

AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC330-R

Harness the power of temporary credentials with IAM Roles Anywhere

Liam Wadman

Solutions Architect, Identity
AWS

Mohamed Keshk

Sr. Product Manager,
Cryptography
AWS

Robert Alcorn (Bob)

Sr. Software Development
Engineer, Cryptography
AWS



What we'll talk about

- What is IAM Roles Anywhere?
- Why/when IAM Roles Anywhere?
- IAM Roles Anywhere in depth
- Best practices

Introducing IAM Roles Anywhere

EXTENDS THE USE OF IAM ROLES TO WORKLOADS OUTSIDE OF AWS

IAM Roles Anywhere



Use **temporary AWS credentials** for workloads outside of AWS using **X.509 certificates** issued by your **Public Key Infrastructure (PKI)**

Allow your **workloads** that run **outside of AWS** to access AWS resources

Use **IAM roles and policies** to access AWS resources

Reduce the **undifferentiated heavy lifting** of accessing AWS from workloads that are outside of AWS

Why should you use IAM Roles Anywhere?



Secure

Obtain temporary AWS credentials; move away from long-term credentials



Reduce ops costs and complexity

No additional charge, no re-factoring required

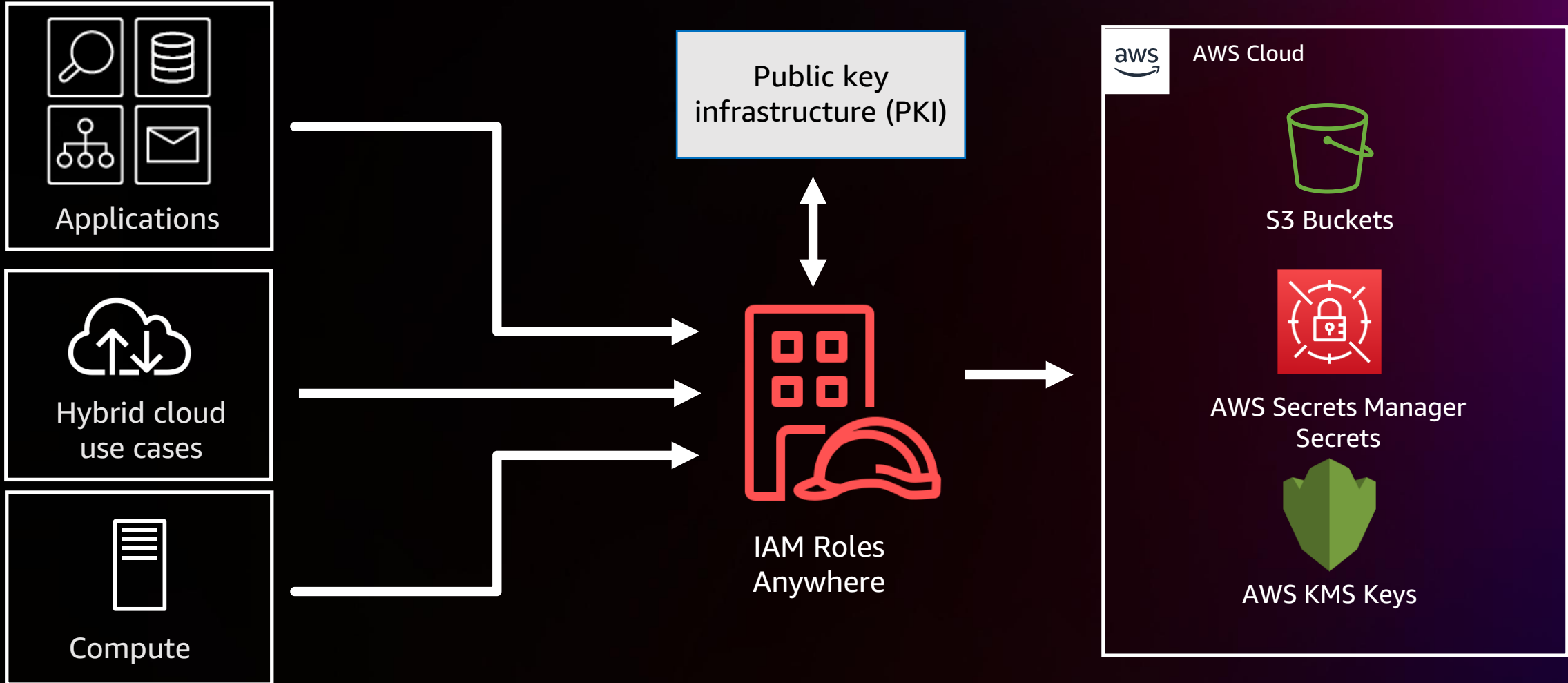


Use AWS services, anywhere

On premises, hybrid cloud, collocated, cross-AWS partition

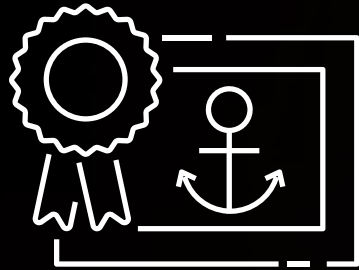
IAM Roles Anywhere in use

Outside of AWS



How IAM Roles Anywhere works in AWS

Step 1: Establish trust



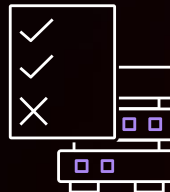
Create trust anchor

Upload your issuing or root Certificate Authority

Step 2: Configure roles

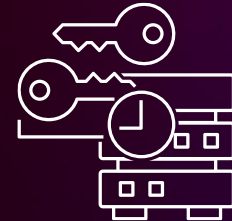


Create roles/modify roles to use IAM Roles Anywhere



Create a profile for your roles

Step 3: Use IAM Roles Anywhere



Request temporary credentials

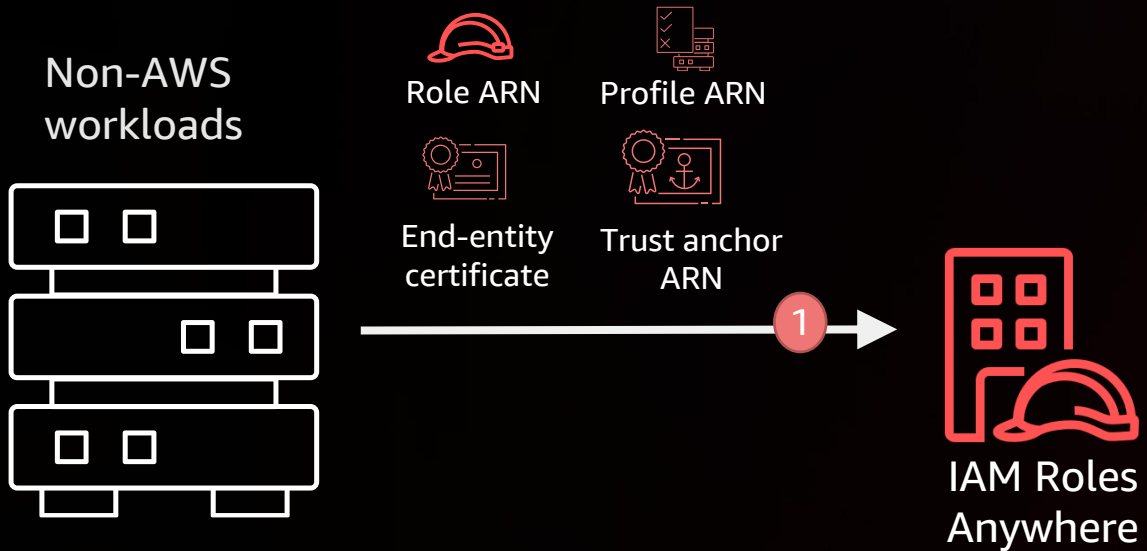
How IAM Roles Anywhere uses your PKI



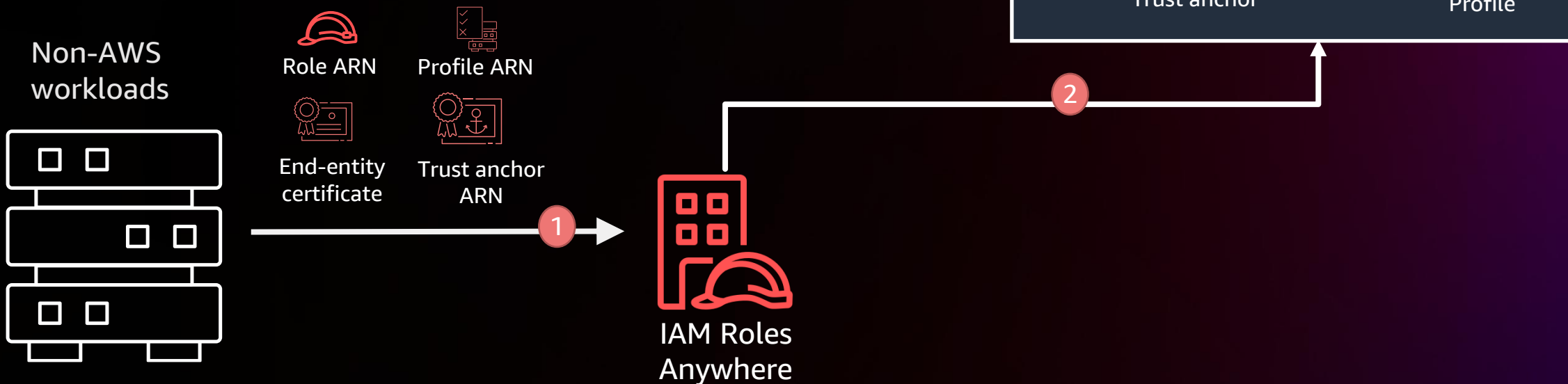
Dive deep into IAM Roles Anywhere



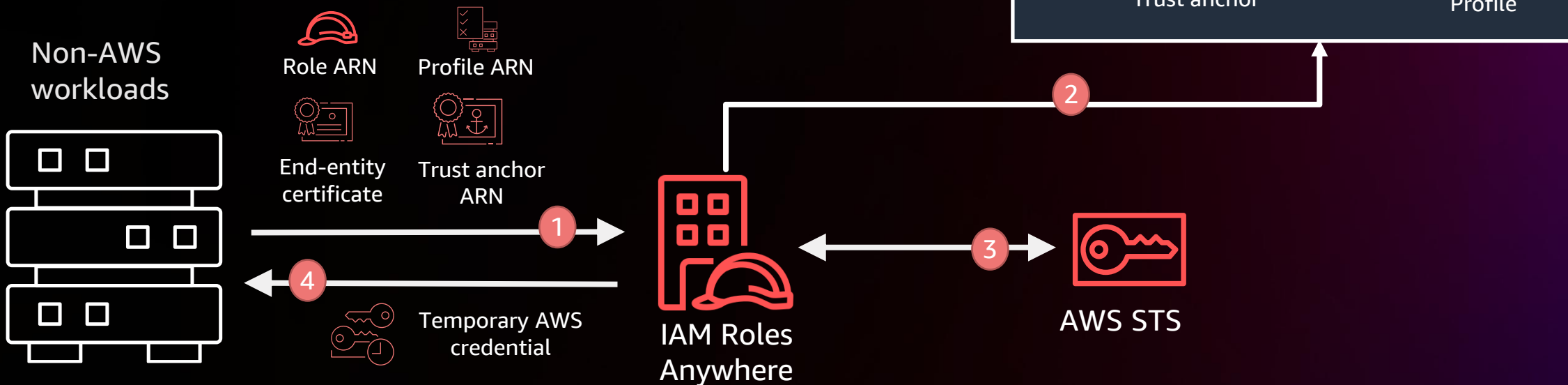
IAM Roles Anywhere in-action



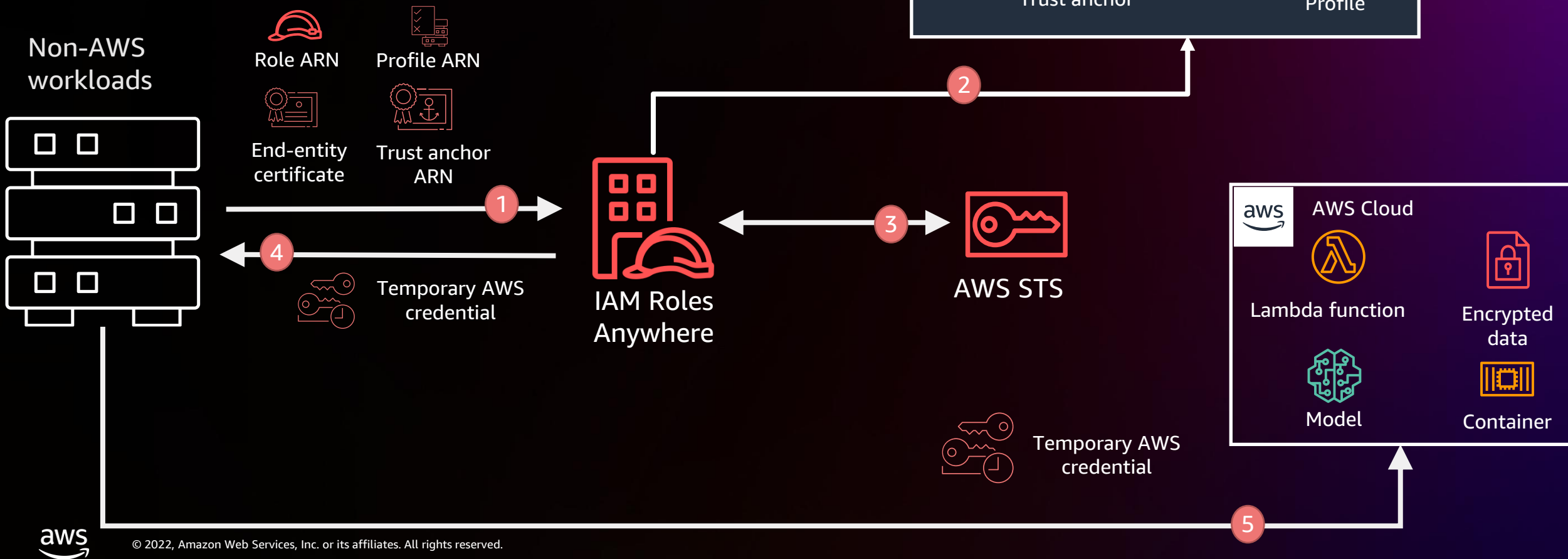
IAM Roles Anywhere



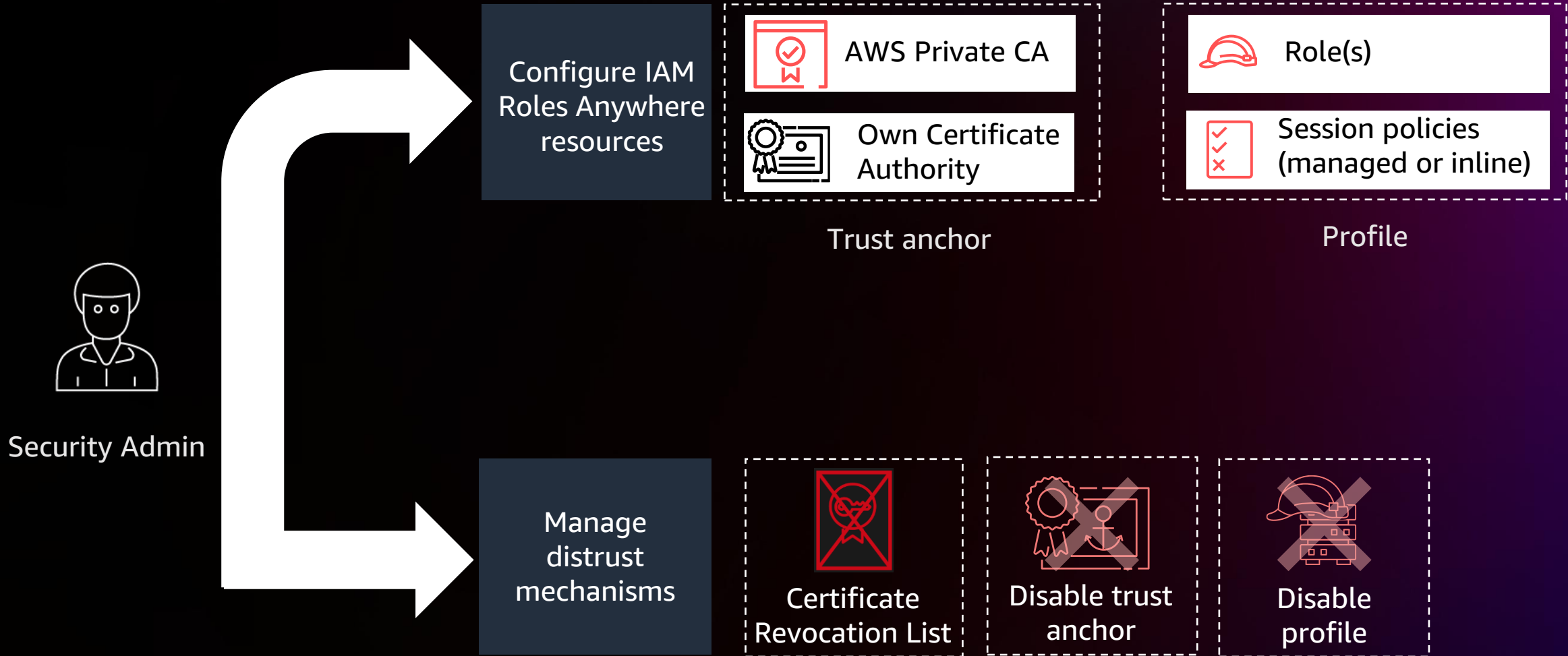
IAM Roles Anywhere in-action



IAM Roles Anywhere in-action



Persona: Security Administrator



Persona: Certificate Issuer



Certificate
Issuer

1

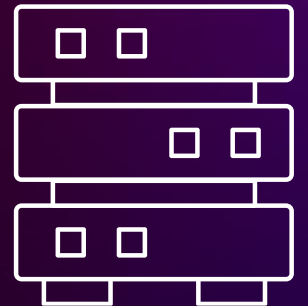
**Generates a
private key and
CSR**

2

**Issues a new end-
entity certificate
from the CA**

3

**Attaches the end-
entity certificate
to the workload**

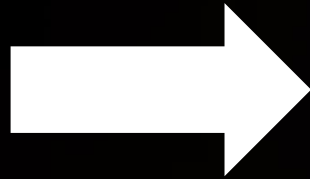


Workload

Persona: Developer



Developer



Configure
workload to
obtain temp
credential

Public end-entity
certificate

Trust anchor ARN

Intermediate
certificate(s)

Profile ARN

Private key

Roles ARN


Subject activity

IAM > Roles > Roles Anywhere > Subject: f19148fd-8aec-4c7c-a5e7-f05cfc3ef8ea

f19148fd-8aec-4c7c-a5e7-f05cfc3ef8ea [Info](#)

Subject details

Subject ID

 f19148fd-8aec-4c7c-a5e7-f05cfc3ef8ea

ARN

 arn:aws:rolesanywhere:us-west-2: :subject/f19148fd-8aec-4c7c-a5e7-f05cfc3ef8ea

Subject

CN=Bob,OU=RolesAnywhere,O=ENG,L=Seattle,ST=WA,C=US

Created at

October 01, 2022, 15:19 (UTC-07:00)

Last used






8 minutes ago

Certificates (5)

Up to 50 of the certificates most recently used for authentication with Roles Anywhere are displayed here.

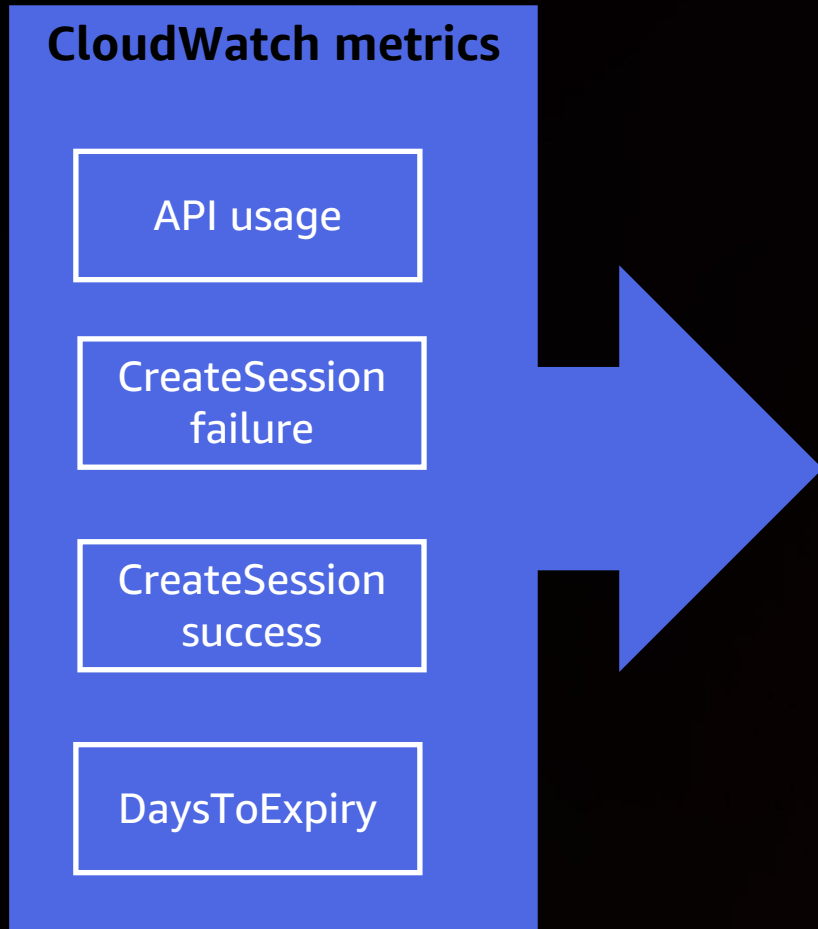


< 1 > 

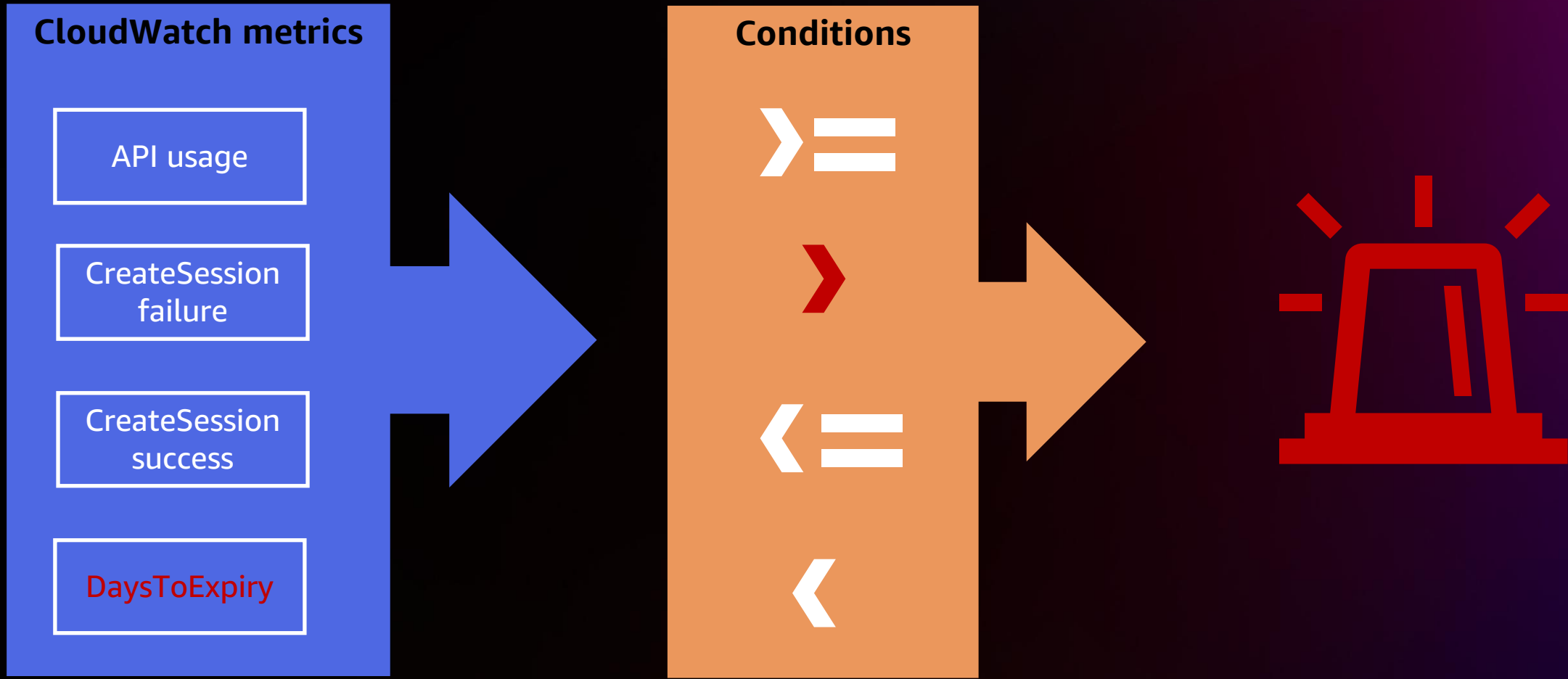
Serial number	Authentication status	Last seen
272870673980797313479151038407433711529	 Failed	8 minutes ago
272870673980797313479151038407433711529	 Success	8 minutes ago
272870673980797313479151038407433711529	 Success	8 minutes ago
272870673980797313479151038407433711529	 Success	8 minutes ago
272870673980797313479151038407433711529	 Success	8 minutes ago



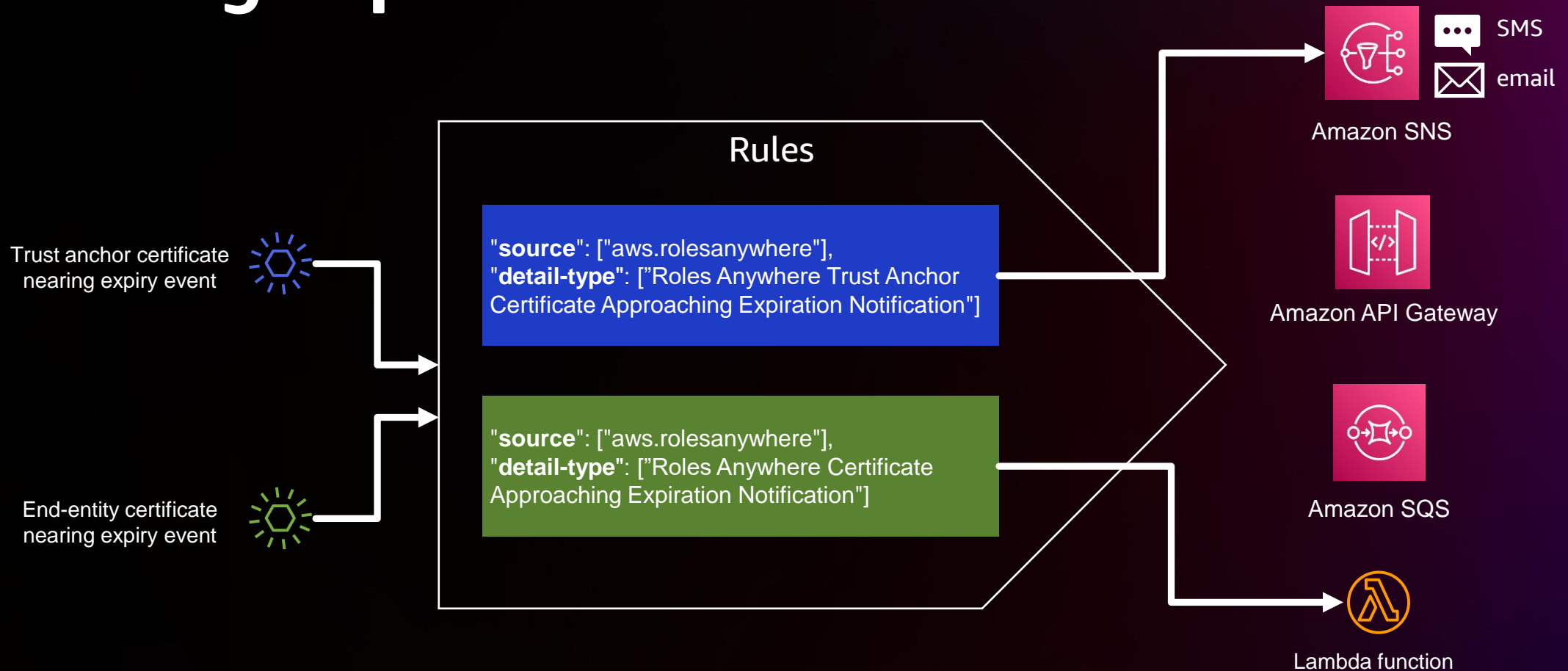
Monitor IAM Roles Anywhere resources using Amazon CloudWatch



Monitor IAM Roles Anywhere resources using Amazon CloudWatch



Receive a notification when certificate is nearing expiration



AWS CloudTrail: PutObject

```
{
  ...
  "userIdentity": {
    "type": "AssumedRole",
    "arn": "arn:aws:sts::111122223333:assumed-role/roleReInvent2022/00cd48faee27f96eb0b4fcac79a142efa9",
    "accountId": "111122223333",
    "SessionContext": {
      "sourceIdentity": "CN=Bob"  },
    ...
  },
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-west-2",
  "requestParameters": {
    "bucketName": "myreinvent2022bucket",
    "Host": "myreinvent2022bucket.s3.us-west-2.amazonaws.com",
    "key": "object.pdf"},
  ...
}
```

AWS CloudTrail: PutObject

```
{
  ...
  "userIdentity": {
    "type": "AssumedRole",
    "arn": "arn:aws:sts::111122223333:assumed-role/roleReInvent2022/00cd48faee27f96eb0b4fcac79a142efa9",
    "accountId": "111122223333",
    "SessionContext": {
      "sourceIdentity": "CN=Bob" },
    ...
  },
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-west-2",
  "requestParameters": {
    "bucketName": "myreinvent2022bucket",
    "Host": "myreinvent2022bucket.s3.us-west-2.amazonaws.com",
    "key": "object.pdf" },
  ...
}
```

sourceIdentity =
Certificate subject
common name

AWS CloudTrail: PutObject

```
{
  ...
  "userIdentity": {
    "type": "AssumedRole",
    "arn": "arn:aws:sts::111122223333:assumed-role/roleReInvent2022/00cd48faee27f96eb0b4fcac79a142efa9",
    "accountId": "111122223333",
    "SessionContext": {
      "sourceIdentity": "CN=Bob" },
    ...
  },
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-west-2",
  "requestParameters": {
    "bucketName": "myreinvent2022bucket",
    "Host": "myreinvent2022bucket.s3.us-west-2.amazonaws.com",
    "key": "object.pdf"},
  ...
}
```

role-session-name =
HEX{CERT_SERIAL_NUMBER}

Identity-based policy: AllowRolesAnywhereActions

```
{ "Statement": [  
  {  
    "Sid": "AllowRolesAnywhereActions",  
    "Effect": "Allow",  
    "Action": "rolesanywhere:${ACTION}",  
    "Resource": "arn:aws:rolesanywhere::${accountId}:${RESOURCE/RESOURCE_ID}",  
  }  
]}
```

ACTION:

Create
Update
List
Get
Enable
Disable
Delete
...

TrustAnchor
Profile

RESOURCE/RESOURCE_ID:

trust-anchor/\${TrustAnchorId}
profile/\${ProfileId}
cr1/\${Cr1Id}
subject/\${SubjectId}

Assume role policy document

```
{
  "Statement": [
    {
      "Sid": "TrustPolicyWorkloadRole",
      "Effect": "Allow",
      "Principal": { "Service": "rolesanywhere.amazonaws.com" },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:PrincipalTag/x509Subject/OU": "Eng"
        }
      }
    }
  ]
}
```

- ❖ SourceIdentity
- ❖ PrincipalTag
 - x509SAN/[URI or DNS or Name/\${RDN}]
 - x509Subject/\${RDN or OID}
 - x509Issuer/\${RDN or OID}

Resource-based policy: S3 bucket

```
{
  "Statement": [
    {
      "Sid": "S3Bucket",
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::reinvent-2022-bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalTag/x509Subject/CN": "Bob"
        }
      }
    }
  ]
}
```

Best practices



Do implement fine-grained authorization in role trust policies

```
{  
  "Effect": "Allow",  
  ...,  
  "Condition": {  
    "StringEquals": {  
      "aws:PrincipalTag/x509Subject/CN": "liwadman@amazon.com"  
    }  
  }  
}
```



Manage the validity period of certificates issued by your PKI

Not Valid Before Monday, October 3, 2022 at 12:11:01 Pacific Daylight Saving Time
Not Valid After Friday, December 20, 2030 at 12:11:01 Pacific Standard Time

Safeguard admin actions

```
{  
  "Effect": "Allow",  
  "Action": [  
    "rolesanywhere:DisableTrustAnchor",  
    "rolesanywhere>CreateTrustAnchor",  
    "rolesanywhere:UpdateTrustAnchor"  
  ],  
  "Resource": "*"   
}
```



Manage trust anchor expiry with blue/green deployment

Trust anchors (2) [Info](#)

A trust anchor refers to the trust relationship between Roles Anywhere and your Certificate Authority (CA).

Certificates are used to authenticate against the trust anchor to obtain credentials for an IAM role. You can create a profile to customize what authenticated workloads can do with the role.

 *Filter trust anchors*

	Name	Trust anchor ID
<input type="radio"/>	Green_Trust_Anchor	a623bd55-b0fd-4436-b3d8-427937553454
<input type="radio"/>	Blue_Trust_Anchor	99dde101-e27d-4eef-a45f-c4175ae7f04c

Identity best practices

Create new IAM roles for use with IAM Roles Anywhere



Identity best practices

Create new IAM roles for use with IAM Roles Anywhere



Use different IAM roles for all your workloads



Identity best practices

Create new IAM roles for use with IAM Roles Anywhere



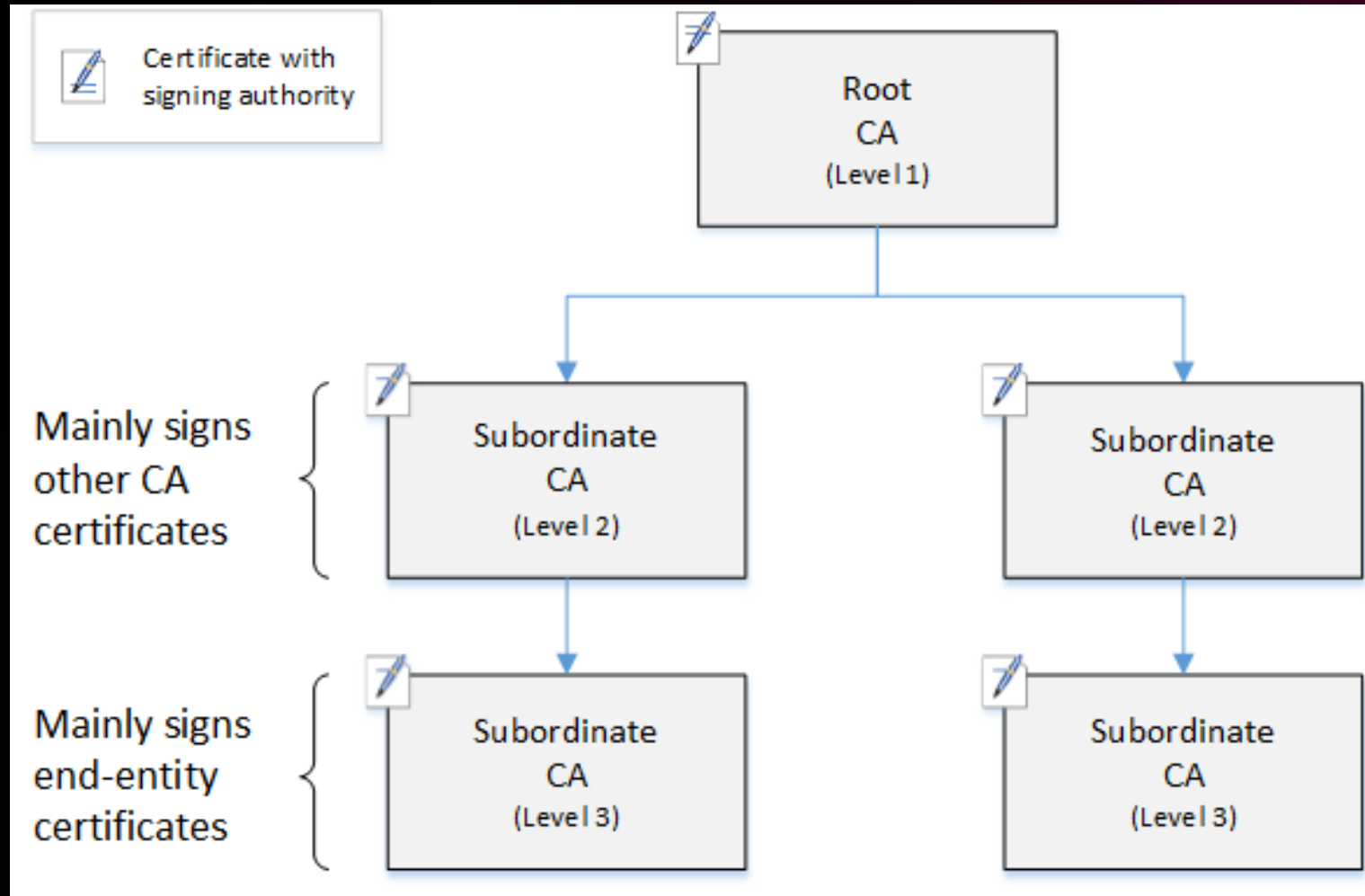
Use different IAM roles for all your workloads



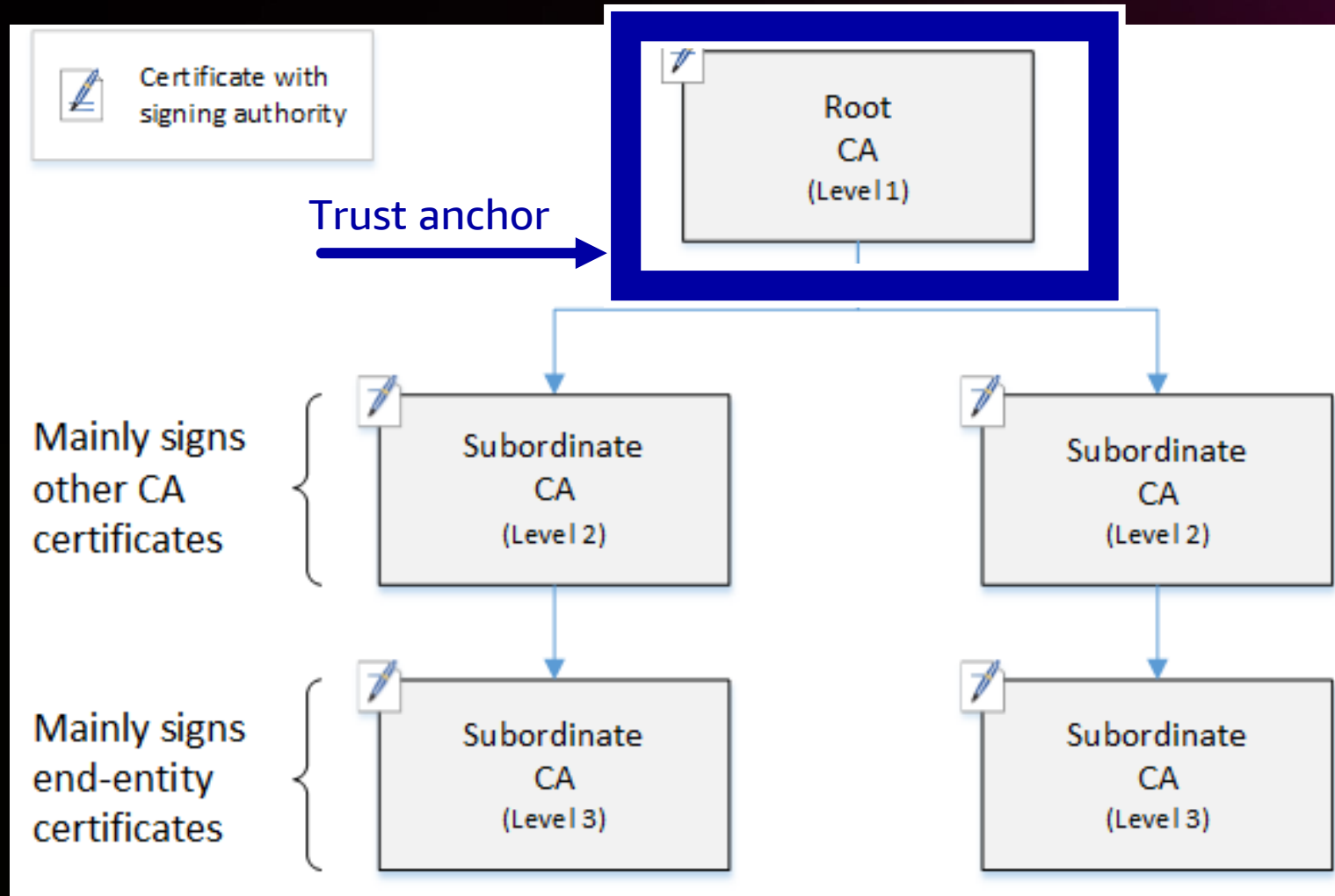
Issue certificates to each instance of a workload



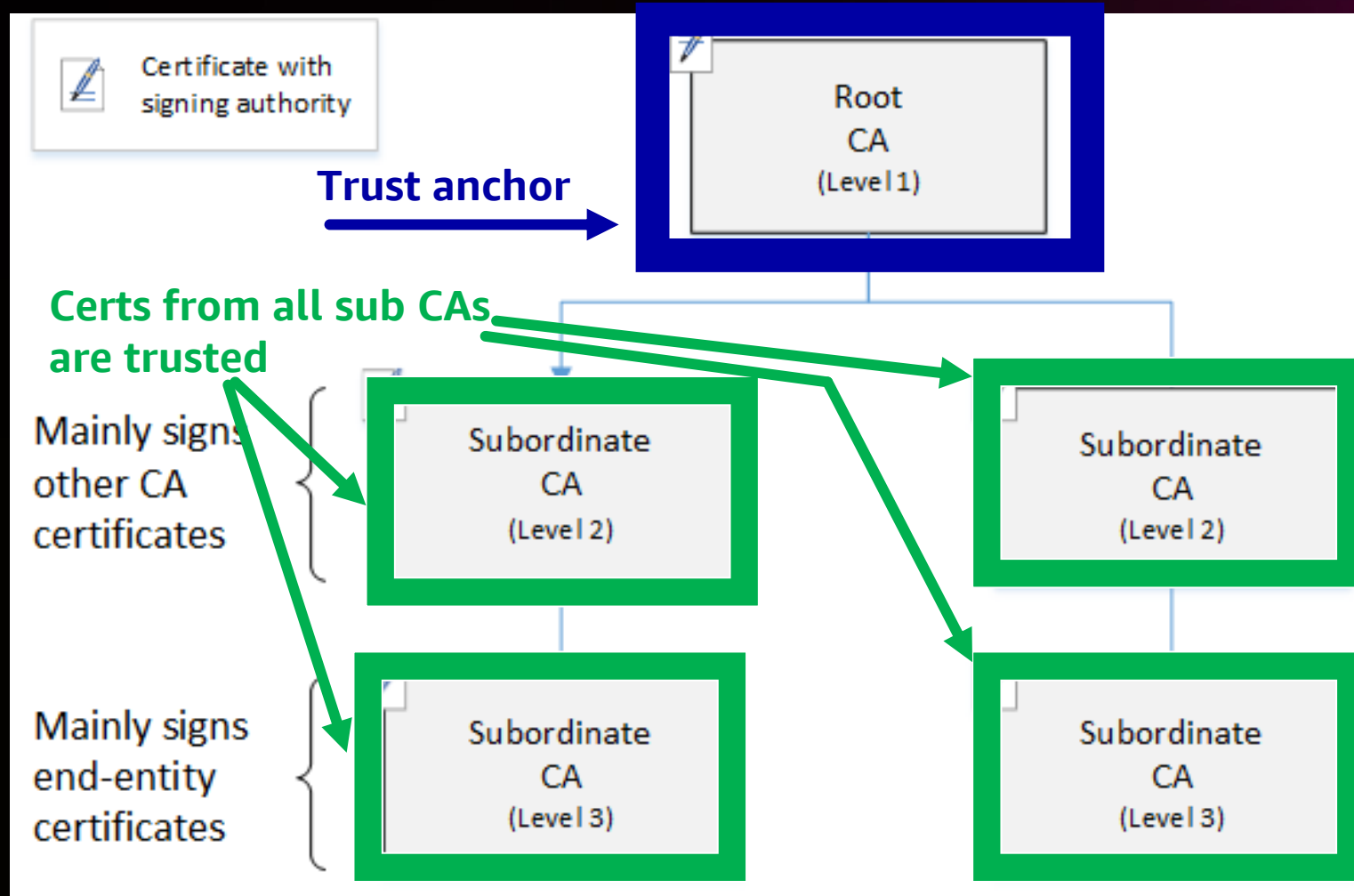
Plan your trust anchor placement within your PKI



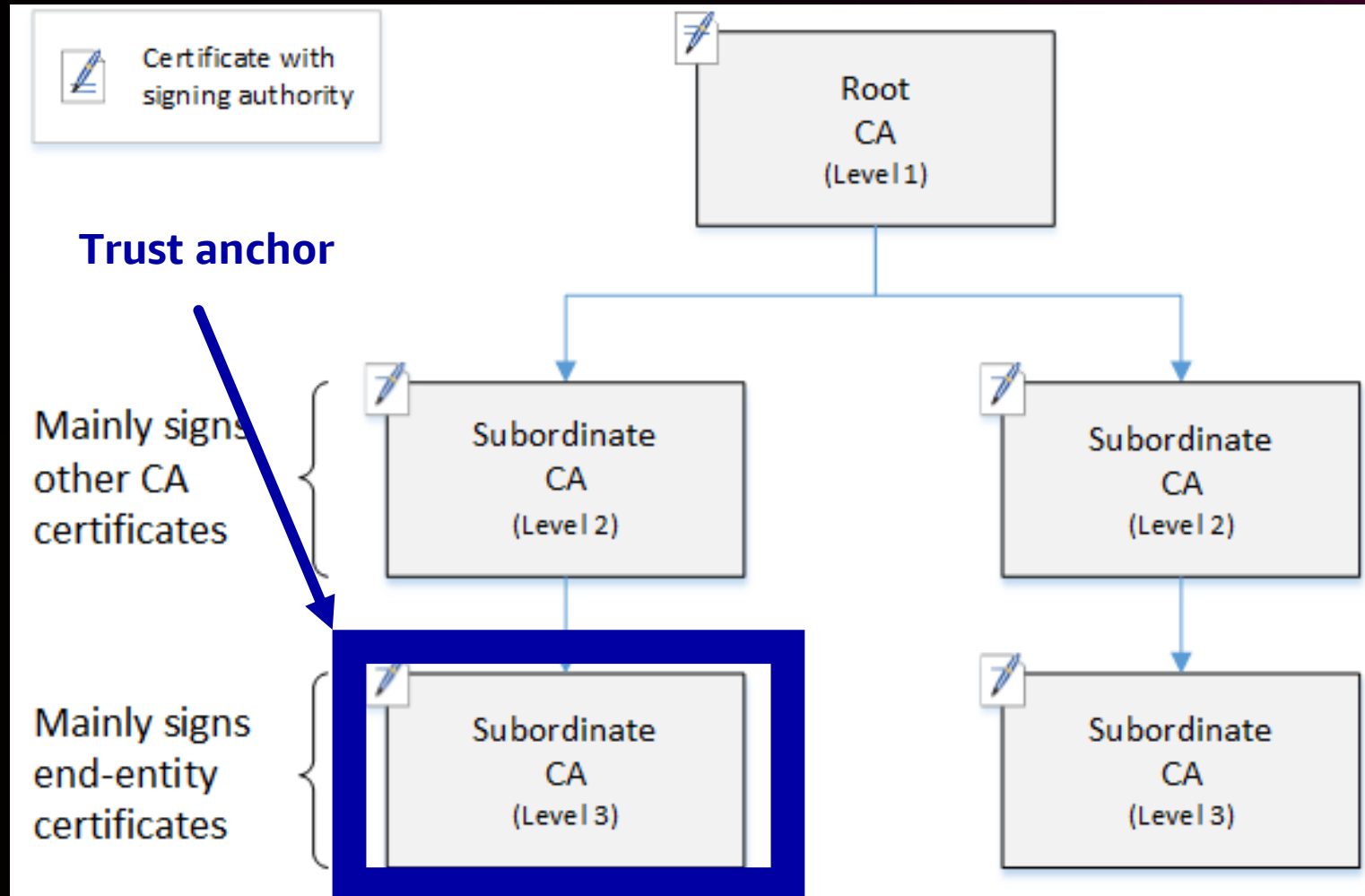
Plan your trust anchor placement within your PKI



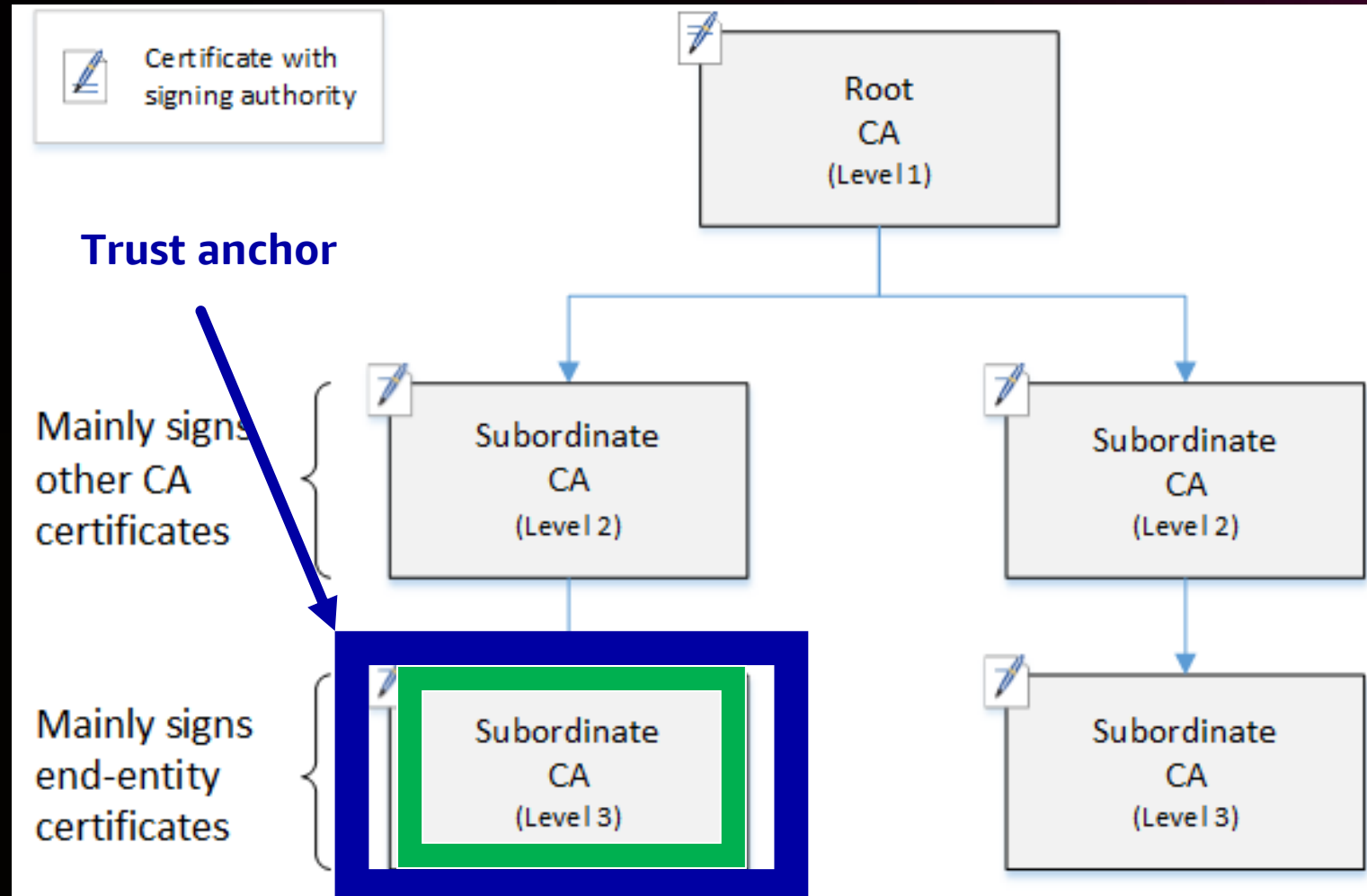
Plan your trust anchor placement within your PKI



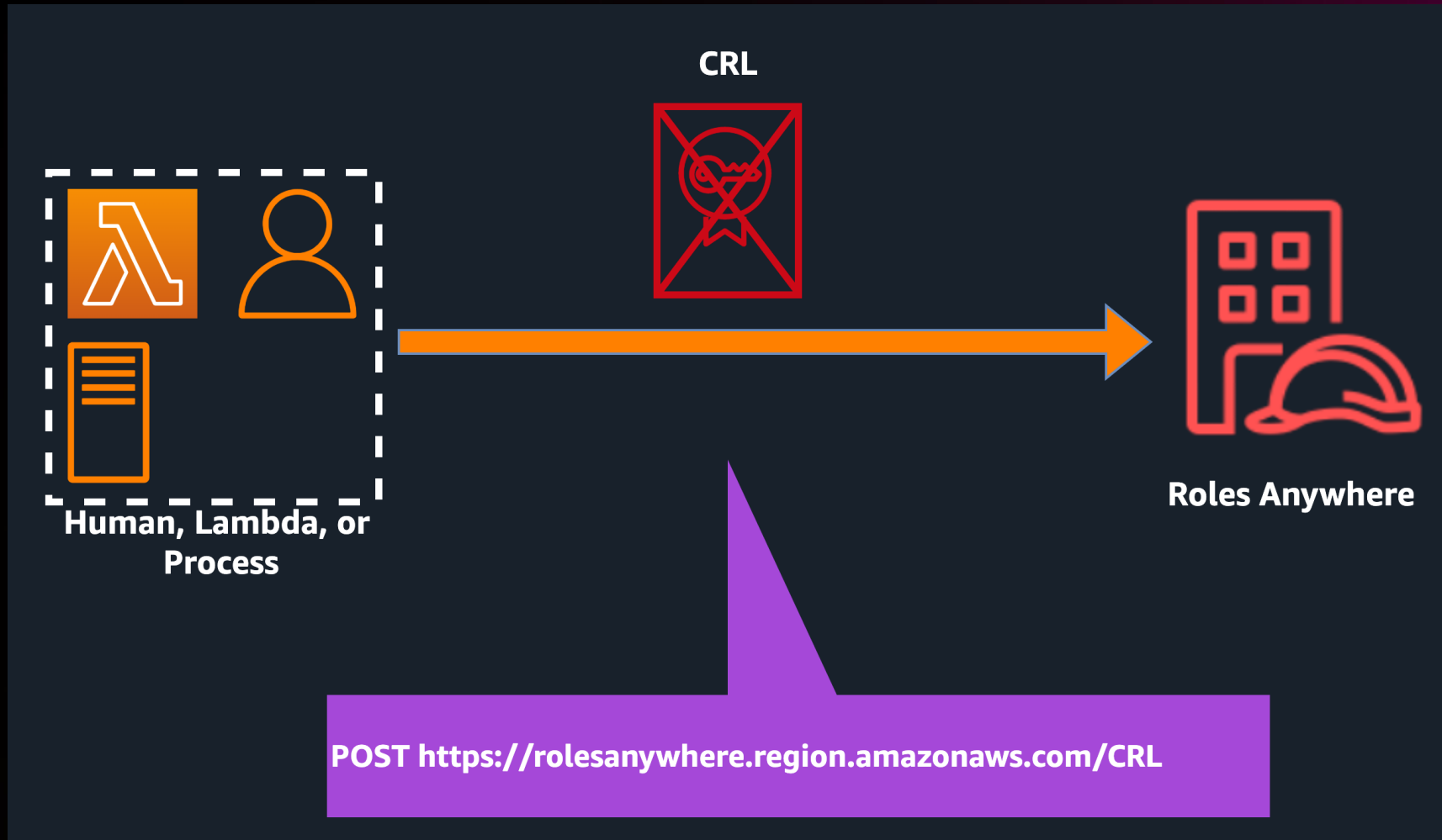
Plan your trust anchor placement within your PKI



Plan your trust anchor placement within your PKI



Push Updates to your CRL



Additional resources



User guide



Technical blog



API reference guide



**Data Protection for Hybrid
Workloads Workshop**



Credential helper GitHub

Thank you!

Liam Wadman

liwadman@amazon.com

Mohamed Keshk

keshkmoh@amazon.com

Robert Alcorn (Bob)

rlalcorn@amazon.com



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



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