SEC 314 – R1

# Building and operating a private certificate authority on AWS

**Ram Ramani**

Security Solutions Architect
Amazon Web Services

**Christine Samson**

Solutions Architect
Amazon Web Services

**Anthony Pasquariello**

Solutions Architect
Amazon Web Services

**Hollister Scholte**

Principal Solutions Architect
Amazon Web Services

AWS re:Invent



aws

# Agenda

- AWS Certificate Manager (ACM) Topics – short presentation
- Hands-on workshop
- Live challenges
- Raffle

# AWS Certificate Manager (ACM)

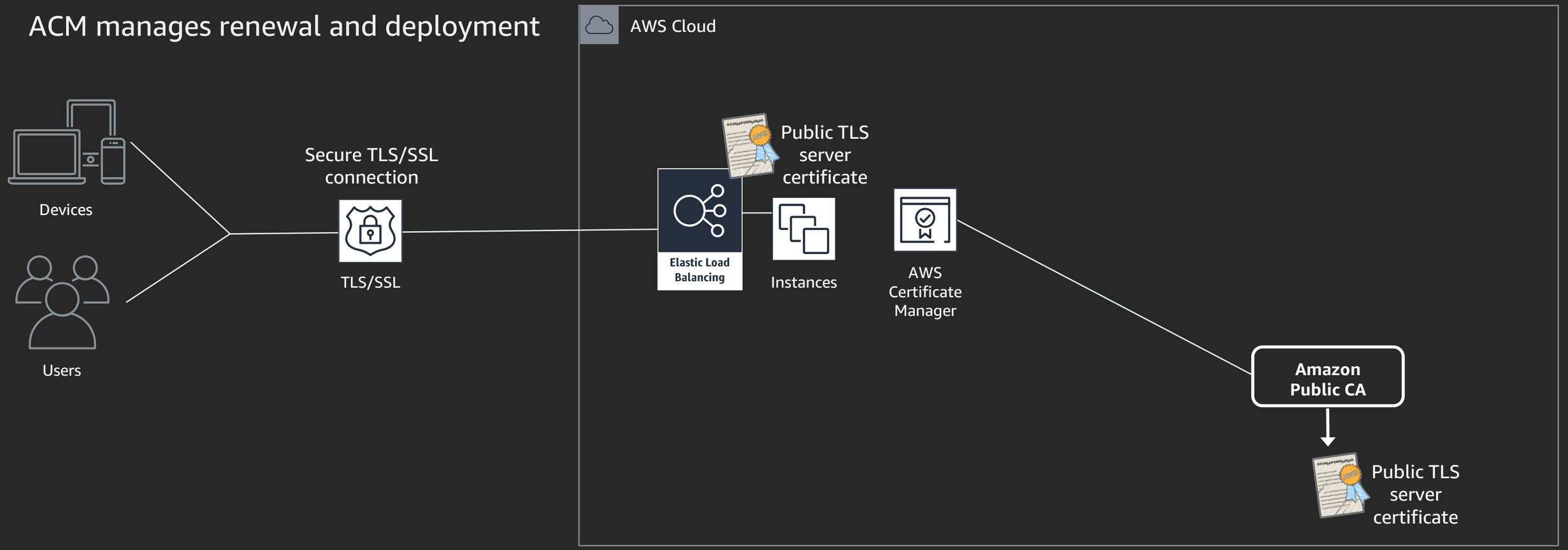
ACM makes it easy to provision, manage, deploy, and renew TLS/SSL certificates on the AWS cloud

# Acronyms

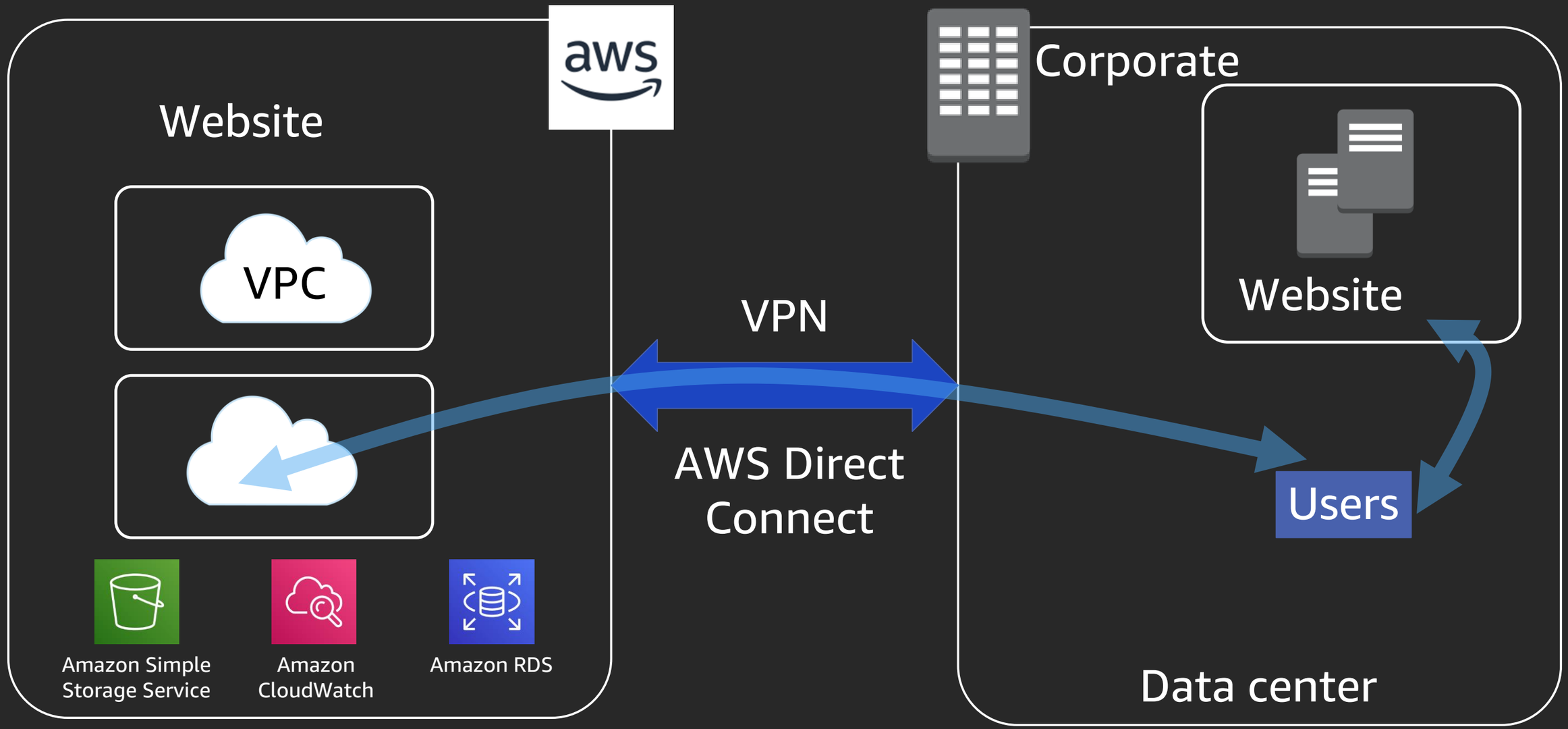
**ACM –** AWS Certificate Manager
**PCA or Private CA –** Private Certificate Authority
**CA** - Certificate Authority
**Cert –** Certificate
**CSR -** Certificate Signing Request
**CRL** – Certificate Revocation List
**ELB** - Elastic Load Balancer
**ALB –** Application Load Balancer

# Example: ACM with Elastic Load Balancing

- Public certificates requested with ACM
- Deployed on ELB
- ACM manages renewal and deployment



# Accessing private web apps in your intranet



# What is a Certificate Authority ?

## Certificate

```
subject = {
        'Country': 'US',
        'Organization': ‘My Org',
        'OrganizationalUnit': ‘My Dept',
        'State': ‘New York',
        'CommonName’: ‘*.myorg.biz’,
        'SerialNumber':’ 0D AD DB AE
7F’,
        'Locality': ‘New York'
    }
```

## Private and Public Keys

```
-----BEGIN PRIVATE KEY-----
j+oU8WtVkTZphwEGr7l1UowYCbZ/dQ9xy03UO7Wb4+TqFQLdn/GgzyR/A8QRljxI
V4rlj3H8Q/ZY/mDEkgjLhEmRCmWJ7ik7S7EahkPxizYixa7SOGXMR2bDPQKBgArz
5E1dcWeQQji5tyBWYesY/rUv3BM7Hh13LWDgGdgdK98DE/FOn4ObivYdjYU5CmU0
J5pSXVHFXfyQU8ELYWFOx9Amw0ASoirPQh2GGOZ8T4/xG3szZTIF9j/8n9tl9TjM
0vGMDFo8BIijxEMR7kLs1l6SnYarOt1ZteplESgZAoGABP+qasDZG4L8bpnvwziz
WzWVgHxmZqdc1n3zQ8B0MCMRWO1Uu379a7KuDKvkXglCAX5nEm46AwCF0duCi/GQ
0chDWggBE6yQDCVPy5DReWiEmKBQkqljgCYTtY2ILZb2Zxf5DX2MIR/tbAru/zwX
YVGd7L3pb4jXDy0XITVVzxA=
-----END PRIVATE KEY-----
```

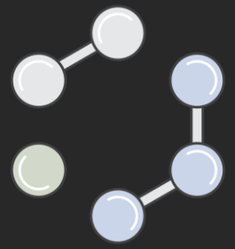
aws

# ACM Private CA

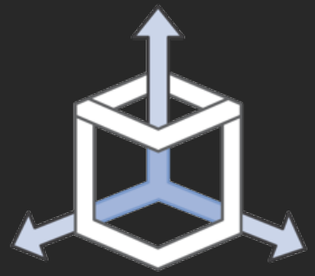
Secure and managed private CA service

Subordinate CAs

Enable developer agility



Flexibility to customize private certificates



Manage certificates centrally

Pay-as-you-go pricing

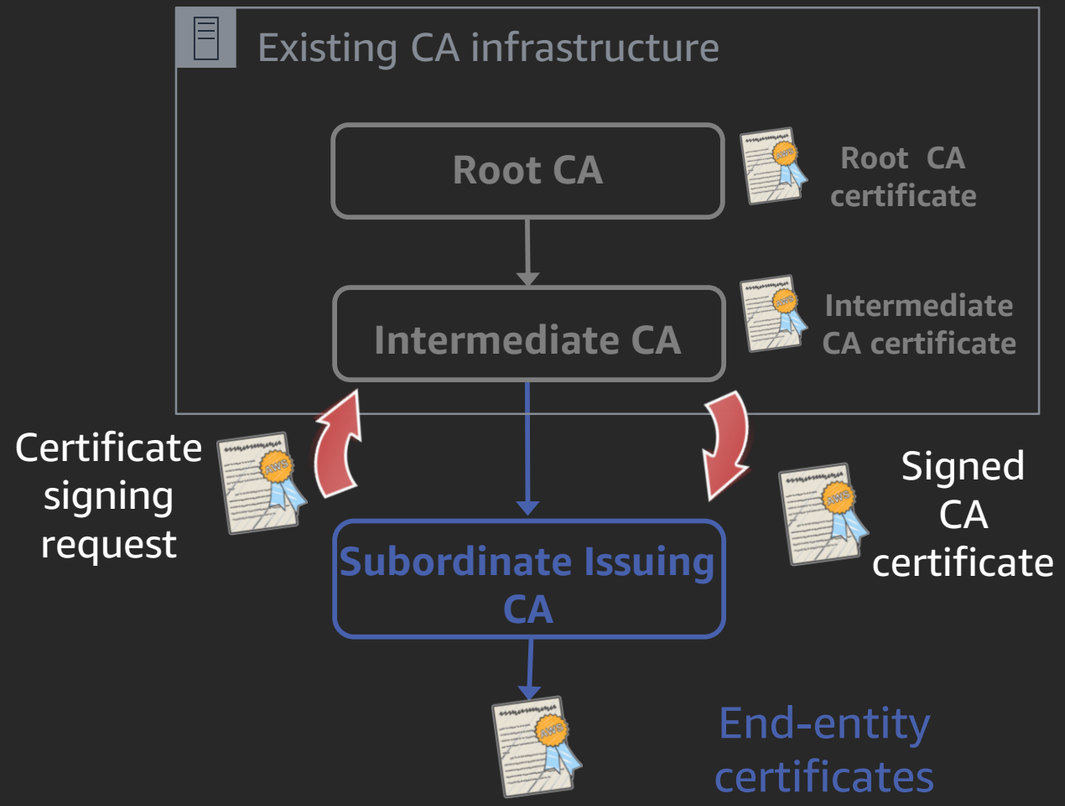
# Root CA hierarchies for ACM Private CA

Root CA and complete
CA hierarchies

CA administrators can now create a complete CA hierarchy, including root and subordinate CAs, with no need for external CAs

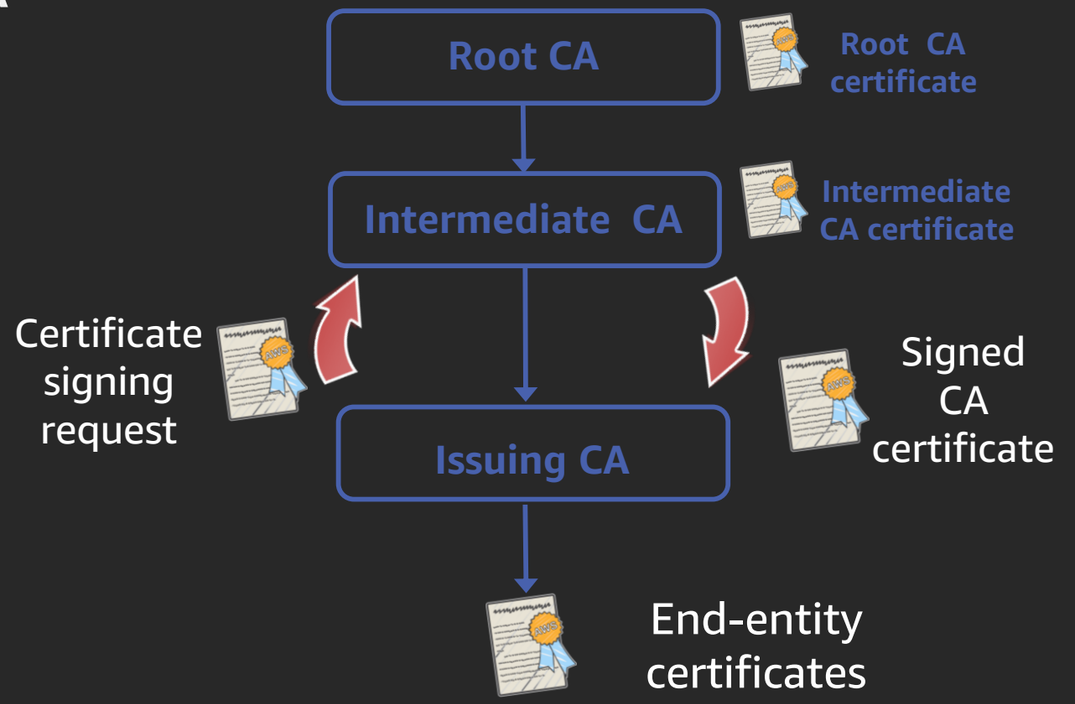
# Before ACM Private CA hierarchies

- Subordinate issuing CA with existing (external) intermediate and root CA



# ACM Private CA hierarchies

- Complete CA hierarchy, including root CA
- Third-party external CA is now optional



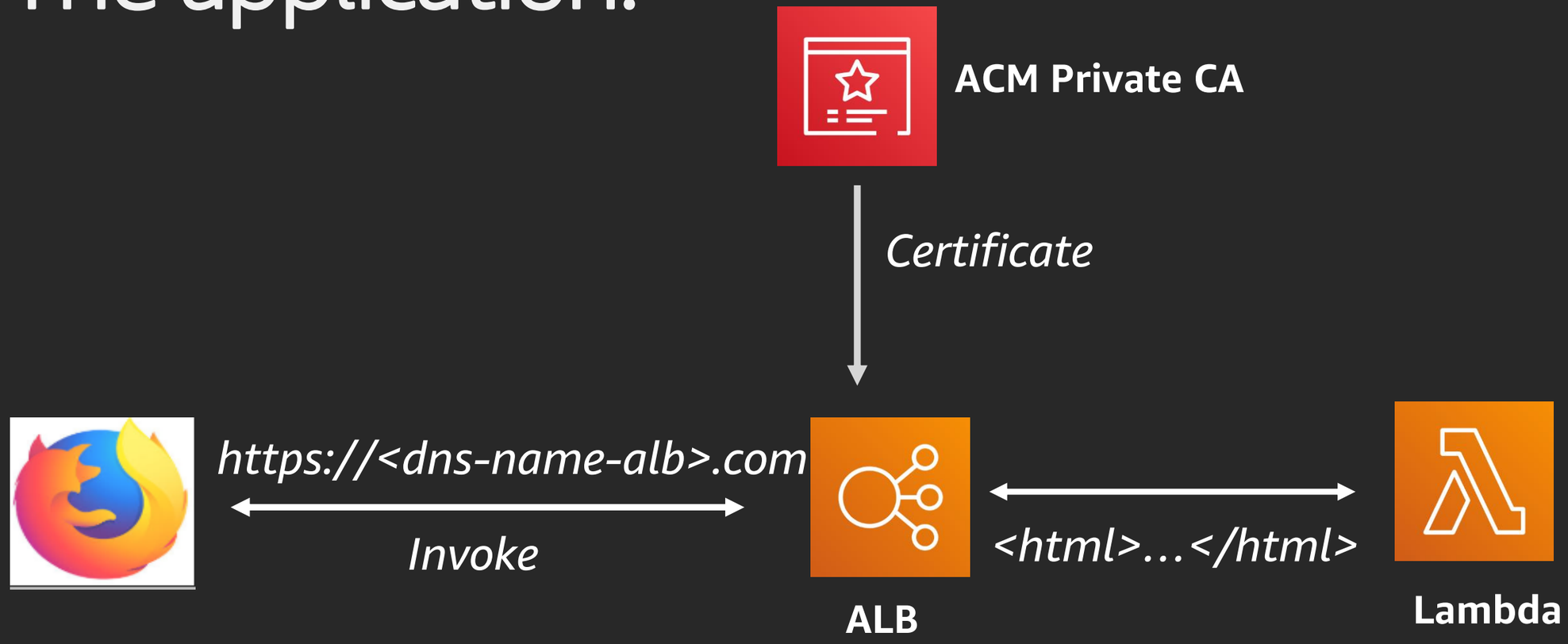
# Why create a CA hierarchy?

- Restrict access to the root CA
- Grant more permissive access to subordinate CAs
- Delegate subordinate CAs for different applications/groups
- Map your security root of trust needs for your organization structure

# What can end-entity certificates identify ?

- TLS endpoints and resources – example: any HTTPS application
- IoT devices
- Code signing certificates
- Certificates for signing OCSP responses

# The application:



# Job Functions :

CA Admin

Application Developer

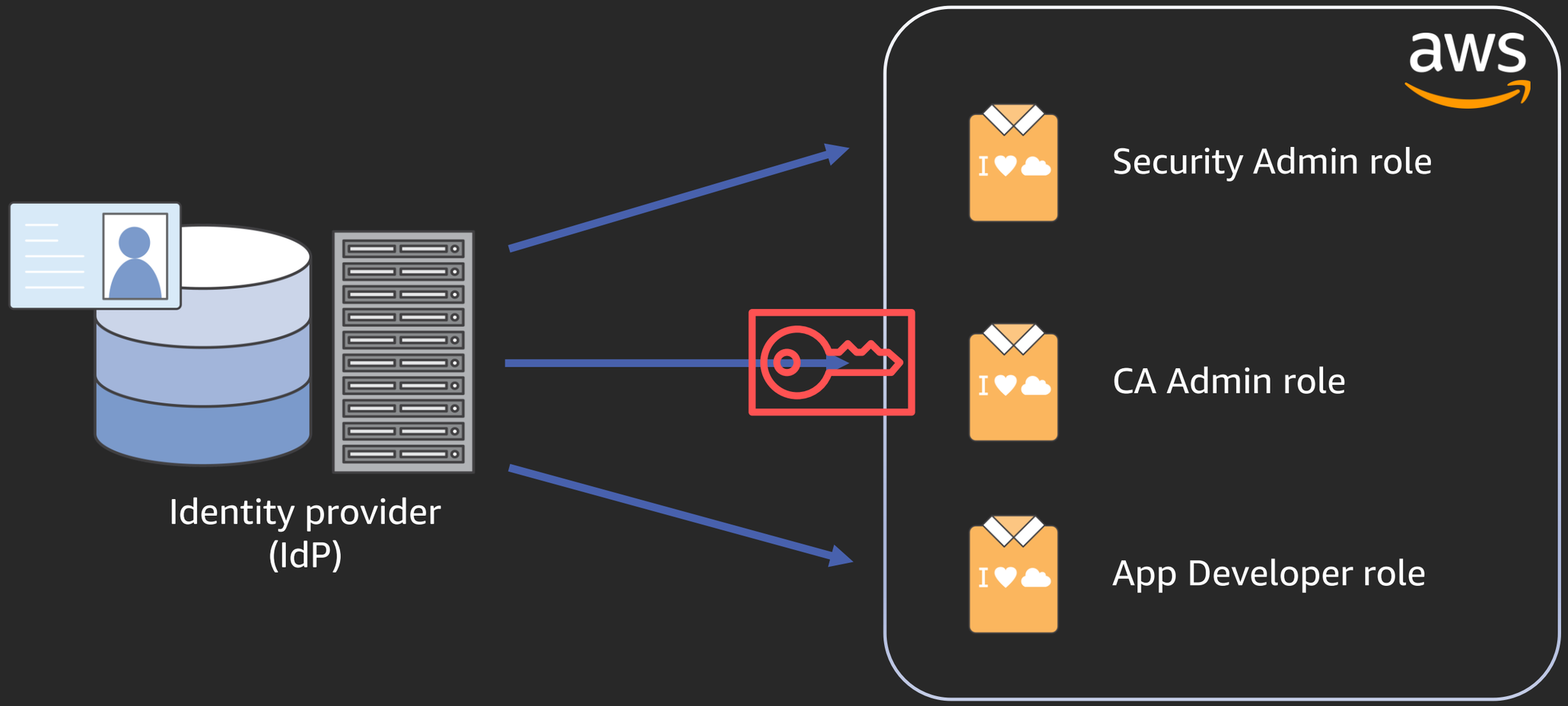
Security Admin

- Create and maintain CloudFormation templates that defines the CA Admin role and the Application Developer role.
- The role policies define permissions that these job functions can perform.

- Responsible for creating and maintaining the certificate authority hierarchy consisting of Root and Subordinate certificate authorities

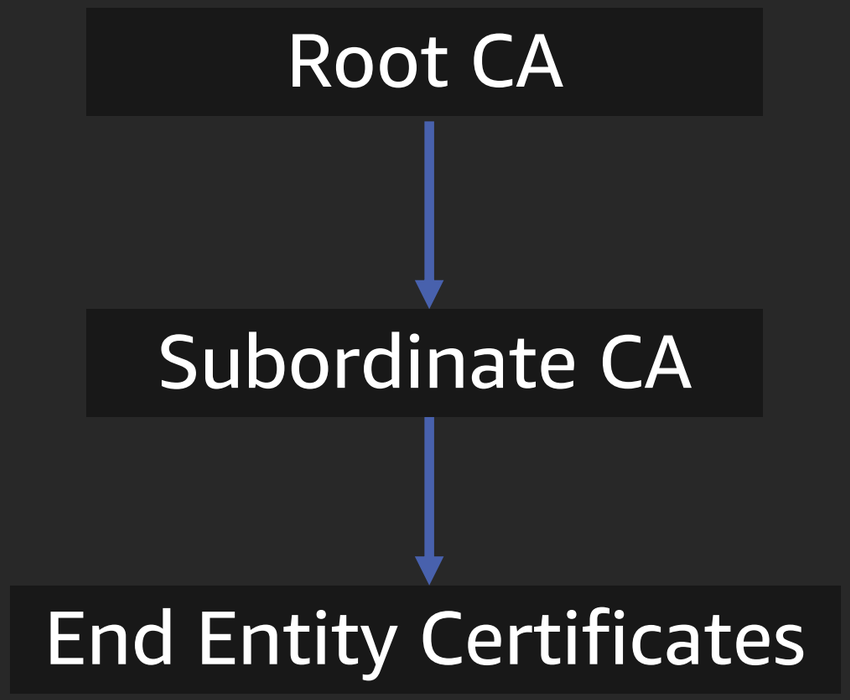
- Responsible for issuing certificates that can be used with an application.
- In this workshop, you will build a web app fronted by an ALB on which a private end entity certificate will be applied.

# Identity Provider Federation

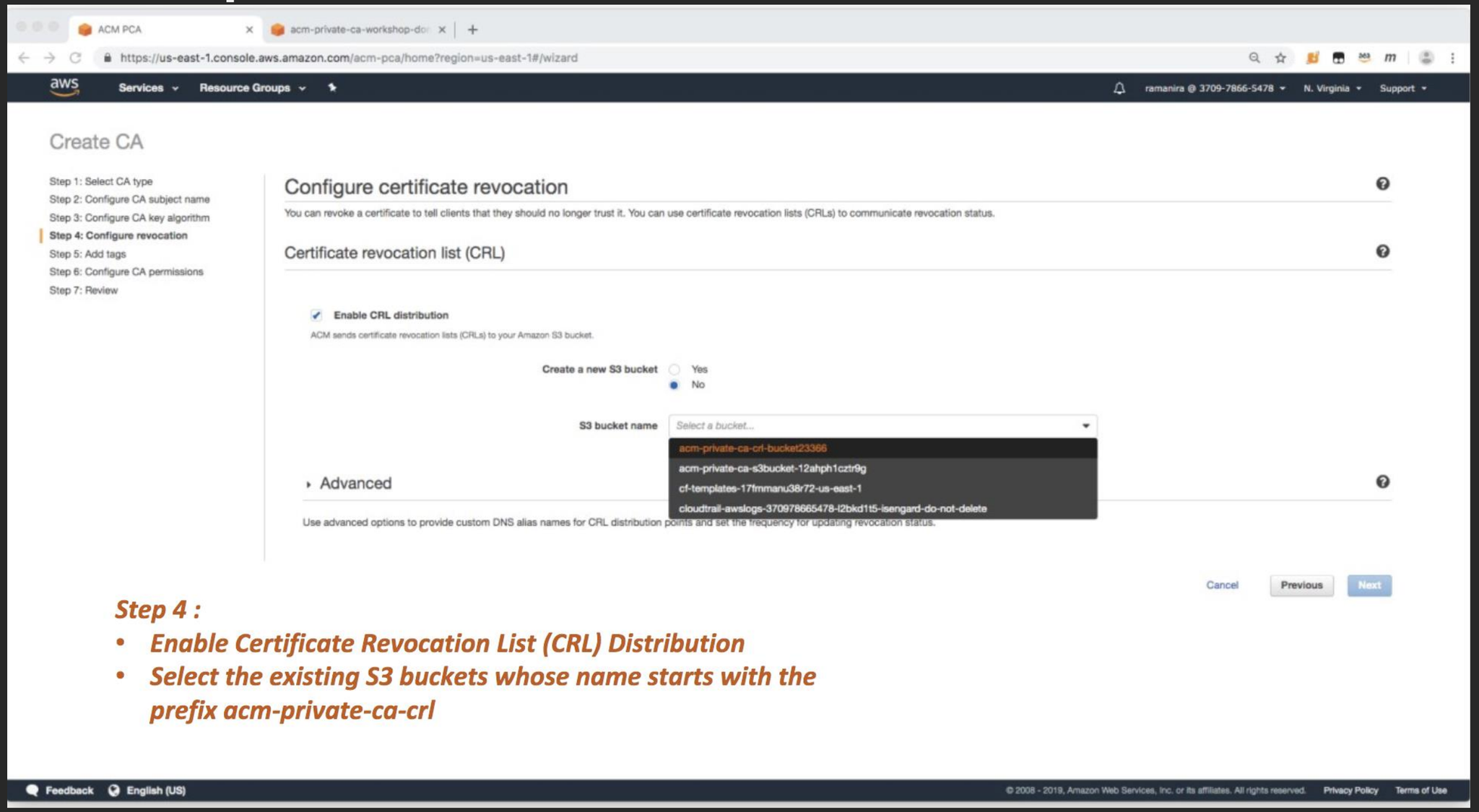



aws

# CA Hierarchy



# Visual steps




***Step 4 :***

- ***Enable Certificate Revocation List (CRL) Distribution***
- ***Select the existing S3 buckets whose name starts with the prefix acm-private-ca-crl***

# Quizzes

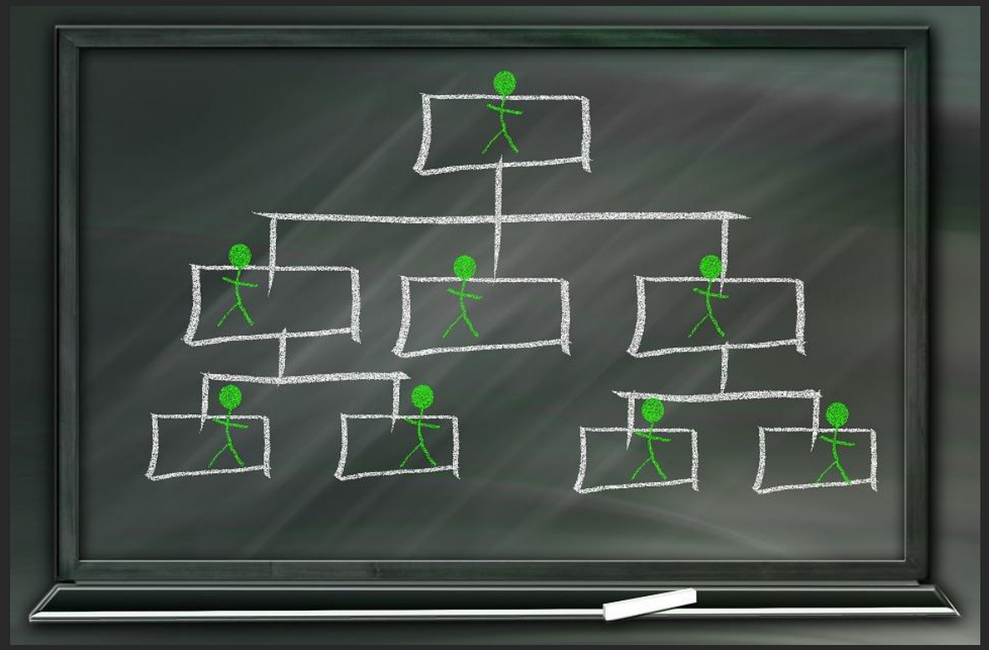
- Quizzes will be infused throughout the visual steps and GitHub instructions
- The correct answer and explanation will appear after answering and submitting the response
- Make sure to read explanations after each quiz to reinforce your learning

# Workshop link

https://bit.ly/2qzpoDG

# Live challenges

# CA Hierarchy



- Use path length constraint to limit CA height
- Why should you reduce height when possible?

# Inventory

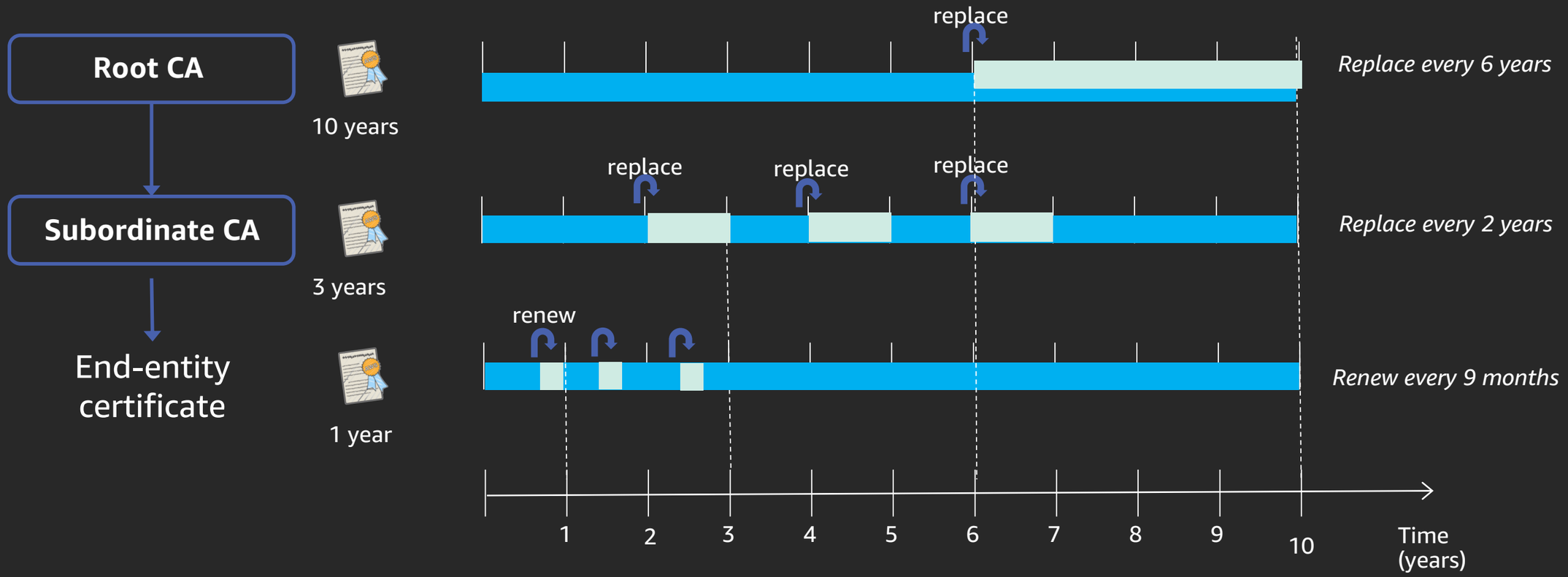
What feature of ACM Private CA should I use to know about the inventory of issued and revoked certificates?

# Inventory

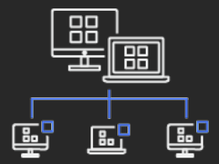

```
[{
    "awsAccountId":[redacted],
    "certificateArn":"arn:aws:acm-pca:us-east-2:[redacted]certificate-authority/3c1081ef-
    "serial":"83:f1:89:88:20:9b:d3:a9:42:bd:aa:ca:e1:b0:62:a1",
    "subject":"CN=acm-pca-usecase-6-alb-1975758280.us-east-2.elb.amazonaws.com",
    "notBefore":"2019-08-19T18:10:42+0000",
    "notAfter":"2020-09-19T19:10:42+0000",
    "issuedAt":"2019-08-19T19:10:42+0000"
},

{
    "awsAccountId":[redacted],
    "certificateArn":"arn:aws:acm-pca:us-east-2[redacted]certificate-authority/3c1081ef-
    "serial":"83:f1:89:88:20:9b:d3:a9:42:bd:aa:ca:e1:b0:62:a1",
    "subject":"CN=acm-pca-usecase-6-alb-1975758280.us-east-2.elb.amazonaws.com",
    "notBefore":"2019-08-19T18:10:42+0000",
    "notAfter":"2020-09-19T19:10:42+0000",
    "issuedAt":"2019-08-19T19:10:42+0000",
    "revokedAt":"2019-08-23T22:39:21+0000",
    "revocationReason":"CESSATION_OF_OPERATION"
}]
```

# Choosing CA validity period



# CA Hierarchy consideration



## Organization

How to create separation?
Who should trust what?

## Access

Who needs access?
How often?
From where?

## Issuance

How many certificates?
Over what time?

## Validity

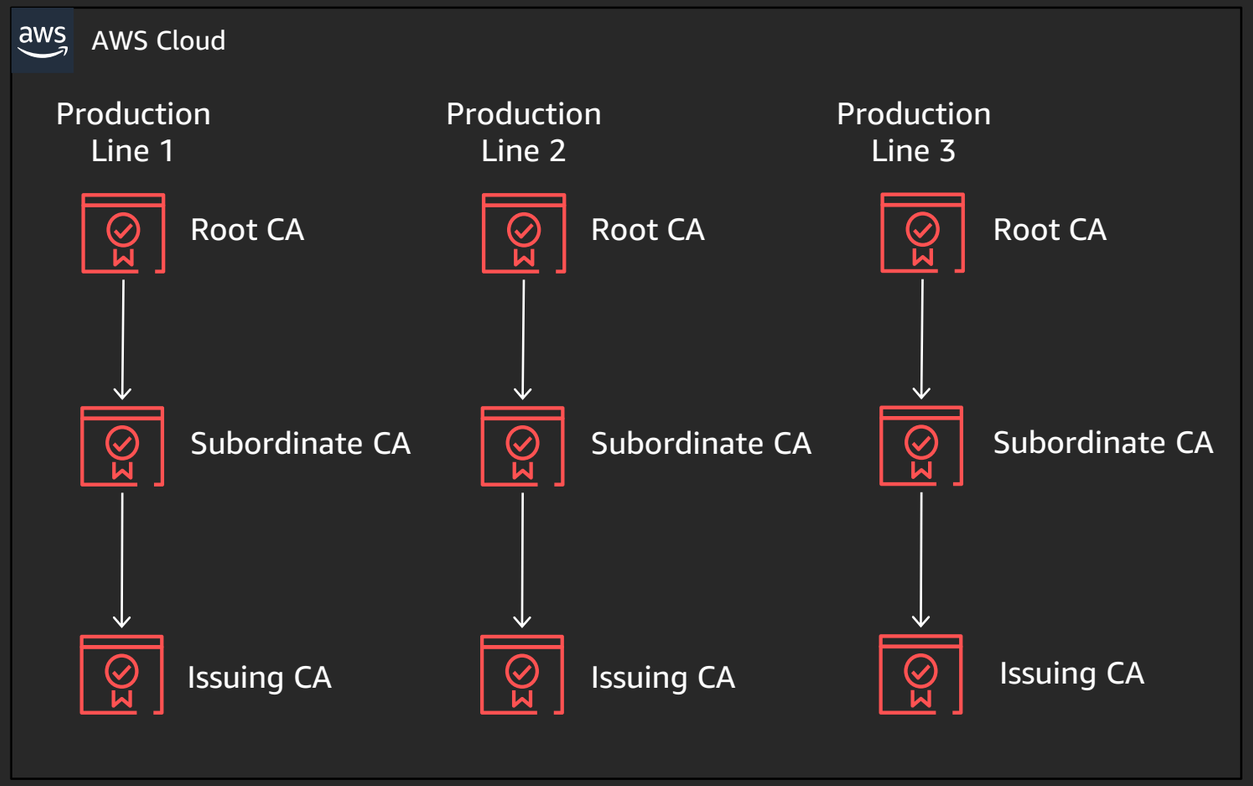
Necessary lifespan?
What if they get out?

## Revocation

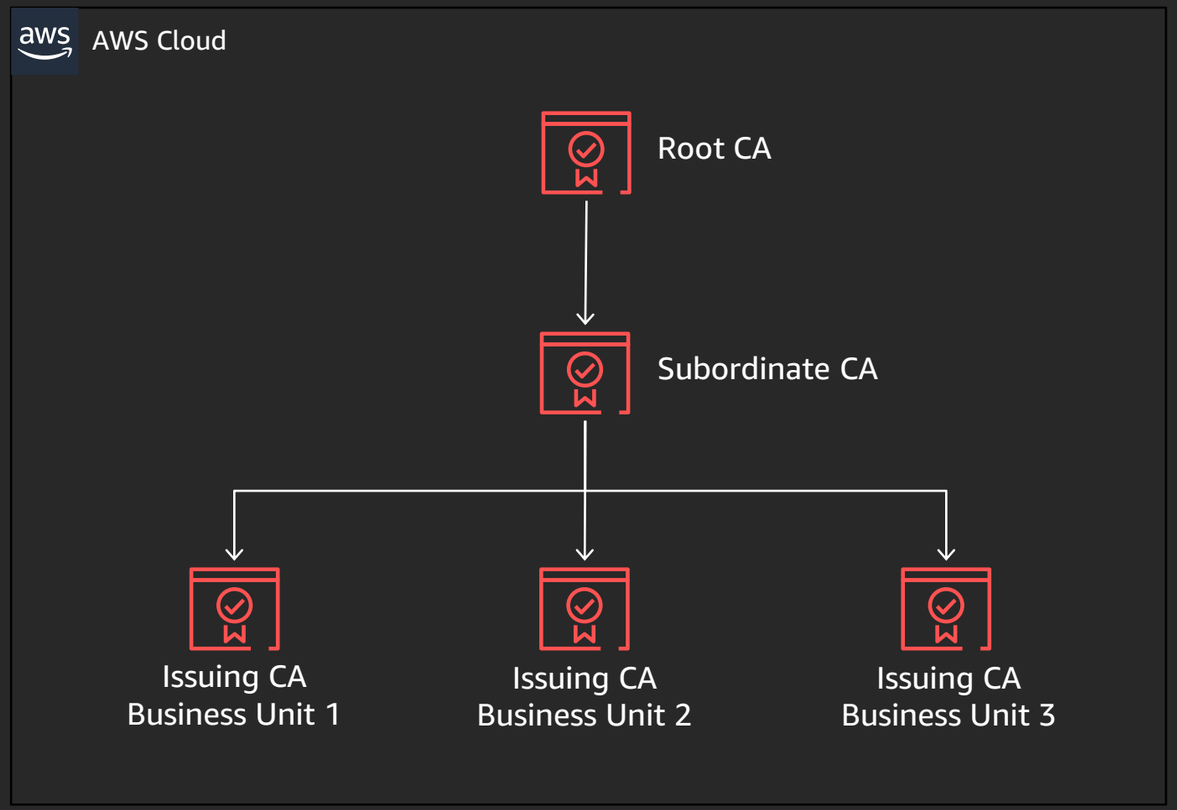
Can I afford it?
What happens in this scenario?

# Hierarchy Design

## Manufacturing Line




## E-Commerce



# Thank you!

**Ram Ramani**

ramanira@amazon.com

AWS re:Invent



aws

# Please complete the session survey in the mobile app.