AWS re:Invent

SEC340-R

Using AWS KMS for data protection, access control, and audit

Raj Copparapu
Sr. Product Manager
AWS Key Management Service
Amazon Web Services

Peter M. O'Donnell
Sr. Security Specialist Solutions Architect
Strategic Accounts
Amazon Web Services

AWS re:Invent

aws

Agenda

Quick encryption primer

AWS KMS overview

AWS KMS protecting your data

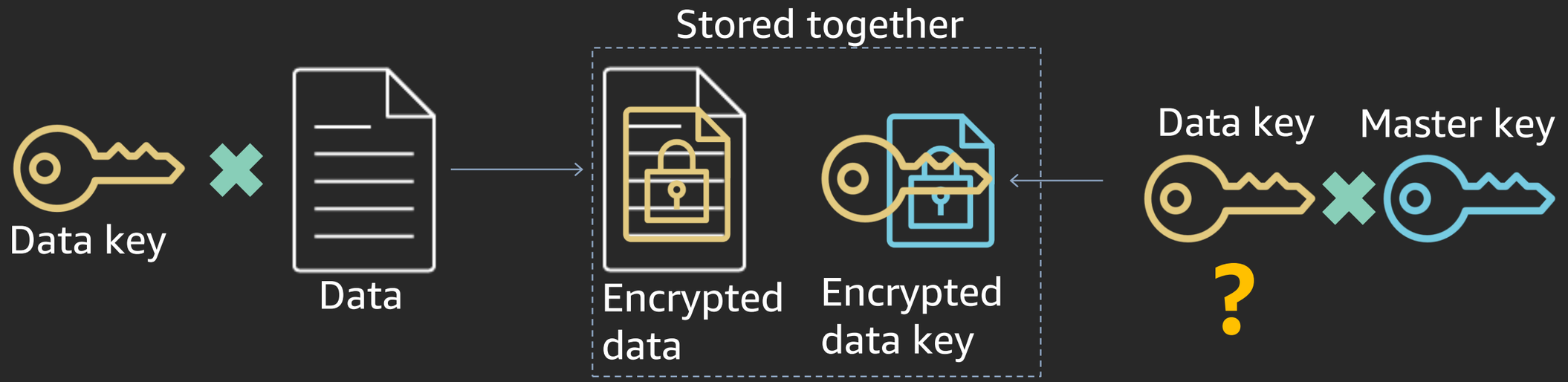
AWS KMS improving audit outcomes

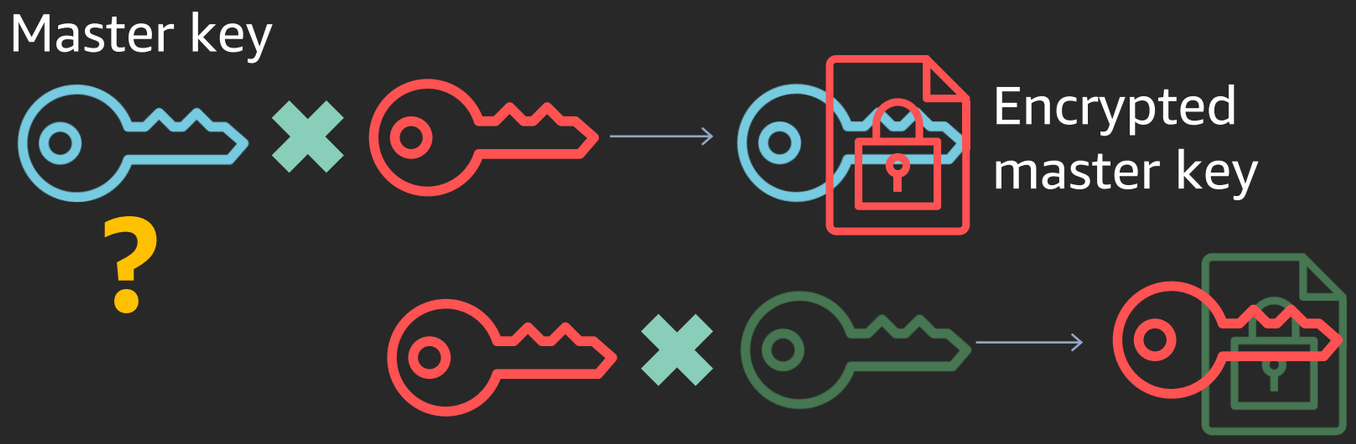
AWS KMS providing operational assurance

New asymmetric capabilities

Encryption primer & AWS KMS overview

Encryption primer





AWS KMS key hierarchy

Stored together

Encrypted data

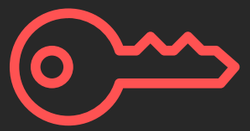
Encrypted data key

Data encryption key

Held by AWS KMS, managed by you

Customer master key (CMK)
Key policy enforcement

Held and managed by AWS KMS



Domain key

Region key

What else can AWS KMS do besides key management?

- AWS KMS gives customers an additional mechanism for access control and data protection

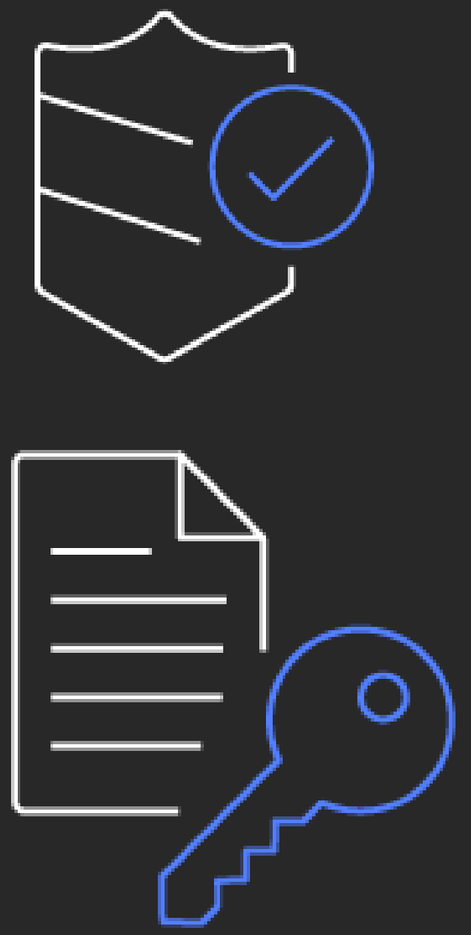
- AWS KMS integration with AWS services provides customers with a robust set of audit records for data events

- AWS KMS enables operational assurance to answer critical questions from stakeholders

AWS KMS protects your data

AWS KMS helps to protect your data

- Customers use separate customer master keys (CMKs) to partition access to data
- CMK key policy defines access
- CMK authorization ought to separate key administrators from encryption key users
- Improves the intentionality and discretion of data access



AWS KMS is an additional plane of access control

- Resources protected by AWS KMS require additional authorization
- Even with Amazon S3 full access, accessing objects backed by SSE-KMS requires authorization to use the AWS KMS CMK
- Customers with teams managing sensitive data on Amazon EBS use separate CMKs with discrete authorization
- Amazon RDS separation of duties – separate access to instances and snapshots from access to secrets and credentials

AWS KMS improves audit outcomes

AWS KMS integration with AWS for audit outcomes

- AWS KMS “encryption context” can be used to correlate events in AWS CloudTrail
- Detective controls & an audit record prove access and ensure non-repudiation
- Use AWS Config to track changes to CMK policy

Amazon S3 data trail

- Must be enabled by bucket or account
- Records object-level access – GETs & PUTs
- Includes the ARN of the user
- Can be ticked & tied against AWS KMS records in CloudTrail

- Answers critical questions:
- "Who accessed this data?"
- "Did accessing this data always require access to the encryption key?"
- "Was everything stored here always properly encrypted?"

AWS KMS provides operational assurance

AWS KMS provides operational assurance

- What if someone opens an Amazon S3 bucket to the world?
- What if someone shares an Amazon EBS snapshot?
- How can I definitively prove who has access?
- How can I definitively prove who does not have access?

Default encryption and robust integrations

- Enable default bucket encryption for Amazon S3 using AWS KMS
- Configure Amazon EBS for default volume encryption using AWS KMS
- Amazon DynamoDB is always encrypted with AWS KMS
- AWS KMS protects TLS certificates with AWS Certificate Manager and Elastic Load Balancing

For the next 20 mins….

New feature in the service

Differences between existing and new key types

Use cases

What to expect from AWS KMS

Your share of responsibility

Asymmetric key support

Digital signature workflow

User creates a signing key

Generates a signature

User sends signature and data to recipient

Recipient verifies signature using public key

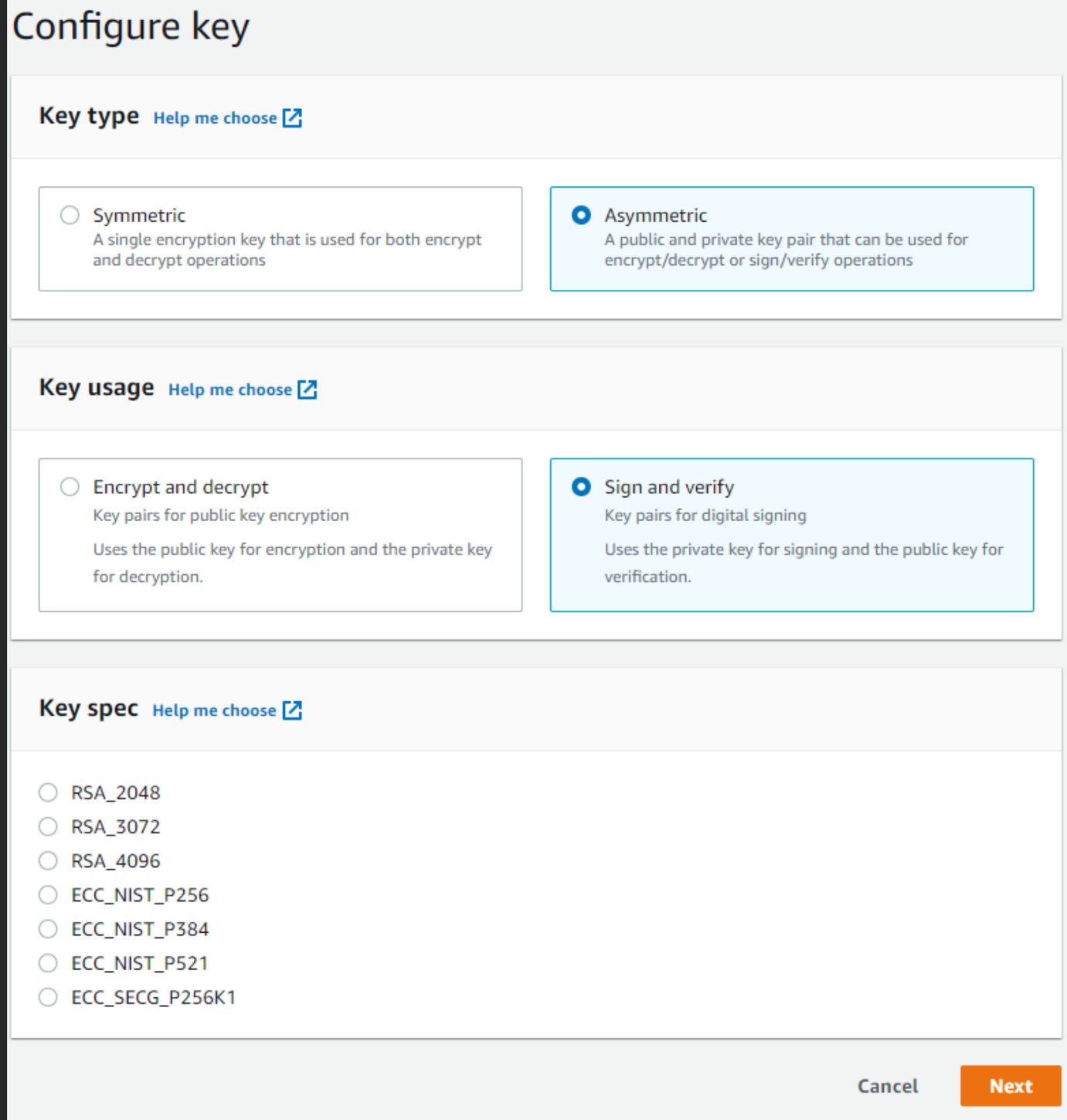
Signing in AWS KMS

RSA and ECC key specs

Sign API
- Message
- Message digest

GetPublicKey API

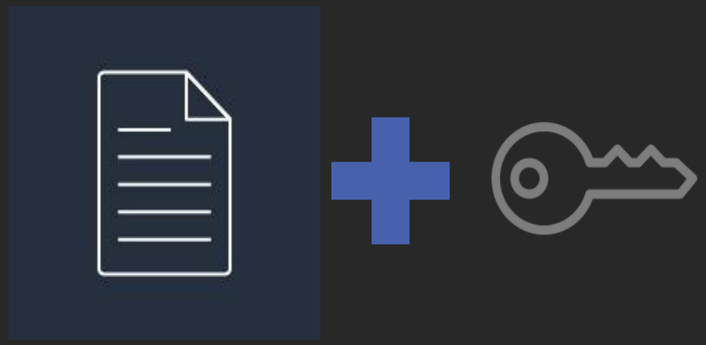
Verify API
- Audit Trail



Asymmetric encryption workflow

User creates an encryption key

Downloads public key



Recipient encrypts using public key and sends ciphertext

User decrypts using private key

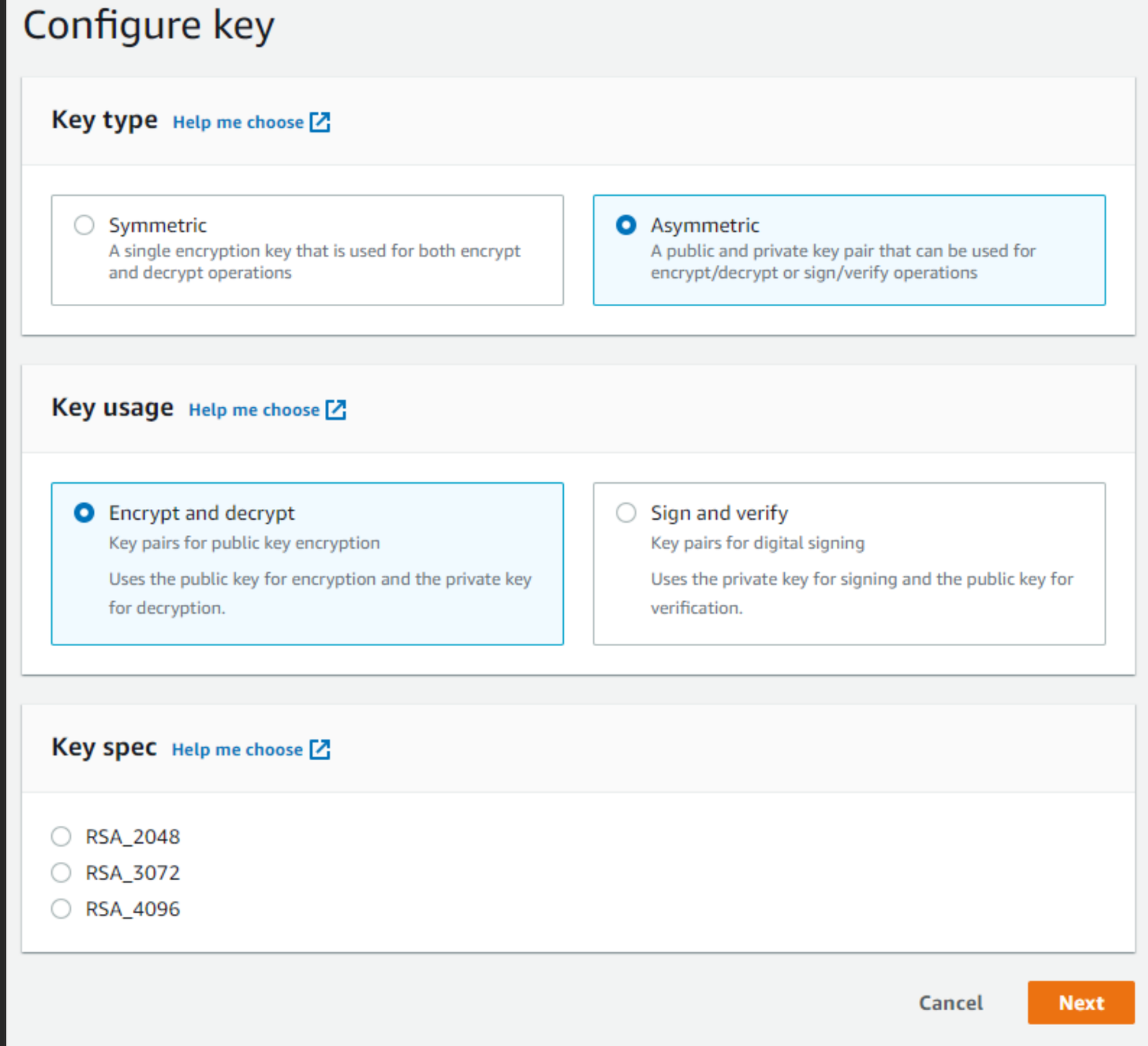
Encryption in AWS KMS

RSA key specs

GetPublicKey API

Decrypt API
- Key ID

Encrypt API
- Audit trail



GenerateDataKeyPair*

Ability to generate public-private key pairs

- As a Customer Master Key
- As a data key pair

Use the public and private portions for cryptographic operations

- Sign and verify
- Encrypt and decrypt

Asymmetric and symmetric differences

Asymmetric and symmetric differences

Key and key pairs

- Single key for encrypt and decrypt operations
- Public and private key pair for encrypt/decrypt or sign/verify operations

Operations inside and outside AWS KMS

- Symmetric key operations happen within the service
- Encryption and Verification operations can happen outside the service

Interoperability

- Ciphertext produced by symmetric keys has AWS KMS specific metadata
- Ciphertext and signatures follow specifications for interoperability

Integration

- No native integration with AWS services YET

Asymmetric use cases

Asymmetric use cases

Confidentiality

Enable third parties to perform unauthenticated encryption outside of AWS KMS using an RSA public key, but enforce authenticated decryption within AWS KMS using the private portion of the key

Integrity

Sign a binary, document, auth token (SAML or JWT), or files
Have third parties verify signatures

AWS KMS's responsibility

AWS KMS's responsibility

Generate keys in HSMs and protect within the service

As with symmetric keys, nobody, including AWS employees, can access plaintext private key material

All access and operations are recorded

Availability and durability still applies

AWS KMS will continue to scale to meet your needs

Your responsibility

Your responsibility

Use keys designated for signing and encryption accordingly

You must not use asymmetric keys in an integrated AWS service that lets you include a KMS *keyId*

Getting certificates for public keys

Setting right policies

Parting words

In Northern Virginia, Oregon, Sydney, Ireland, and Tokyo AWS Regions today (with others to come)

Different limits for asymmetric

GenerateDataKeypair* APIs can only be used with symmetric CMKs

Pricing is different from the current symmetric keys

- Asymmetric keys are excluded from the free tier

At AWS, security is the **top priority**

Resources

Blog Post

https://aws.amazon.com/blogs/security/digital-signing-asymmetric-keys-aws-kms/

Pricing

https://aws.amazon.com/kms/pricing/

Documentation

https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

Related breakouts

SEC322-R - Deep dive into AWS KMS

SEC337 - Toyota Motor North America: Securing the cloud with AWS KMS

SEC348-R - Protecting sensitive data in your AWS workloads (Builder!)

SEC401-R - Using the AWS Encryption SDK for multi-master key encryption (Workshop!)

WPS320-R - Implement access control to data in AWS services using AWS KMS (Builder!)

ENT401-R - A lifecycle approach to governance, compliance, and audit

SEC320-R - We all want the same things: Meeting controls objectives on AWS

STG301-R - Deep dive on Amazon S3 security and management

Learn security with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud security skills

30+ free digital courses cover topics related to cloud security, including Introduction to Amazon GuardDuty and Deep Dive on Container Security

Classroom offerings, like AWS Security Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

AWS re:Invent

aws

Please complete the session survey in the mobile app.