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

SEC212

AWS data protection: Using locks, keys, signatures, and certificates

Param Sharma (she/her)

Principal Software Engineer, PKI
AWS

Jeremy Stieglitz (he/him)

Principal Product Manager, KMS
AWS

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

Our grand tour

Young adults of the 17th and 18th century often spent 2–4 years touring around Europe in an effort to broaden their horizons in an experience known as the Grand Tour



We don’t have 4 years :) so we’ll be quick

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

Our Grand Tour

Our tour today will examine how we use keys, locks, digital certificates, and digital signatures at AWS

Along the way, we will touch on AWS KMS, AWS CloudHSM, AWS Certificate Manager (ACM), AWS Private CA, and AWS Signer



Keys



Locks



Certificates



Signatures



AWS Key Management Service (AWS KMS)



AWS CloudHSM



AWS Certificate Manager (ACM)



AWS Private Certificate Authority

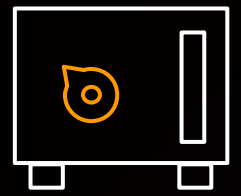


AWS Signer

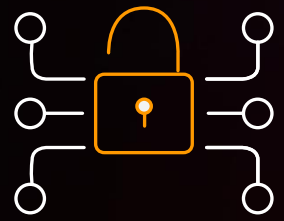
aws

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

Why use data protection on AWS?



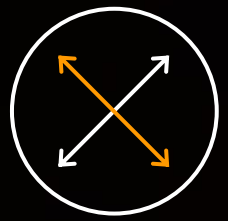
Protect intellectual property and trade secrets



Protect customer information and build a trusted brand



Automate tasks and improve agility



Visibility and control throughout your business growth



Ease of use – integration with hundreds of AWS services



Meet global security and compliance controls

aws

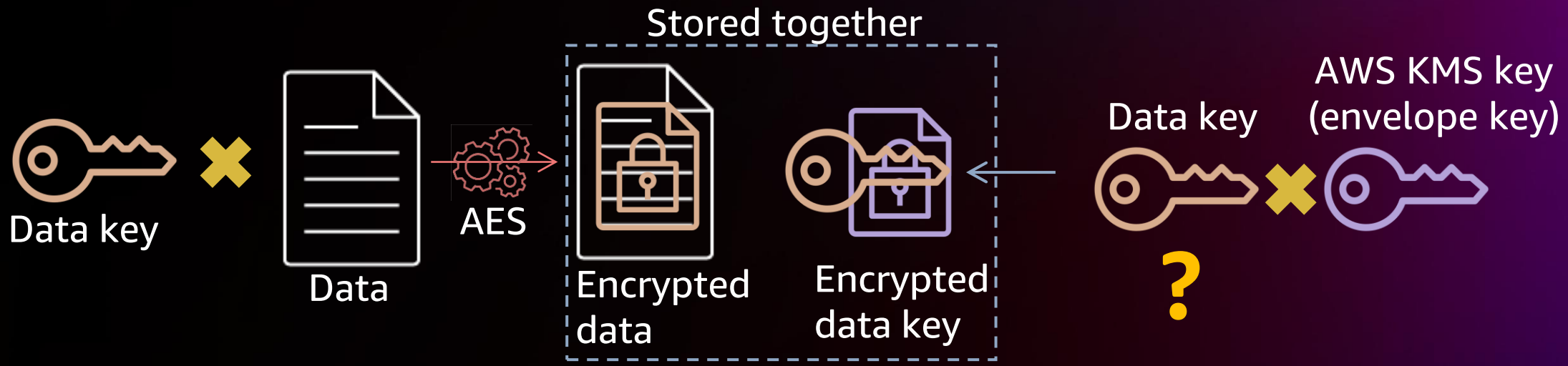
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

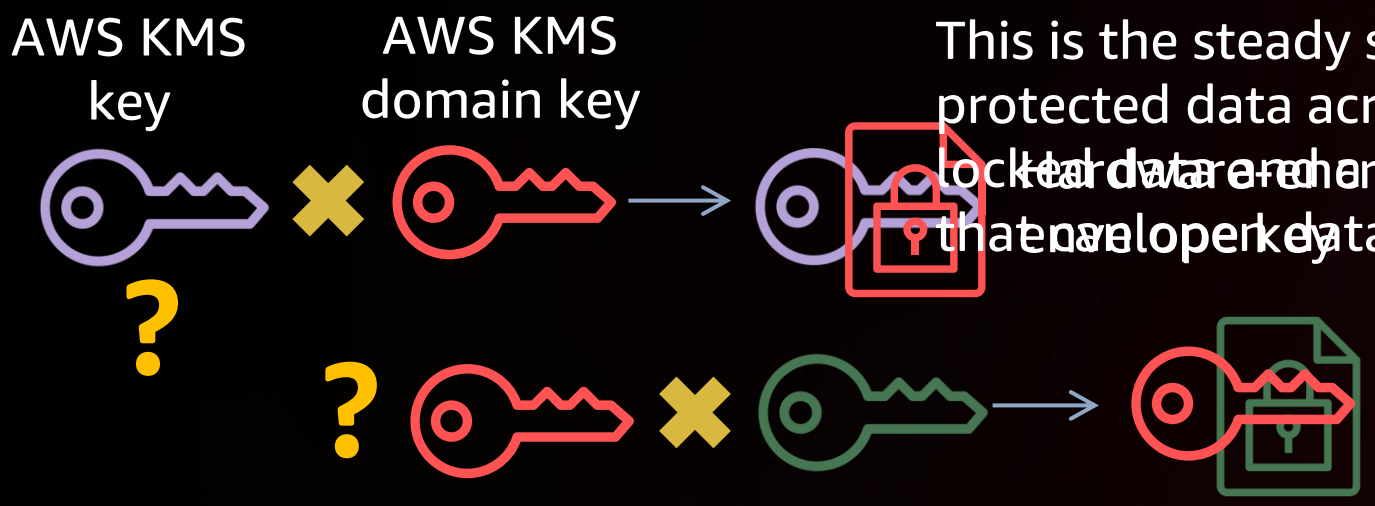
What is a lock

- Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.
  Source: https://csrc.nist.gov/glossary/term/encryption
- AWS primarily uses AES GCM with 256 Bits keys as our algorithm (cipher) of choice for locking data
- But how do I secure the keys? (Hint: We lock them)

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

Envelope encryption





This is the steady state of ALL protected data across AWS:

Locked data and locked key that envelope key

Locked data encrypted data next to it

This is the steady state of ALL AWS KMS keys: they remain encrypted and can only be opened inside the AWS KMS HSMs

AWS KMS
(root of trust)

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

What is AWS KMS?

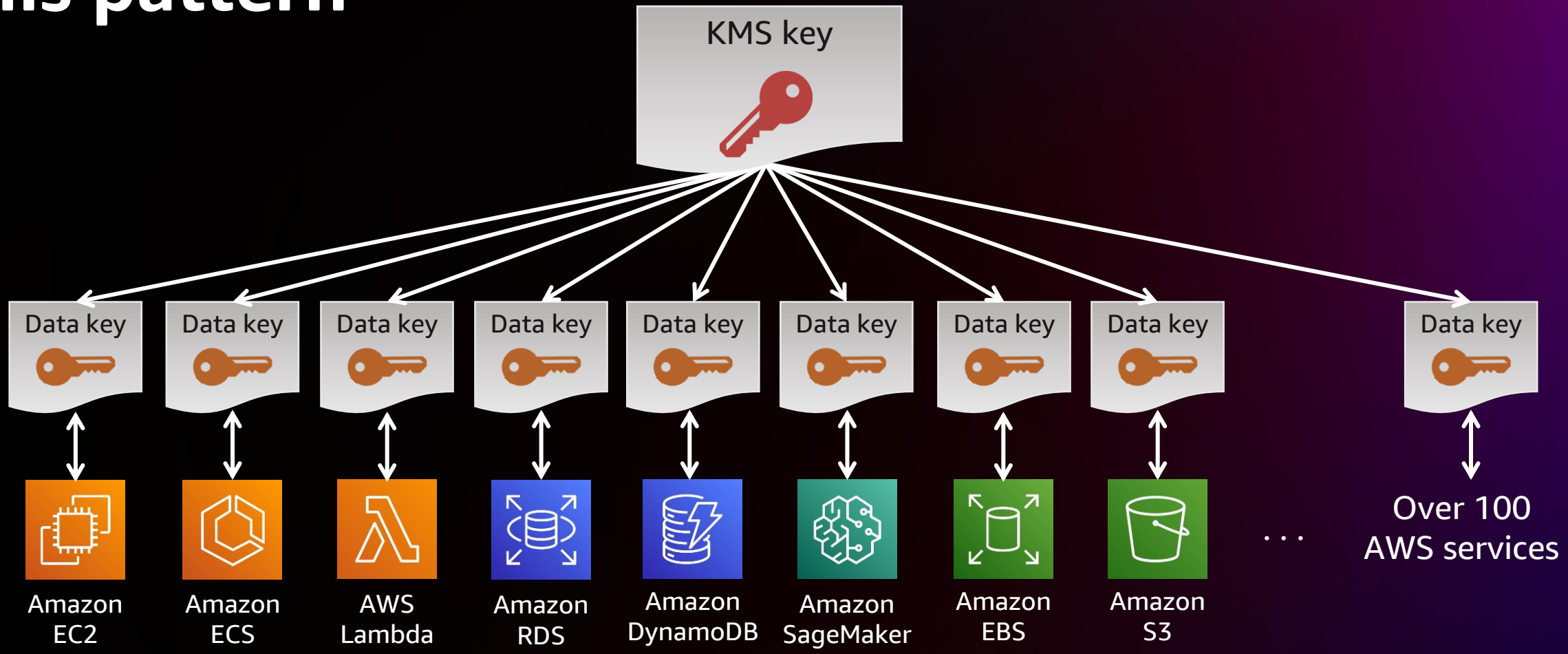


- AWS KMS lets you create, manage, and control cryptographic keys across your applications
- Scales to any workload (50,000 TPS) with low latency and 99.999% public SLA
- All sensitive key operations protected inside FIPS 140 certified fleet of HSMs
- AWS KMS is incorporated in over 100 AWS services to encrypt sensitive data and create digital signatures

aws

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

All AWS services with customer data support this pattern



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

Can AWS see my keys?

- **Keys never exist in plaintext outside the HSM**
- **When operational with keys provisioned**
  - No AWS operator can access the HSM (no human interfaces)
  - No software updates allowed (must tear down HSM to blank)
- **After reboot and in a non-operational state**
  - No key material on host
  - Software can only be updated after multiple AWS employees have reviewed the code
    - Under quorum of multiple AWS KMS operators with valid credentials
  - Third-party evidence
  - SOC 1 – Control 4.5: Customer master keys used for cryptographic operations in AWS KMS are logically secured so that no single AWS employee can gain access to the key material



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

How many keys will I need?

- Depends on goals and security policies (e.g., Is there preference for centralized or distributed?)
- Typically isolated by service (different keys for Lambda and EKS), isolated by project/tag/data classification, and must be isolated by Region
- We recommending tying keys to data owners. Key ownership most often belongs with your data owners (best person to determine access policies)
- Keys can be rotated yearly, but we recommend you skip rotation unless you are required to



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

Which KMS key type is right for me?

Customer-managed key

- You control the policy, you own the key
- AWS CloudTrail logging and Amazon CloudWatch alerts
- Support for multi-region keys

AWS-managed

- Hybrid option
- CloudTrail and CloudWatch
- Cannot access cross-accounts
- On deprecation path within AWS

AWS-owned

- Less headache, “it just works”
- No costs to you
- But no audit or changes to policies on key



$1 per key/month
Most flexibility

No costs but limited customer control & visibility

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

Controlling access to your AWS KMS key

- Key policies
  - Primary way to control access to your key
  - No principal, including the key creator, has any permission to the key unless explicitly allowed
- IAM policies
  - Optional
  - Control access to any AWS KMS operation
  - “Child policies” …cannot use IAM policies to allow access to a key, unless key policy explicitly allows it



AWS KMS key

aws

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

Enforce separation of duties for AWS KMS keys

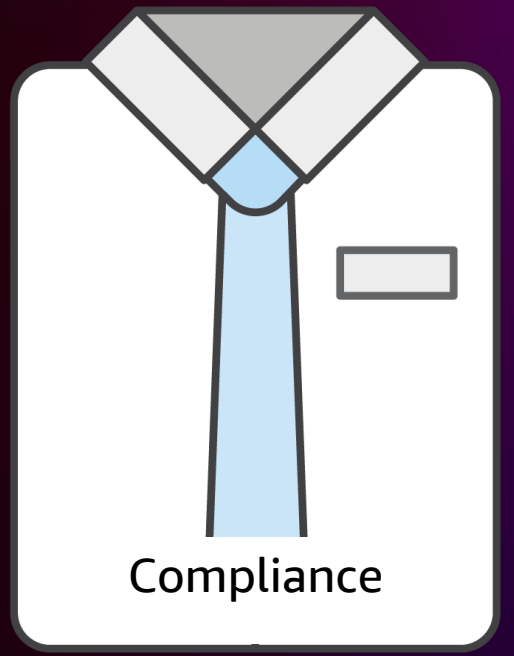
Use **IAM policy** and AWS KMS **key policy** to enable different personas to perform different key management tasks



Manages key access policies



Uses keys to protect data



Verifies configuration and historical access

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

More ways to build locks and keys… What is AWS CloudHSM?



- Standalone, dedicated HSM cluster that you own and operate in your VPC
- Extensive support for “lift and shift” on-premises HSM workloads
- Offers more specialized cryptographic algorithms and legacy ciphers than KMS
- Certified at FIPS 140-2 Security Level 3
- Can become the backend HSM for KMS using the KMS custom key store feature

aws

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

Part two: Certs and sigs





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

What are cryptographic signatures?

- Cryptographic signatures provide a way to ensure the integrity and authenticity of digital messages, objects, or files
- Two types:
  - **“Raw” signatures**
  - **Certificate-based signatures**





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

Certificate

- Allow web browsers to identify and establish encrypted network connections
- Used within a cryptographic system known as a public key infrastructure (PKI)

Cryptographic signature of original file







Certificate with information about signer, their public key, and signature of the certificate issuer

aws

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

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            11:dd:45:4d:db:0d:b5:2a:34:b0:4a:9e:c9:82:3e:f5
    Signature Algorithm: ecdsa-with-SHA512
        Issuer: 0.3.2.2.9.3=lgl/0.8.6.3.9.5=sbm/0.6.2.6.8=prl/0.6.7.8=tlqby/0.3.6.4=vhwn
        Validity
            Not Before: Nov 21 04:15:57 2022 GMT
            Not After : Nov 21 05:15:57 2023 GMT
        Subject: 0.3.2.2.9.3=lgl/0.8.6.3.9.5=sbm/0.6.2.6.8=prl/0.6.7.8=tlqby/0.3.6.4=vhwn
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:66:0c:6e:54:ba:2a:e1:5a:c9:c6:04:d5:e1:70:
                    e7:fa:33:a1:12:01:69:5d:f9:6f:79:3b:33:e7:c0:
                    ee:ea:d7:2c:d0:49:a3:70:e7:8d:1c:ff:fc:81:f9:
                    57:e6:e5:ff:ce:5a:fb:16:7c:d3:c1:15:d6:a1:7f:
                    39:00:fb:6c:30
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                FA:B4:7D:27:96:19:86:97:C1:B2:91:7F:90:75:26:D5:E0:DC:02:33
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: ecdsa-with-SHA512
         30:45:02:21:00:d8:50:ab:05:07:42:bf:0c:9b:06:90:4d:d9:
```

aws

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

What is the role of certificates?

Issue certificates to encrypt data in transit (TLS) + identify and authenticate endpoints



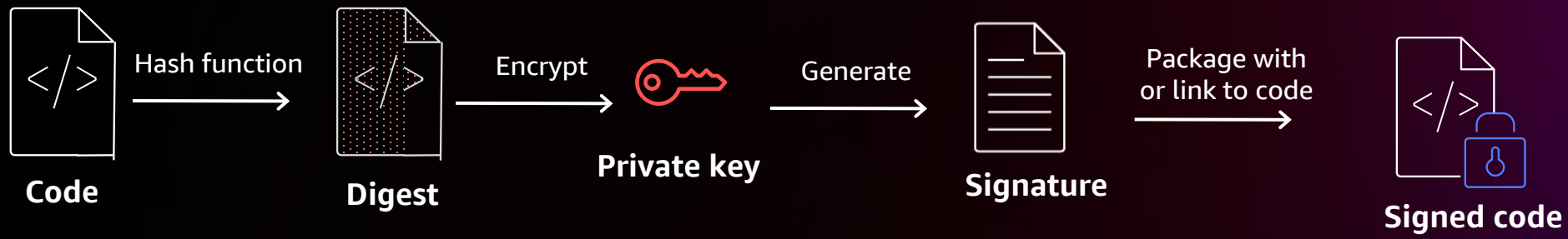
Certificates provide a unique digital identity to endpoints

aws

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

What is code signing?

Code signing is an industry-standard technique used to confirm that the code is unaltered and comes from an approved source



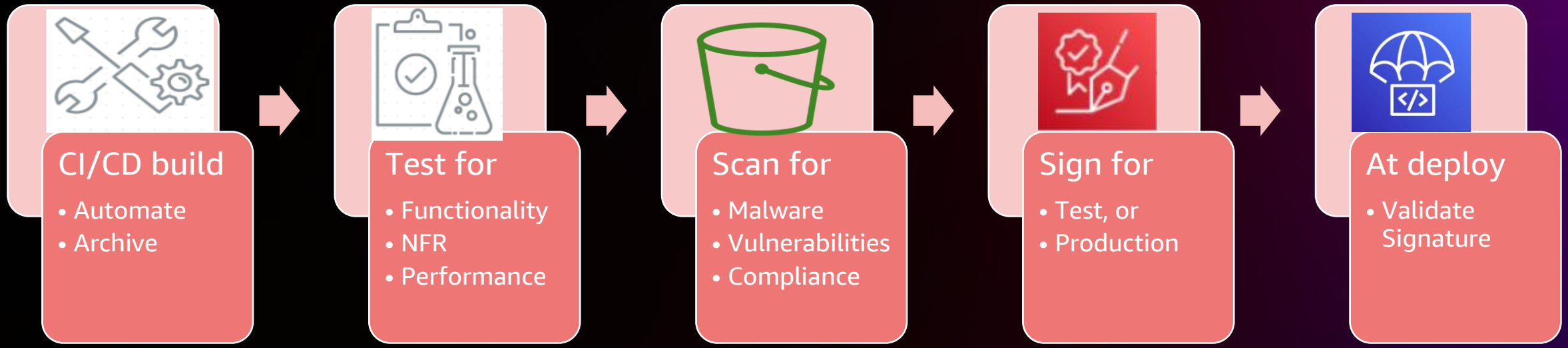
Recipient of signed code verifies hash using public key




```
If (decrypted hash  == hash of original code)
{
        // The code is correctly signed
}
```

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

Scan before you sign; validate before you deploy



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

AWS certificate services

AWS Certificate Manager (ACM)

Easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources

AWS Private Certificate Authority

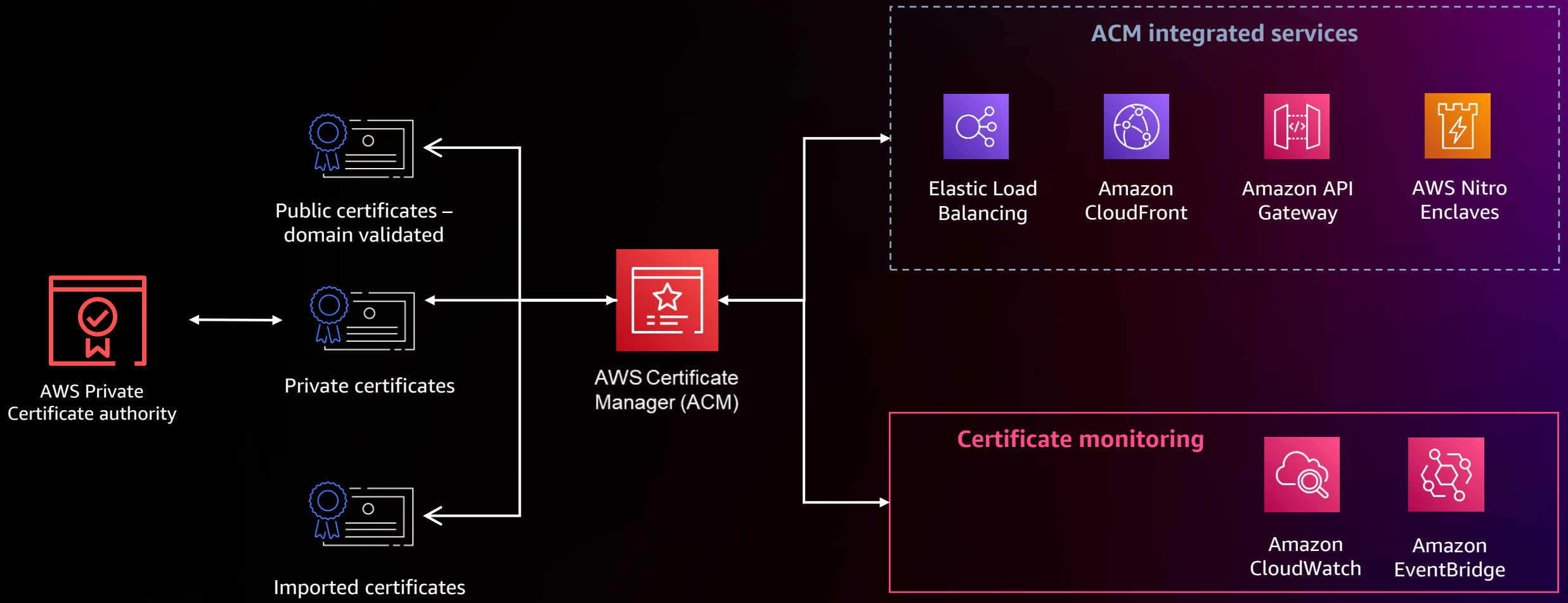
Highly available private certificate authority service without the upfront investment and ongoing maintenance costs of operating your own private CA

AWS Signer

Fully managed code-signing service to ensure the trust and integrity of your code

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

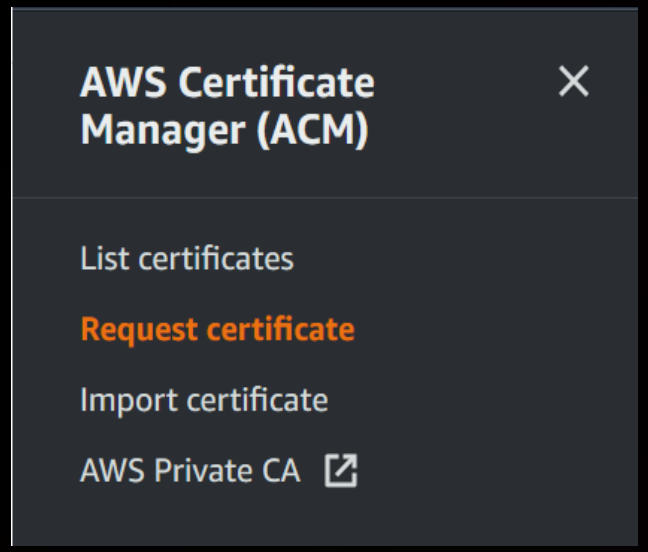
AWS Certificate Manager (ACM)

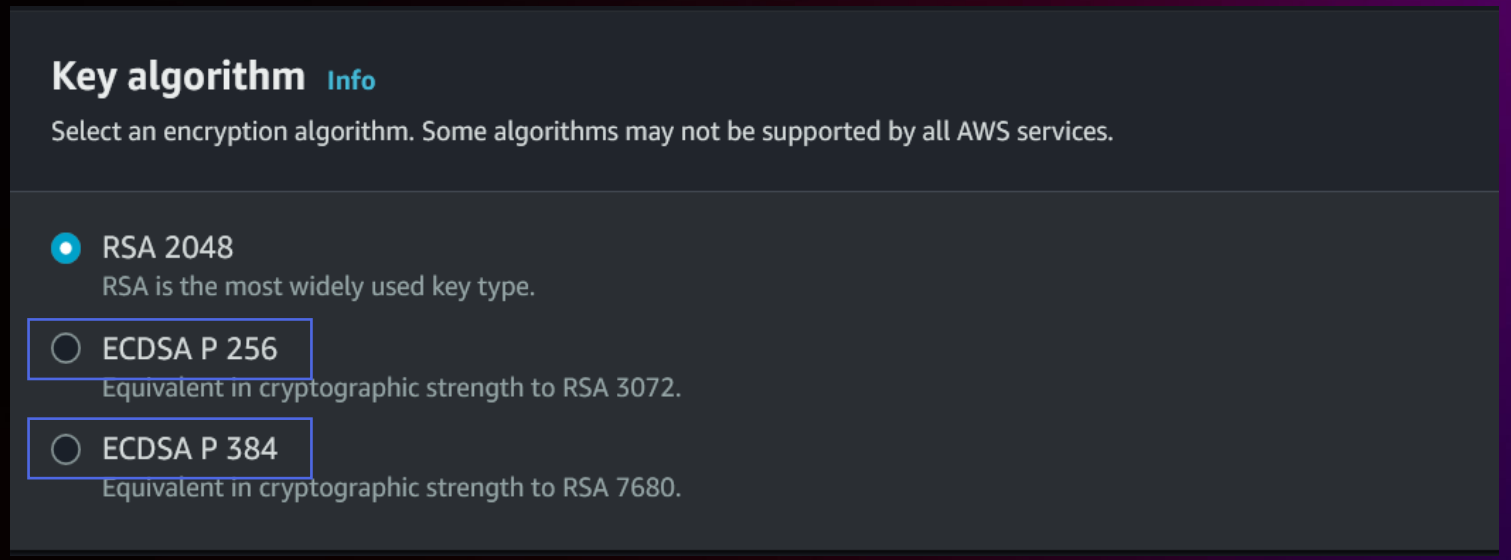


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ECDSA launch

- Nov 8, 2022 – Customers can issue ECDSA P 256 and P384 certificates from ACM





API / CLI

```
aws acm request-certificate \ --domain-name www.example.com \ --key-algorithm EC_Prime256v1 \
```

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

ACM – Best practices

- Do – Use DNS domain name validation for *public* certs
- Do - Use managed renewals and binding
- Do – Monitor expiry with Amazon CloudWatch / Amazon EventBridge
- DON'T – Use pinning. If you have to pin, pin to the root and not subordinates

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

What is AWS Private CA?



Secure and managed
private certificate authority



Root CA and complete
CA hierarchies



Enable developer agility



Flexibility to customize
private certificates



Manage certificate
authorities centrally

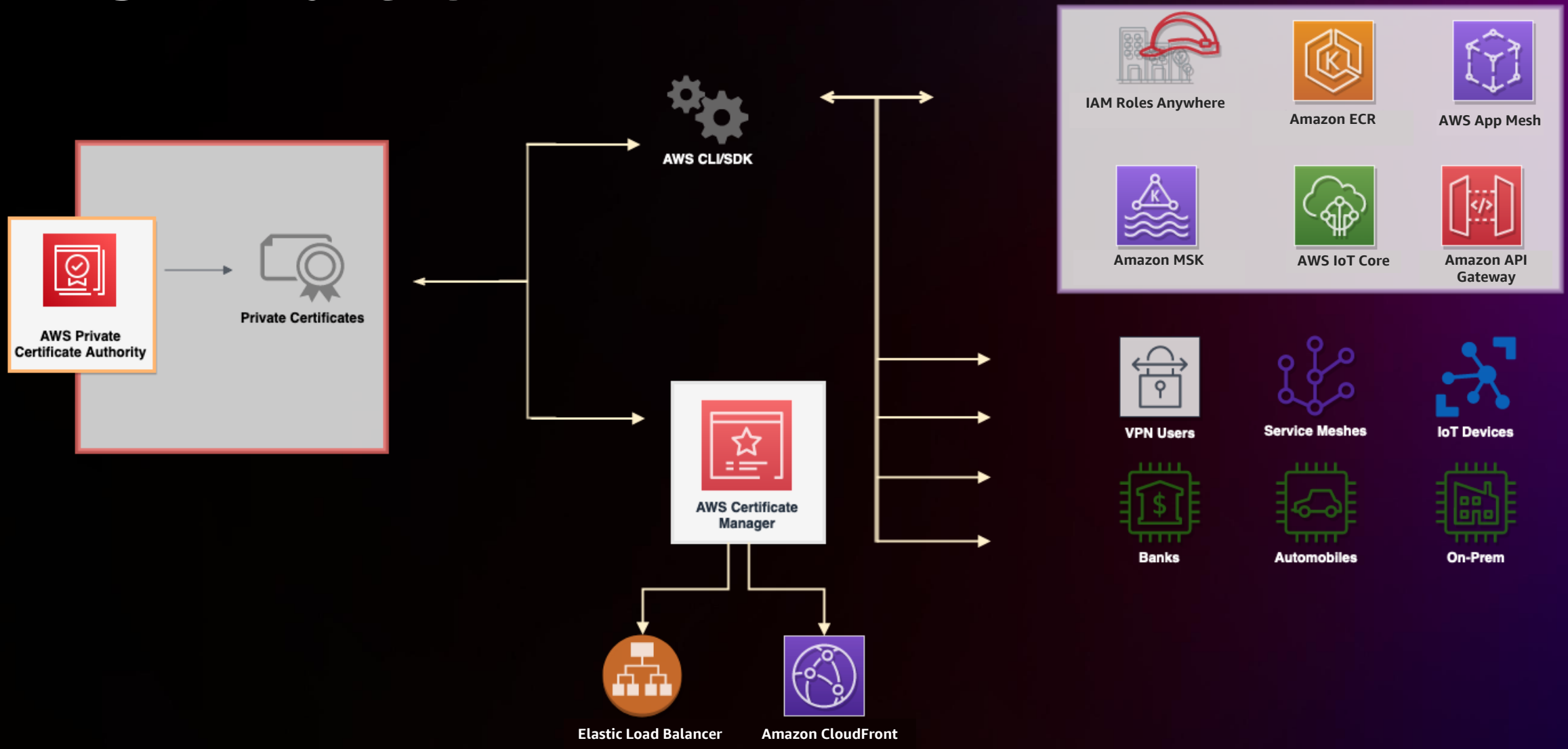


Pay-as-you-go pricing

aws

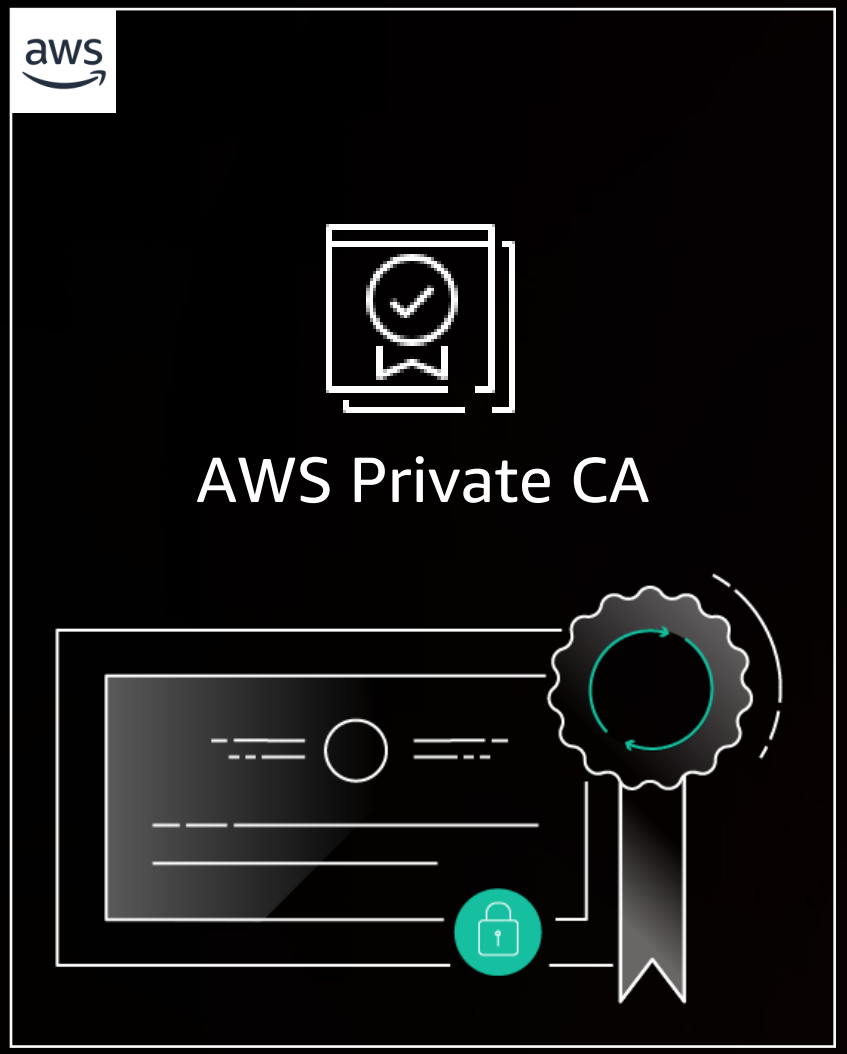
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Private CA



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

When to use a private CA?



AWS resources

- Implement end-to-end encryption to AWS resources or on-premises servers

IoT and device apps

- Issue certificates for IoT or manufactured devices

Service mesh and containers

- Provide real-time certificates for service meshes and container workloads

Identity

- Issue identity certificates for devices, machines, and users

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

Customization for private certificates

Flexible certificate attributes

- Custom certificate lifetimes
- Custom subjects and name constraints
- Custom extensions

Use cases for certificate customization

- IAM Roles Anywhere
- Identify devices by name or serial number (IoT), e.g., Matter
- Kubernetes and service meshes



Flexibility to customize private certificates



Custom lifetimes



Custom extensions



Private certificate

aws

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

What is AWS Signer?

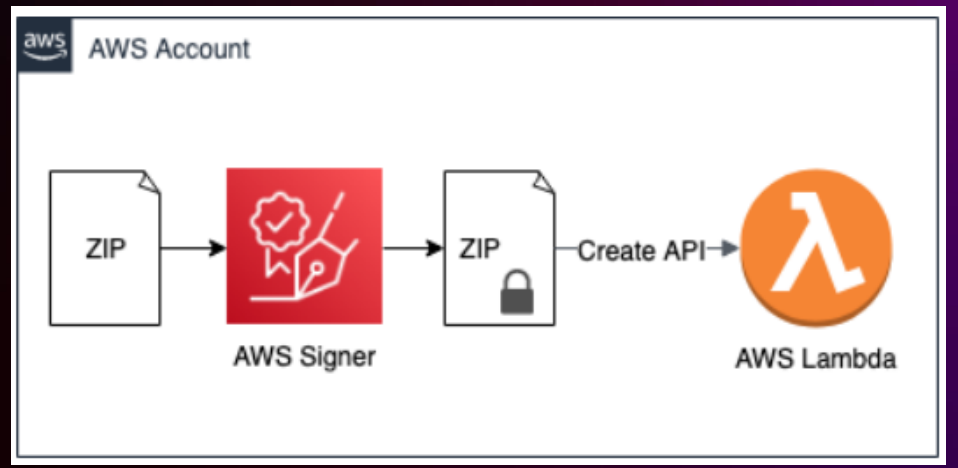
- Fully managed service for code integrity and authenticity
- Eliminates customer overhead of managing cryptographic resources
- Available for IoT Firmware, Lambda and Container Images
- Integrate signing with build pipelines and CI/CD systems
- Meet compliance and security requirements to ensure SW is tamper-free

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

AWS Signer use cases

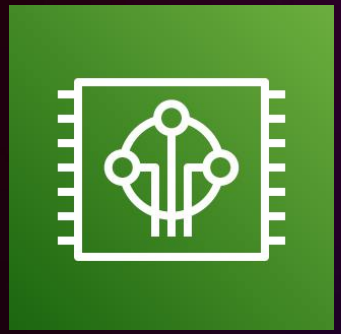
AWS Lambda

- Ensures that only trusted code runs in your Lambda functions
- Create digitally signed packages for Lambda deployment
- Revocation support



AWS IoT

- Integrated with AWS Certificate Manager (ACM)
- Sign updates in FreeRTOS and AWS IoT Device Management



FreeRTOS

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

AWS Certificate Services in nutshell



AWS Certificate Manager (ACM)

Certificates

Certificates – public, private, and imported

Managed renewal – with ACM integrated services

Monitoring – ACM health events and expiry metrics



AWS Private Certificate Authority

Certificate authorities

Certificates – private, customized

Renewal – automate, automate, automate

Monitoring – AWS CloudTrail and audit reports



AWS Signer

Signatures

Signatures – code signing for lambdas and IoT

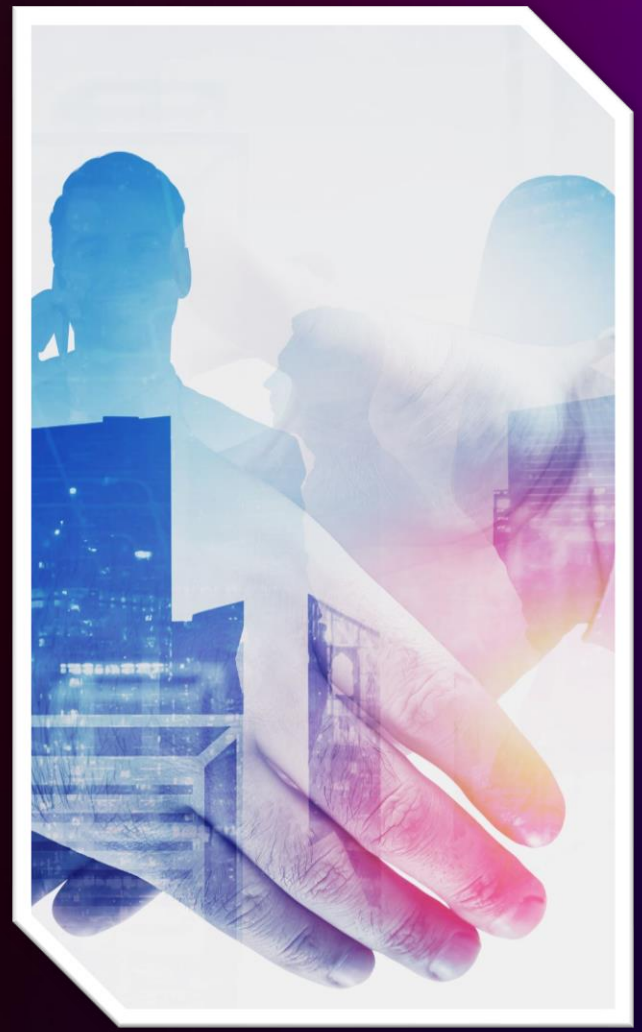
Monitoring – AWS CloudTrail

aws

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

Summary

- AWS KMS makes it easy to secure your data within AWS
  - Server-side encryption
  - Client-side encryption
- AWS Certificate Services
  - Full lifecycle certificate management
  - Securing traffic over HTTPS
  - Ensures that you run trusted code



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

Further viewing

Ken Beer	Mark Ryland	Raghu Prabhu	Peter O'Donnell
How encryption works in AWS https://www.youtube.com/watch	Security benefits of the Nitro architecture https://www.youtube.com/watch	Data, S3 bucket, AWS account, and encryption strategies for data lakes on S3 https://www.youtube.com/watch	Using AWS KMS for data protection, access control, and audit https://www.youtube.com/watch

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

Further viewing

Todd Cignetti	Param Sharma	Channy Yun	Louay Shaat
Introducing AWS Private Certificate Authority (CA) https://www.youtube.com/watch	TLS-enabled Kubernetes clusters with ACM Private CA and Amazon EKS https://www.youtube.com/watch	Code signing, a trust and integrity control for AWS Lambda https://aws.amazon.com/blogs/aws/new-code-signing-a-trust-and-integrity-control-for-aws-lambda/	How to use AWS Certificate Manager with AWS CloudFormation https://aws.amazon.com/blogs/security/how-to-use-aws-certificate-manager-with-aws-cloudformation/

aws

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

Thank you!



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

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