Demystifying PKI and Certificates on AWS

Chandan Kundapur

Sr. Product Manager

From this session …

- Understand PKI offerings from AWS
  - AWS Certificate Manager and Private Certificate Authority
  - Best Practices
- Stand up your own PKI infrastructure
  - Use Cases
  - Best Practices
  - Frequently asked Questions
- Q &A

Goals …

"I have teams who need to terminate TLS, mTLS and identify resources using SSL/TLS certificates"

Resources include - Websites, applications, load balancers, API, service mesh

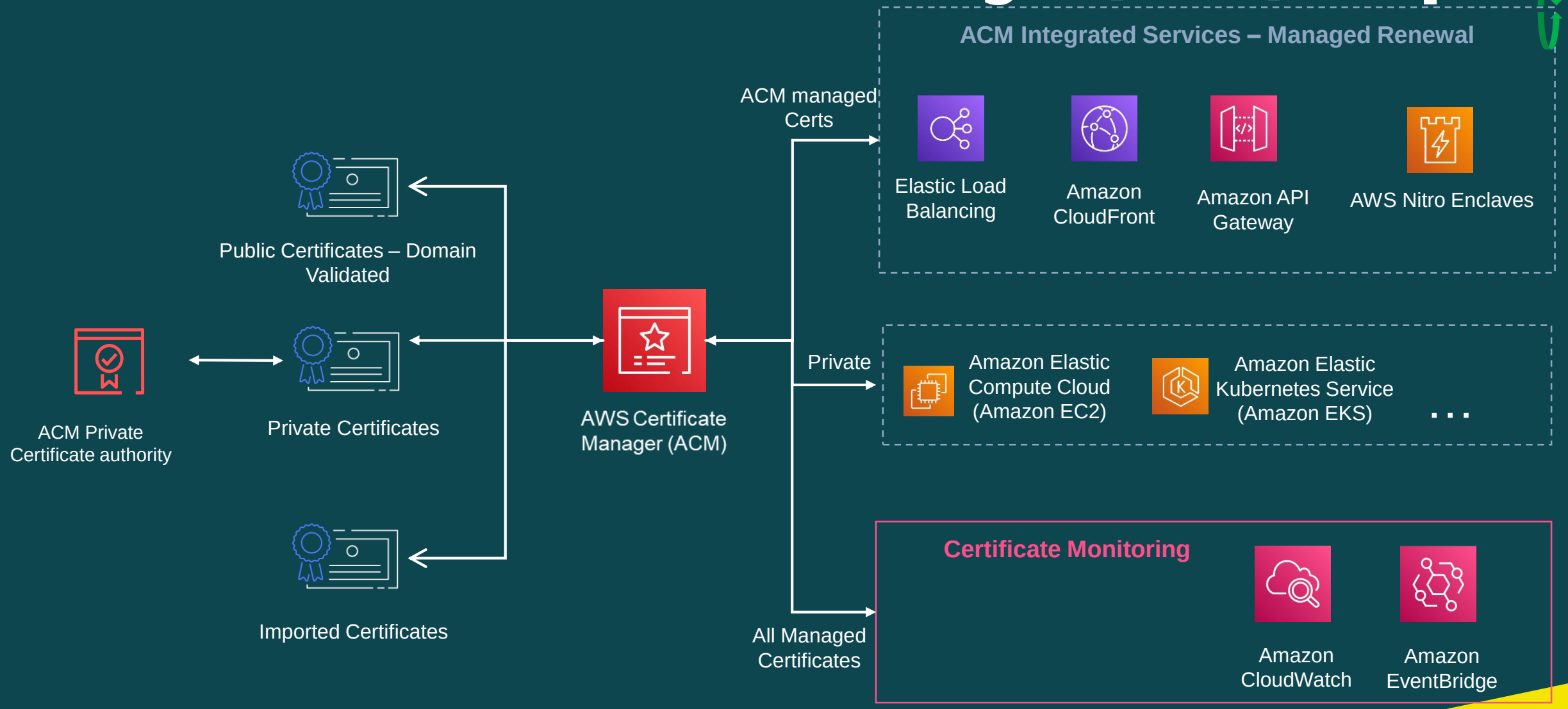
And associated concerns …

Cloud PKI

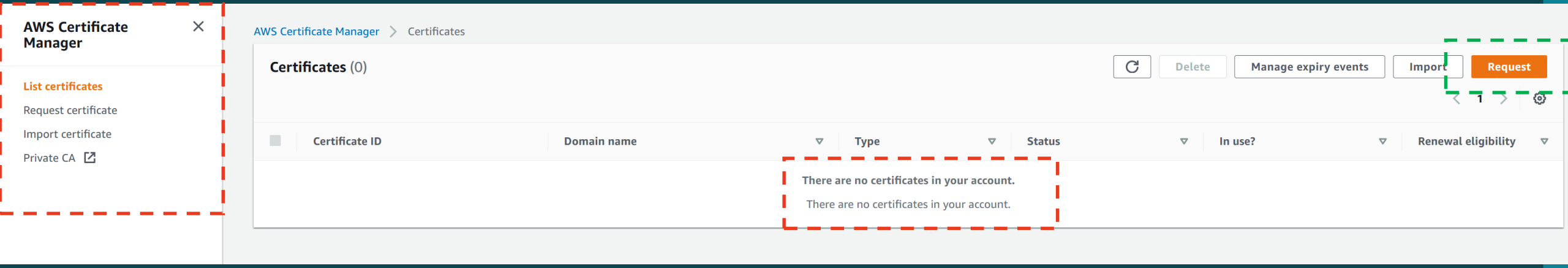
Operationalization

Cost…

How can AWS Certificate Manager (ACM) help ?



ACM – Public Certificate Issuance



ACM – Public Certificate Issuance

AWS Certificate Manager > Certificates > Request certificate

Request certificate

Certificate type Info

ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for acm to provide.

- (selected) **Request a public certificate**
  Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.
- (disabled) Request a private certificate
  No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit ACM Private Certificate Authority

Cancel | Next

ACM – Public Certificate Issuance

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Request public certificate

Domain names

Fully qualified domain name Info

acmmodweekdemo.com

Add another name to this certificate

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Select validation method Info

Select a method for validating domain ownership

- (●) DNS validation - recommended
  Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.
- ( ) Email validation
  Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Tags Info

To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key: Enter key

Tag value - *optional*: Enter value

Remove tag

Add tag

You can add 49 more tag(s).

Cancel | Previous | Request

ACM – Public Certificate Issuance

Certificate status

Identifier
97587d37-b7d3-4aa8-bc0c-6c132c62a3ef

Status
Pending validation

ARN
arn:aws:acm:us-west-2:256187702185:certificate/97587d37-b7d3-4aa8-bc0c-6c132c62a3ef

Detailed status
The status of this certificate request is "Pending validation". Further action is needed to validate and approve the certificate. Info

Type
Amazon Issued

Domains (1)

Create records in Route 53 | Export to CSV

1

Domain	Status	Renewal status	Type	CNAME name	CNAME value
acmmodweekdemo.com	Pending validation	-	CNAME	_0fc8474ac3e221791d9cdba809f22651.acmmodweekdemo.com.	_109996125ef48387f71b6e7a272b4d8c.bgpjyrktby.acm-validations.aws.

Details

In use?
No

Serial number
N/A

Requested at
February 09, 2022, 17:23:14 (UTC-08:00)

Renewal eligibility
Ineligible

Domain name
acmmodweekdemo.com

Public key info
RSA-2048

Issued at
N/A

Number of additional names
0

Signature algorithm
SHA256WITHRSA

Not before
N/A

Can be used with
CloudFront, Elastic Load Balancing, API Gateway and other integrated services.

Not after
N/A

ACM – Public Certificate Issuance

AWS Certificate Manager > Certificates > 9a4ab21f-44d5-4483-856b-5b65fa60b530 > Create DNS records in Amazon Route 53

Create DNS records in Amazon Route 53 (1/1)

Search domains

1 match

1

Validation status: Pending validation ✕ | Validation status: Failed ✕ | Is domain in Route 53?: Yes ✕ | Clear filter

☑	Domain	Validation status	Type	CNAME name	CNAME value	Is domain in Route 53?
☑	acmmodweekdemo.com	Pending validation	CNAME	_0fc8474ac3e221791d9cdba809f22651.acmmodweekdemo.com.	_109996125ef48387f71b6e7a272b4d8c.bgpjyrktby.acm-validations.aws.	Yes

Cancel | Create records

ACM – Public Certificate Issuance

AWS Certificate Manager > Certificates > 9a4ab21f-44d5-4483-856b-5b65fa60b530

9a4ab21f-44d5-4483-856b-5b65fa60b530

Delete

Certificate status

Identifier
9a4ab21f-44d5-4483-856b-5b65fa60b530

ARN
arn:aws:acm:us-west-2:256187702185:certificate/9a4ab21f-44d5-4483-856b-5b65fa60b530

Type
Amazon Issued

Status
Issued

Detailed status
The certificate was issued at February 09, 2022, 18:52:07 (UTC-08:00).

Domains (1)

Create records in Route 53 | Export to CSV

1

Domain	Status	Renewal status	Type	CNAME name	CNAME value
acmmodweekdemo.com	Success	-	CNAME	_0fc8474ac3e221791d9cdba809f22651.acmmodweekdemo.com.	_109996125ef48387f71b6e7a272b4d8c.bgpjyrktby.acm-validations.aws.

Details

In use?
No

Domain name
acmmodweekdemo.com

Number of additional names
0

Serial number
0f:84:70:09:65:ee:14:7a:2b:19:56:50:65:32:70:ac

Public key info
RSA-2048

Signature algorithm
SHA256WITHRSA

Requested at
February 09, 2022, 18:42:32 (UTC-08:00)

Issued at
February 09, 2022, 18:52:07 (UTC-08:00)

Not before
February 09, 2022, 16:00:00 (UTC-08:00)

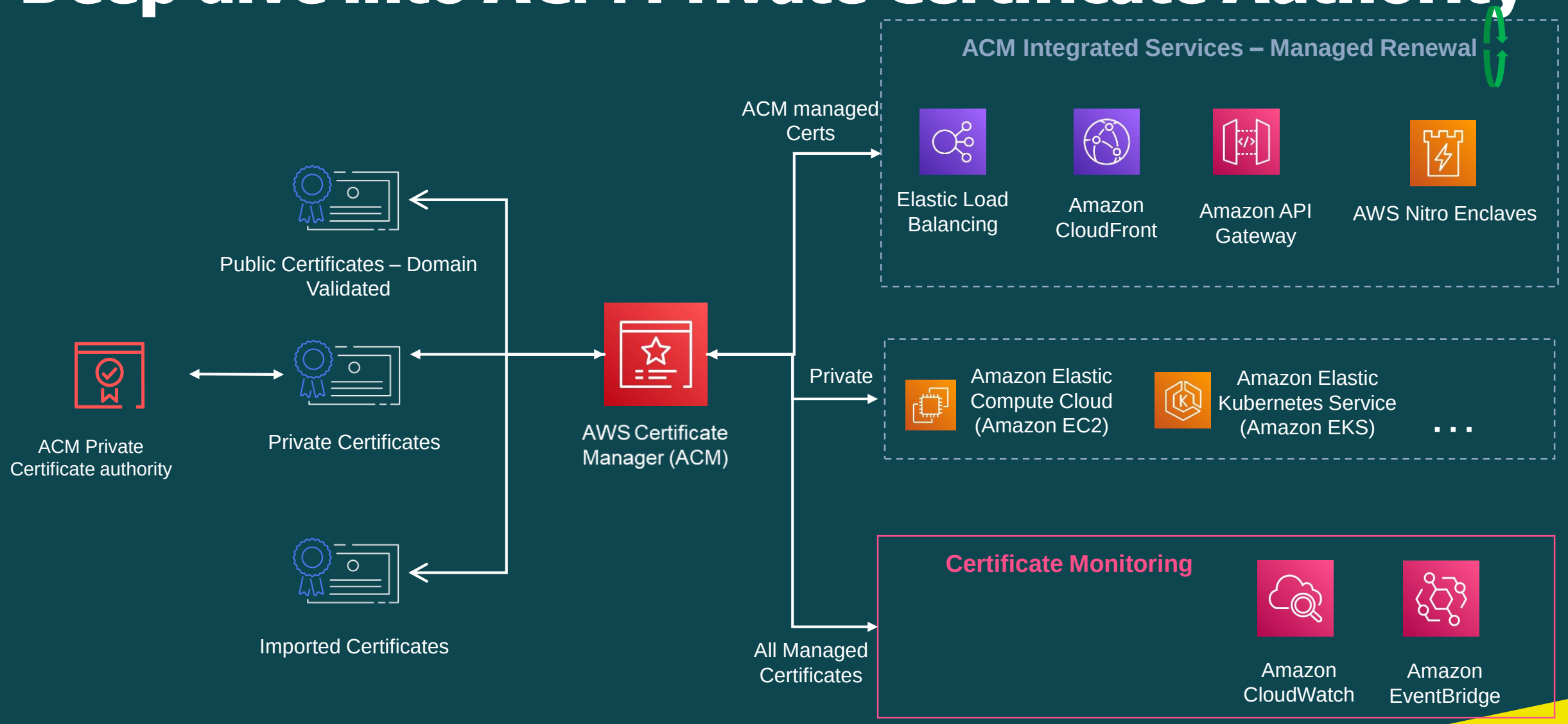
Renewal eligibility
Ineligible

- Through API – Request-Certificate ; Describe-Certificate

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

Deep dive into ACM Private Certificate Authority

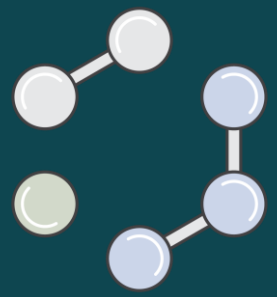


What is ACM Private Certificate Authority ?

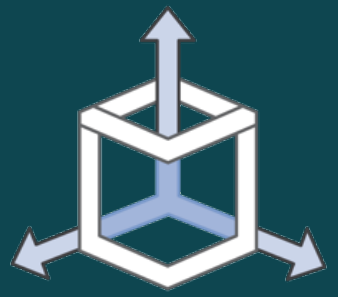
Secure and Managed Private Certificate Authority

Root CA and complete CA Hierarchies

Enable Developer Agility



Flexibility to Customize Private Certificates



Manage Certificate Authorities Centrally

Pay as You Go Pricing

AWS Certificate Services

AWS Certificate Manager (ACM)

- Certificate Life cycle Management
- Certificates – Public, Private and Imported
- Managed Renewal – With ACM Integrated Services
- Monitoring – ACM health events and Expiry metrics
- Access – Through ACM console and ACM APIs

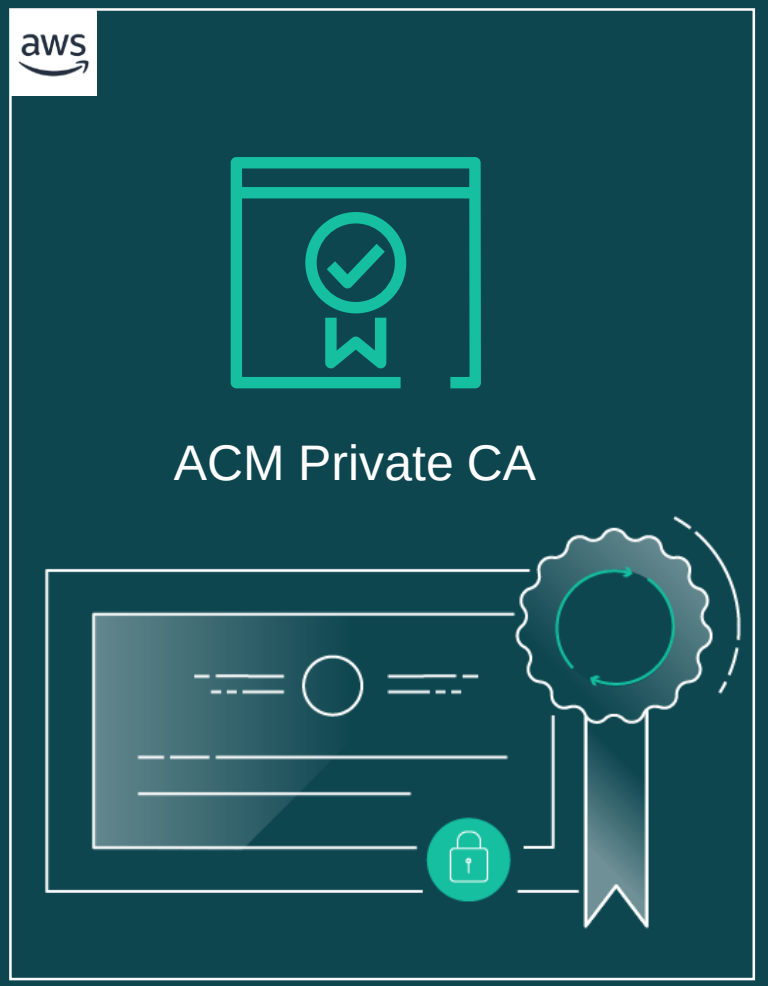
  (Ex : *RequestCertificate*)

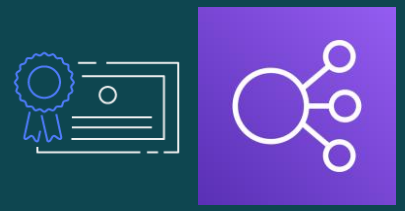
ACM Private Certificate authority

- Certificates – Private, customized | Ex : ECDSA
- CA lifecycle Management
- Renewal - Automate, automate, automate
- Monitoring – AWS CloudTrail and Audit Reports
- Access – Through ACM PCA APIs from any AWS accessible workload

  (Ex : *IssueCertificate*)

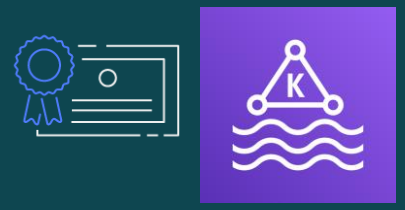
Use cases





AWS Resources and Containers

- Implement end-to-end encryption to AWS resources



Service Mesh and Containers

- Provide real time certificates for service meshes and container workloads

IOT Devices and Apps

- Issue certificates for IoT or manufactured devices

Identity

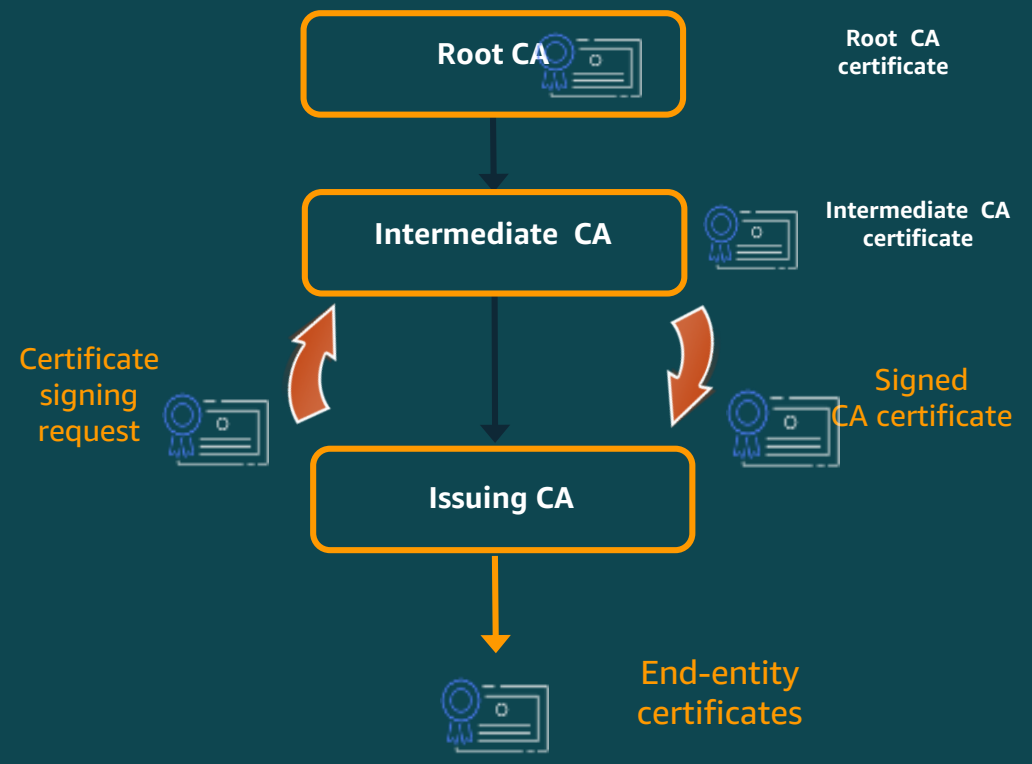
- Issue identity certificates for devices, machines, and users

ACM Private CA Hierarchies

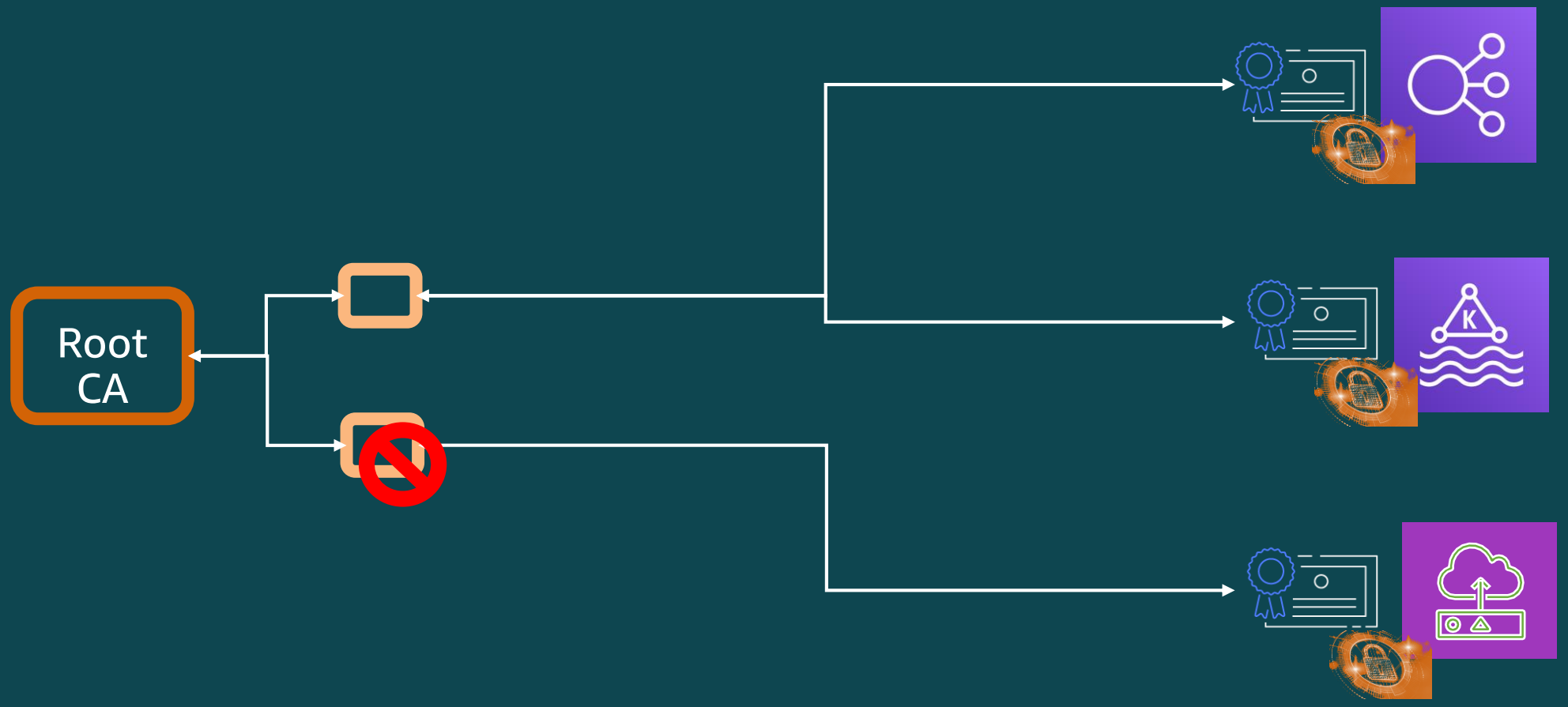
- Complete CA hierarchy, including root CA
- Third-party external CA is optional
- PCA supports complex hierarchies with up to five levels

Notable benefits of a CA hierarchy:

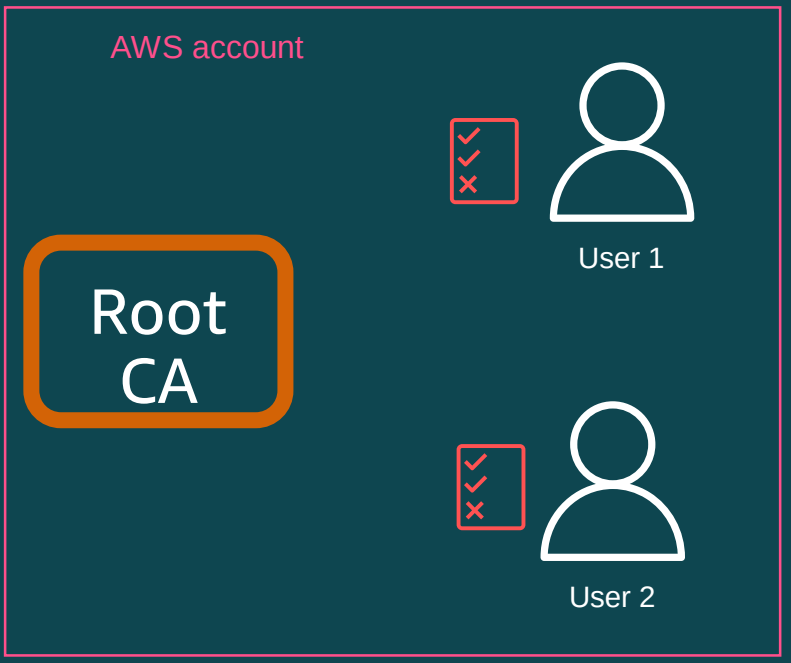
- Granular security controls appropriate to each CA
- Flexibility to map CA hierarchy to organizational needs



Planning your PKI – Root Hierarchy



CA Hierarchy and Access



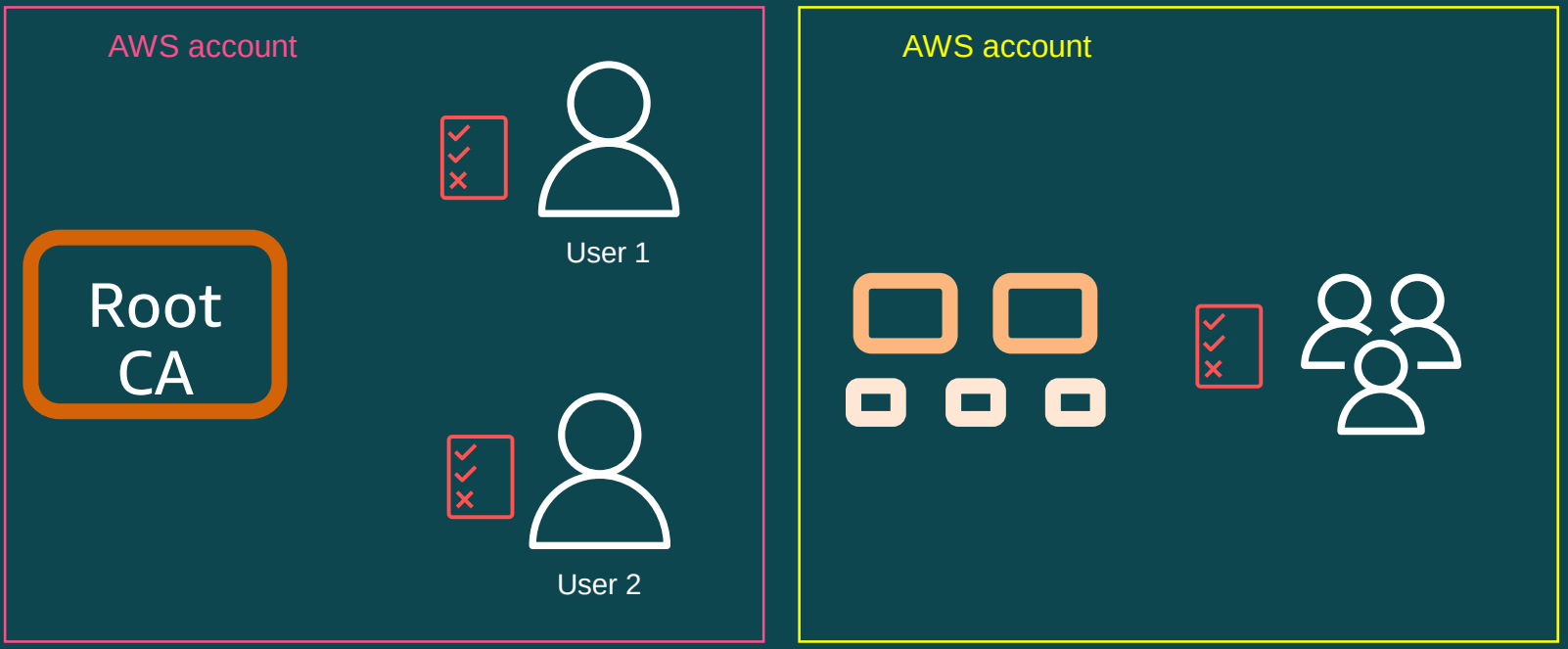
IAM rule for 2 person access

```
{
    "Effect": "Allow",
    "Action": [
        "acm-pca:IssueCertificate"
    ],
    "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*",
    "Condition": {
        "StringLike": {
            "acm-pca:TemplateArn": [
                "arn:aws:acm-pca:::template/*CACertificate*/V*"
            ]
        }
    }
},
{
    "Effect": "Deny",
    "Action": [
        "acm-pca:UpdateCertificateAuthority"
    ],
    "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*",
},
```

IAM rule for 2 person access

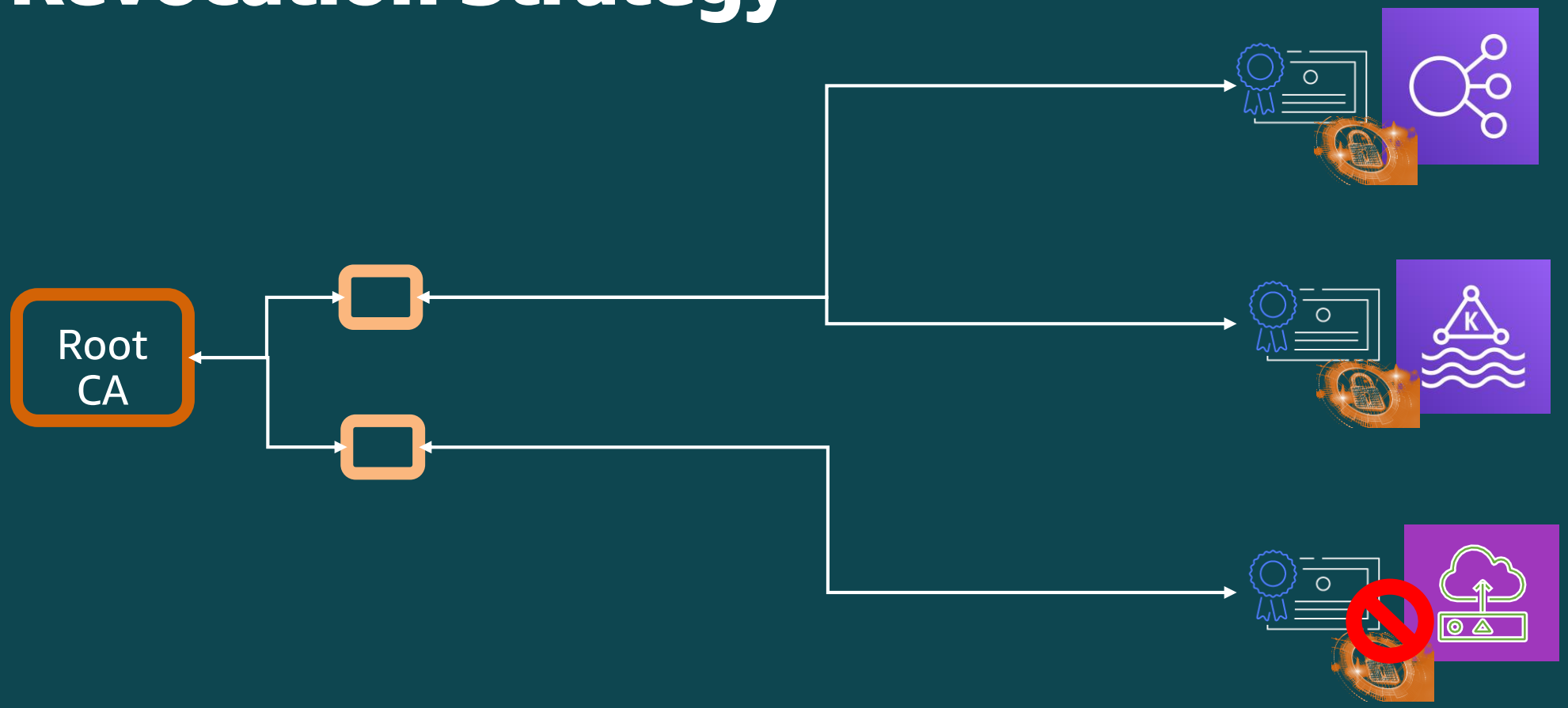
```
{
    "Effect": ”Deny",
    "Action": [
        "acm-pca:IssueCertificate"
    ],
    "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*",
},
{
    "Effect": ”Allow",
    "Action": [
        "acm-pca:UpdateCertificateAuthority"
    ],
    "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*",
},
```

CA Hierarchy and Access



- Do – Start with IAM Policies
- Do – Disable CA
- Do – Monitor Root CA
- Do – Rotate Subordinate
- Do – Audit Reports

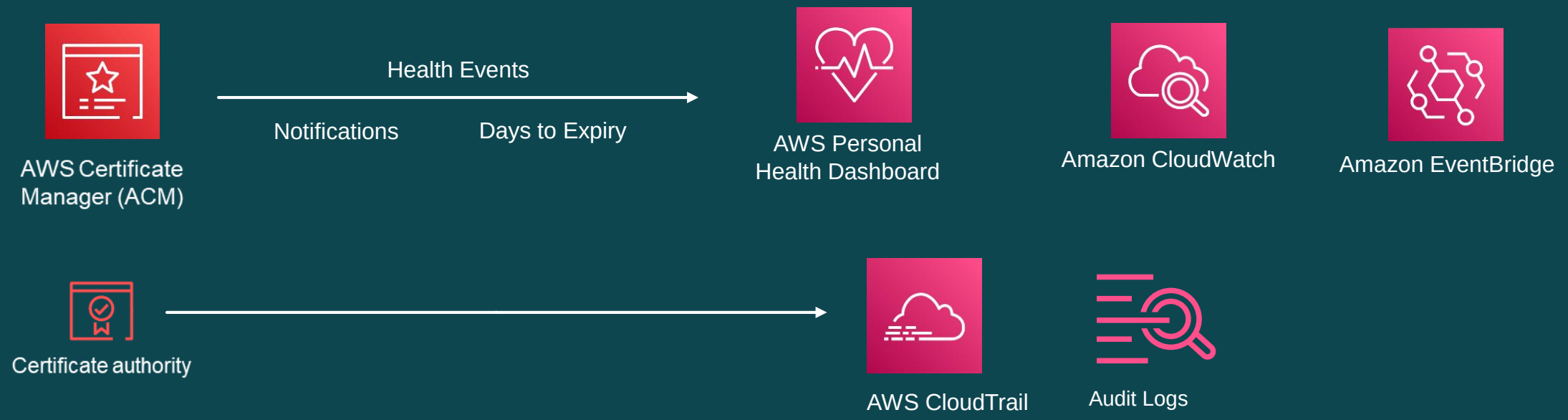
Revocation Strategy



Short-lived certs and/or revocation through CRL or OCSP

Monitoring

Monitoring instead of scanning



Blog : https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/

Pricing

Public Certificates

- No cost

Private Certificates issued

- You pay for certificates for which you have access to the private key *(i.e. issued directly from Private CA or exported from ACM)*

Private CA Operation

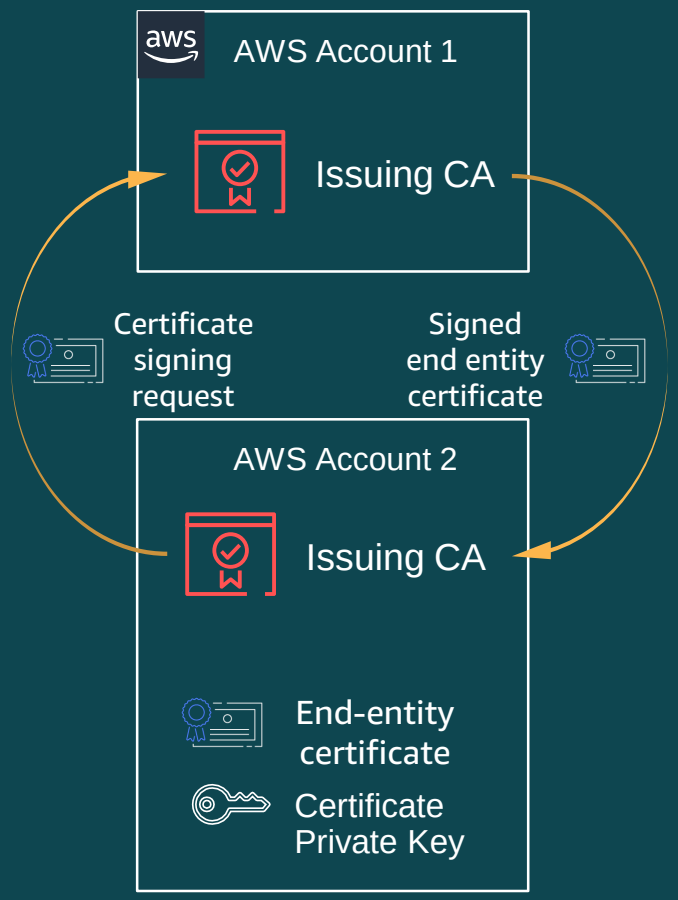
- $400 per month, per CA
- Monthly fee for the operation of each ACM Private CA until you delete it

Certificates issued (per month, per region)	Price per certificate
0–1,000	$0.75
1,000–10,000	$0.35
10,000+	$0.001

- Free Trial – First 30 days of CA operation for the first CA are free for new accounts. You pay for certificates issued during the trial.

Cross Account CA Sharing

- CA sharing via AWS Resource Access Manager (RAM)
- CAs with granular access control in shared accounts
- Share to specific accounts or an AWS Organization
- Use ACM to issue, associate and renew certificates from shared CAs



Thank you!