |
| GetHealthStatus | Gets the health status of the external key manager | Can be called periodically as a part of the ConnectCustomKeyStore API |

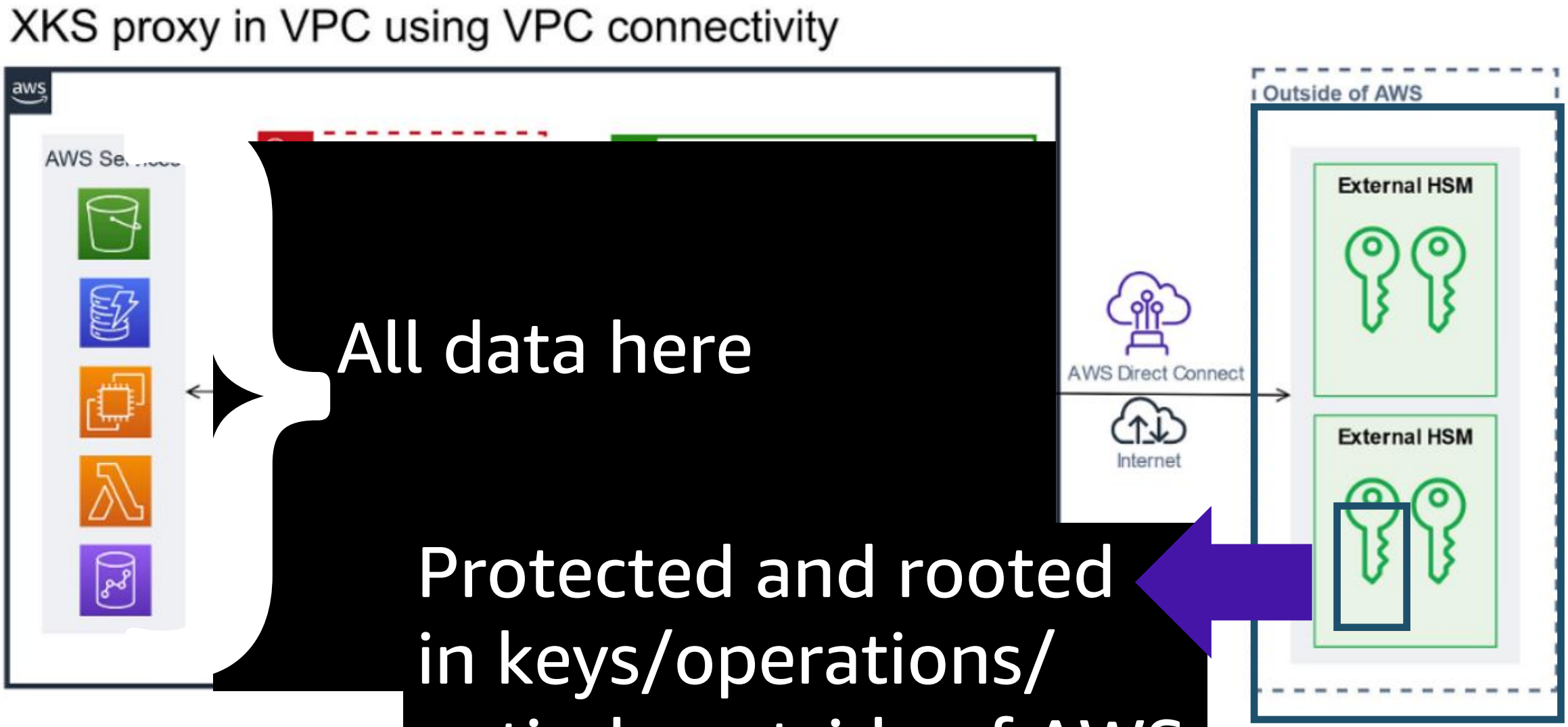
- Keys in external key stores *support all AWS KMS APIs supported by keys in AWS CloudHSM custom key stores.* No support for asymmetric operations, multi-Region keys, or automatic rotation at launch.
- Supported AWS KMS APIs map to just four APIs for the XKS Proxy.
- AWS KMS HSMs still used to generate key material for data keys.

aws
Amazon Proprietary

# Key hierarchy



# The need for XKS double enveloping



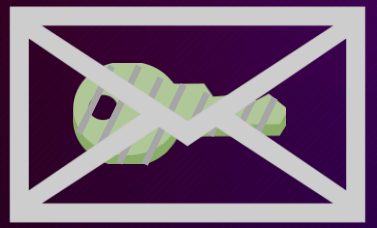

© 2022, Amazon Web Services, Inc. or its affiliates. A

# XKS double encryption of data keys workflow

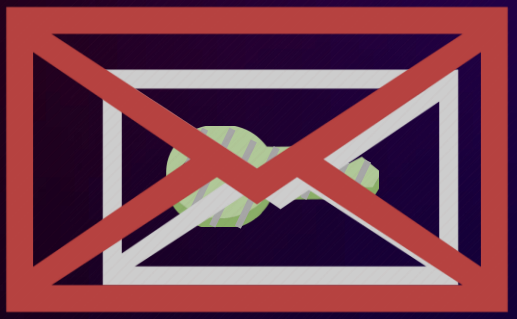
1. AWS KMS generates a new data key



2. AWS KMS creates key envelope (Using AWS KMS-owned keys)



3. Customer creates outside envelope (Using XKS keys in customer's external key manager)



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# XKS vs. standard AWS KMS keys

## What stays the same

- AWS KMS APIs for symmetric encryption identical. Not even changing ARNs for XKS
- Customer-controlled permissions to use AWS KMS keys, CloudTrail logging, and CloudWatch metrics
- Same pricing as other AWS KMS keys and API operations

## New with XKS

- Customer OWNS availability, durability, performance, and latency boundaries of key operations
- Additional customer controlled authorization, auditing, monitoring at the XKS Proxy and external key manager layer
- Operating and licensing costs for external key manager system

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

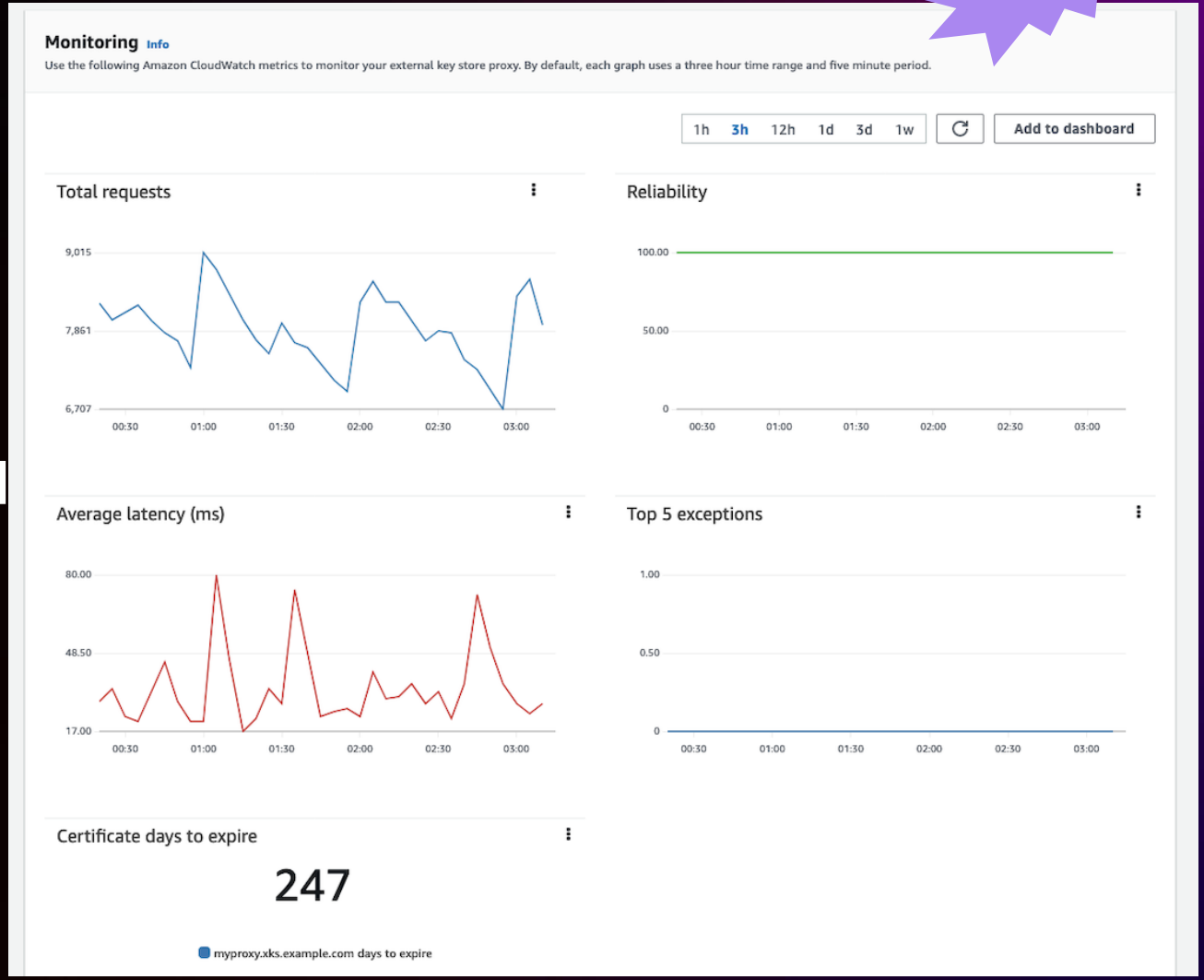
# Monitoring console

- Keeping your external key manager available, performant, and with low latencies will be critical to successful AWS KMS operations using external keys

- Monitoring
  - total requests
  - availability (of proxy)
  - latency (roundtrip from KMS)
  - top errors
  - days to proxy cert expiration

- Use CloudWatch to setup customizable alarms on these metrics

New




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Vendor support for AWS KMS XKS






















- We have also published the XKS spec & XKS test client to Github project page:

  https://github.com/aws/aws-kms-xksproxy-api-spec




aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Authentication of XKS proxy communications

- AWS KMS signs all requests to the XKS proxy using AWS SigV4 credentials that you configure on your proxy and provide to AWS KMS
- AWS KMS authenticates your external key store proxy using server-side TLS certificates
- Optionally, your proxy can enable mutual TLS for additional assurance that it only accepts requests from AWS KMS

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

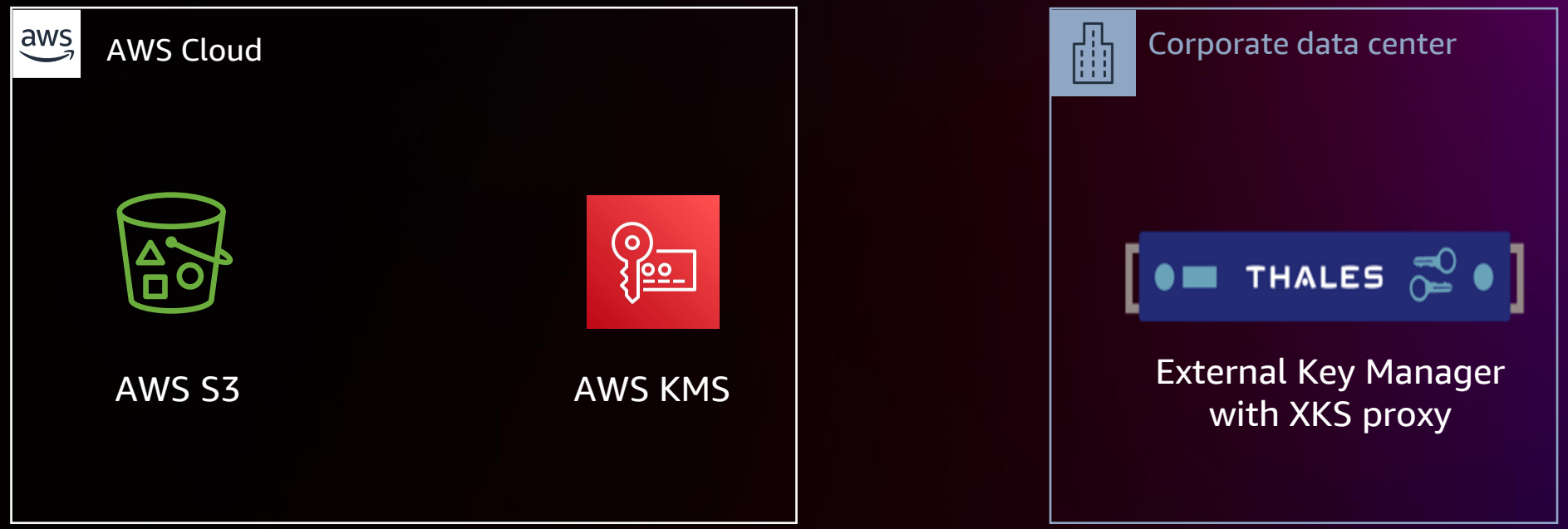
# Secondary authorization (optional)

- Uses standard WS KMS authorization in IAM and AWS KMS resource policies.
- In addition, XKS Proxy can implement secondary layer of authorization based on condition keys included in XKS Proxy API requests

```
"requestMetadata": {
    "awsPrincipalArn": "arn:aws:iam::123456789012:user/Alice",
    "kmsKeyArn": "arn:aws:kms:us-east-2:123456789012:/key/1234abcd-12ab-34cd-56ef
    "kmsOperation": "Encrypt",
    "kmsRequestId": "4112f4d6-db54-4af4-ae30-c55a22a8dfae",
    "kmsViaService": "ebs"
},
```

# Demo Time!

External key Id:
38fcb860-c81c-47ee-b703-872aa829e3a7

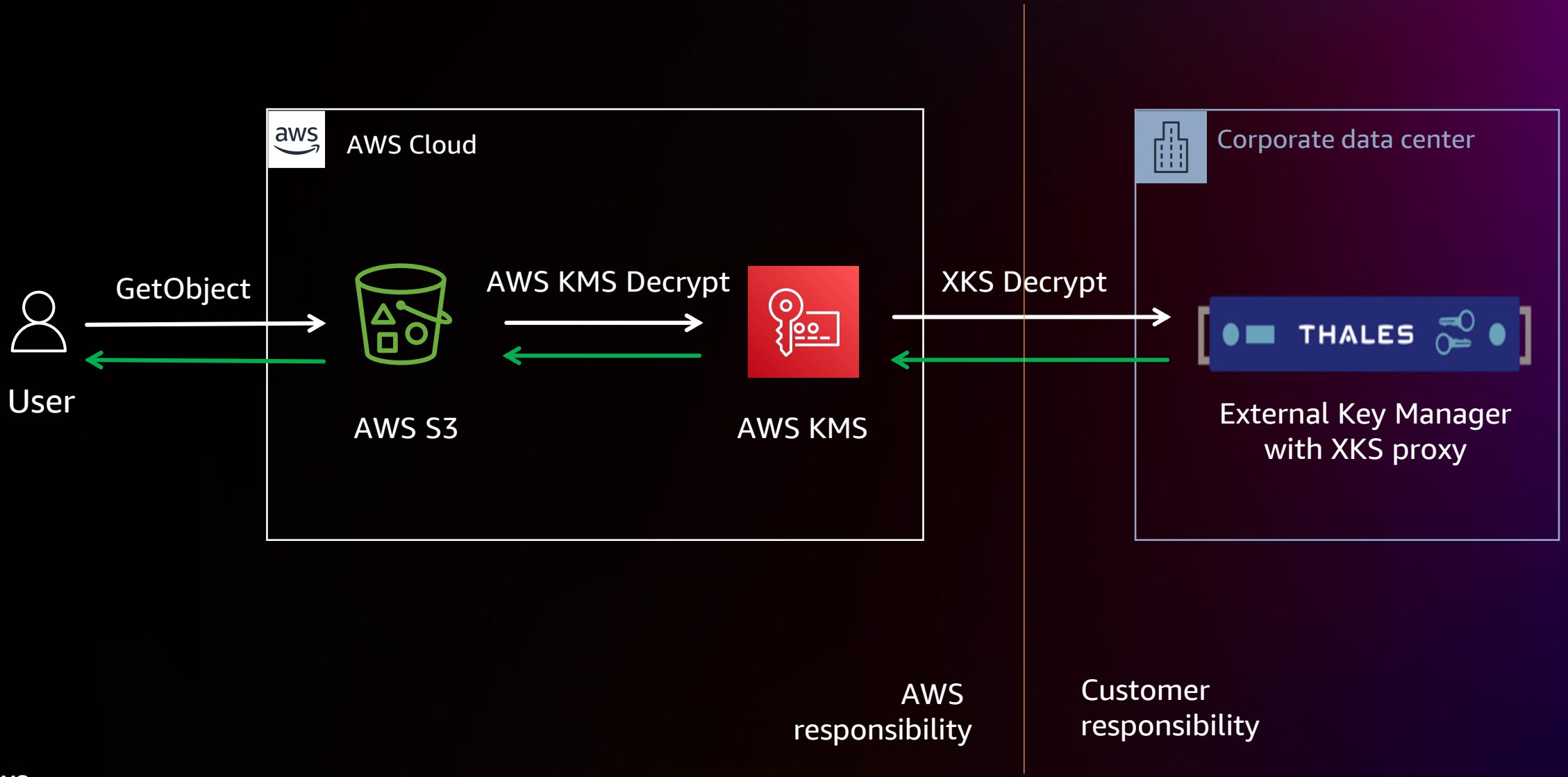



Bucket:
reinvent2022-xks-demo
Object:
AWS-whats-new-xks.png

KMS key Id:
f68a156c-dbb8-4623-b579-3434da7edea0
Origin:
External key store

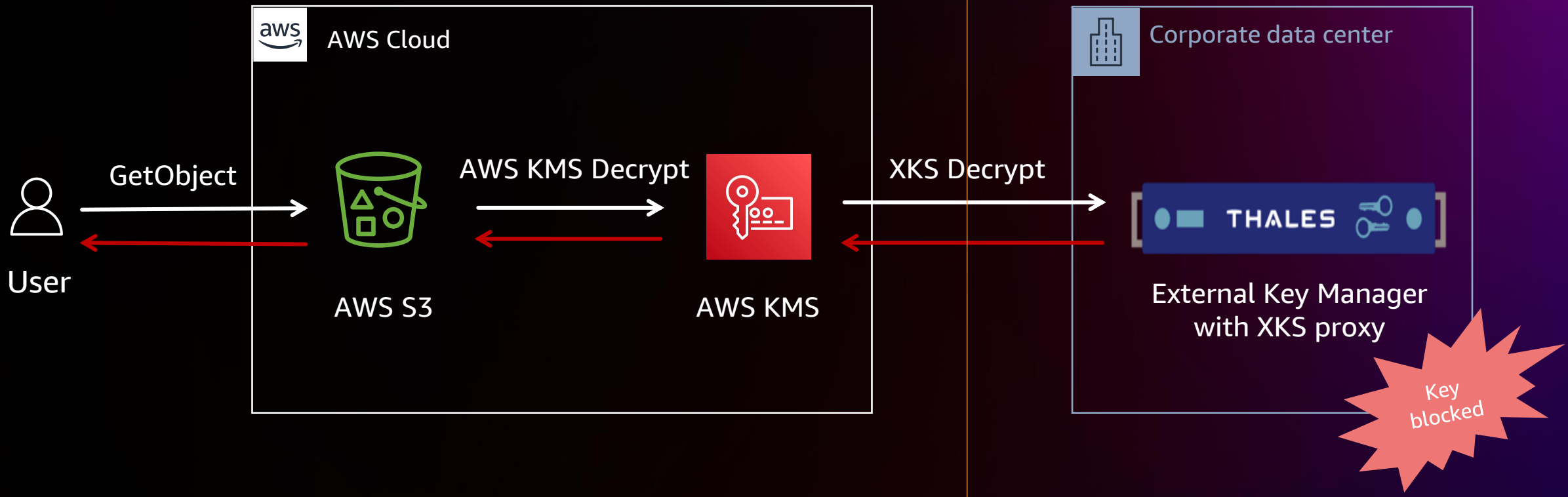
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Request Flow (Successful)




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Request Flow (Unsuccessful)




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3 Management Console — Mozilla Firefox

CipherTrust Manager | CipherTrust Manager | CipherTrust Manager | S3 Management Console

https://s3.console.aws.amazon.com/s3/buckets?region=us-east-1&region=us-east-1

aws | Services | Search [Alt+S] | Global | pheshmati @ lmartins

Amazon S3 > Buckets

## Account snapshot

Last updated: Nov 21, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more

View Storage Lens dashboard

| Total storage | Object count | Average object size |
|---|---|---|
| 306.9 GB | 2.9 M | 111.3 KB |

You can enable advanced metrics in the "default-account-dashboard" configuration.

## Buckets (14) Info

Buckets are containers for data stored in S3. Learn more

Copy ARN | Empty | Delete | Create bucket

Find buckets by name

1

| Name | AWS Region | Access | Creation date |
|---|---|---|---|
| cckm-cloudtrail-logs | US East (Ohio) us-east-2 | Bucket and objects not public | October 5, 2020, 14:03:27 (UTC-07:00) |
| cckm-files | US East (Ohio) us-east-2 | Bucket and objects not public | October 6, 2020, 11:57:48 (UTC-07:00) |
| cckm-xks-demo | US East (N. Virginia) us-east-1 | Bucket and objects not public | November 15, 2022, 14:59:01 (UTC-08:00) |
| cckm-xks-test | US East (N. Virginia) us-east-1 | Bucket and objects not public | October 21, 2022, 10:50:20 (UTC-07:00) |
| cckm-xks-test2 | US East (N. Virginia) us-east-1 | Objects can be public | November 3, 2022, 12:53:01 (UTC-07:00) |
| elasticbeanstalk-us-east-1-136846862618 | US East (N. Virginia) us-east-1 | Objects can be public | February 19, 2015, 19:29:20 (UTC-08:00) |
| gtocloudtraillogs | US East (N. Virginia) us-east-1 | Objects can be public | December 19, 2016, 14:06:38 (UTC-08:00) |
| hotlink-4542cc1e-7713-11e3-9888-005056b92ea0 | US East (N. Virginia) us-east-1 | Objects can be public | January 7, 2014, 11:25:15 (UTC-08:00) |


© 2022, Amazon Web Services, Inc. or its affiliates.

# Data key “caching” realities

- In some cases, such as Amazon EBS volumes, DynamoDB table key caching, Amazon SQS, and Amazon S3 bucket keys, a service may be able to continue working with protected data for a while without making a decrypt call to AWS KMS
- For such data, disconnecting the external HSM will not result in immediate cessation of data access; the kill-switch effect will be delayed until the AWS KMS key is needed again

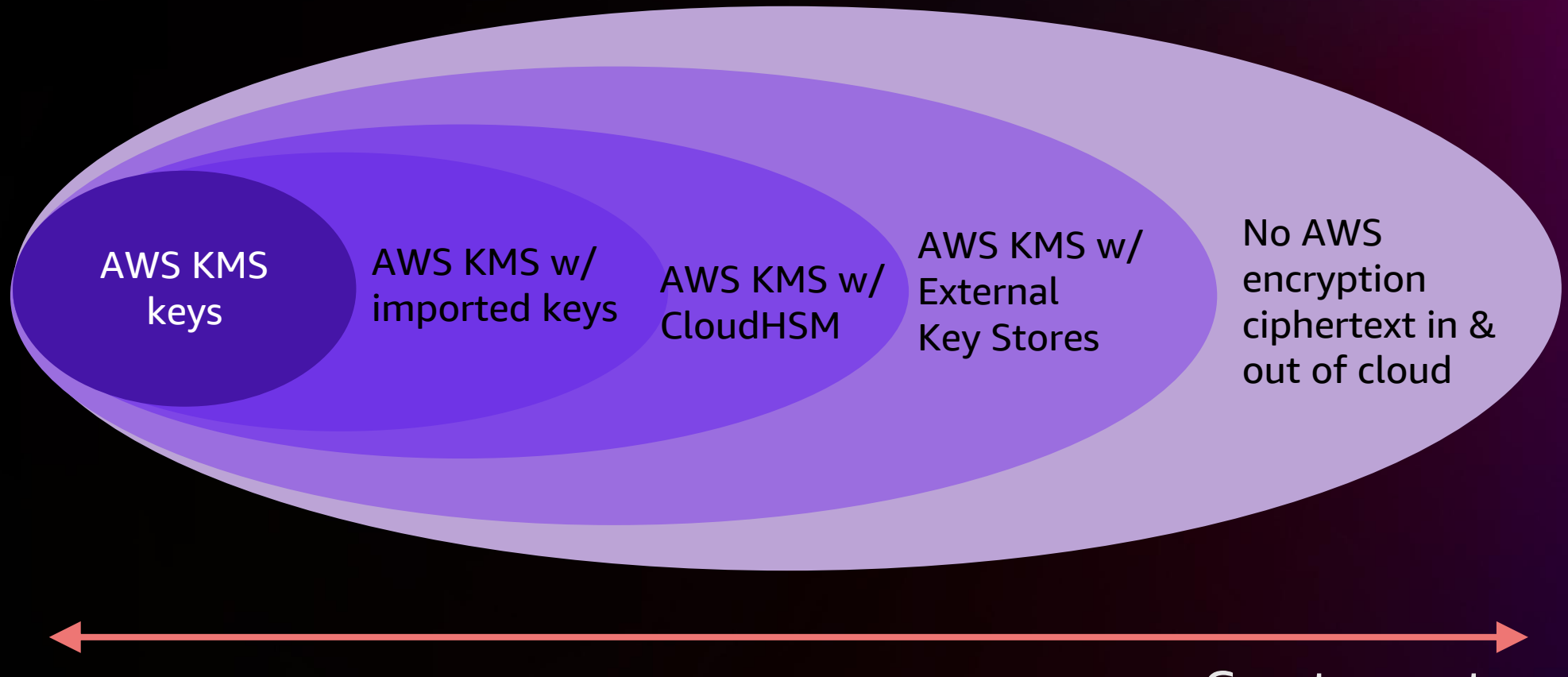
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# XKS and AWS Service Level Agreements

- The entire scope of the external key manager is outside the technical and operational control of AWS
- Therefore, the availability of external key managers, of all KMS operations on external keys, and of all AWS services that rely on external keys, are also outside the scope of AWS Service Level Agreements
- In fact, the use of external key stores is specifically excluded from the AWS KMS Service Level Agreement (SLA)

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# External key store (XKS) positioning




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# No, really, why?

- XKS may look attractive for several use cases, but we recommend that you scope your requirements for external keys around:
    - You have strict regulatory workloads that mandate possession of keys in key management systems outside the AWS Cloud
    - You've exhausted all paths to using standard AWS KMS where AWS generates and stores the keys for you
    - The regulatory need for XKS will ebb and flow over time as geopolitical agreements between countries change
    - You should limit external keys to the least amount of data required by your regulators

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Additional resources (how do I kick the tires?)

- XKS Developer Guide details
  https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html
- Network-to-Amazon VPC connectivity options
  https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/network-to-amazon-vpc-connectivity-options.html
- Connect Your Data Center to AWS (with AWS Direct Connect)
  https://aws.amazon.com/getting-started/hands-on/connect-data-center-to-aws/
- Create a service powered by AWS PrivateLink
  - https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

Jeremy Stieglitz
@jstieglitz



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.