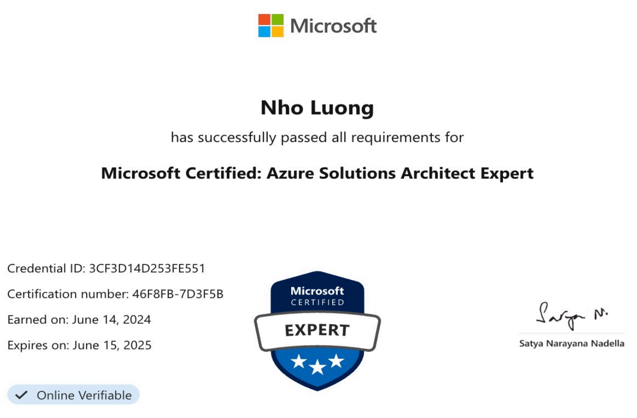
# Kubernetes Ochestration

Author: Nho Luong

Skill: DevOps Engineer Lead



Microsoft

**Nho Luong**

has successfully passed all requirements for

**Microsoft Certified: Azure Solutions Architect Expert**

Credential ID: 3CF3D14D253FE551

Certification number: 46F8FB-7D3F5B

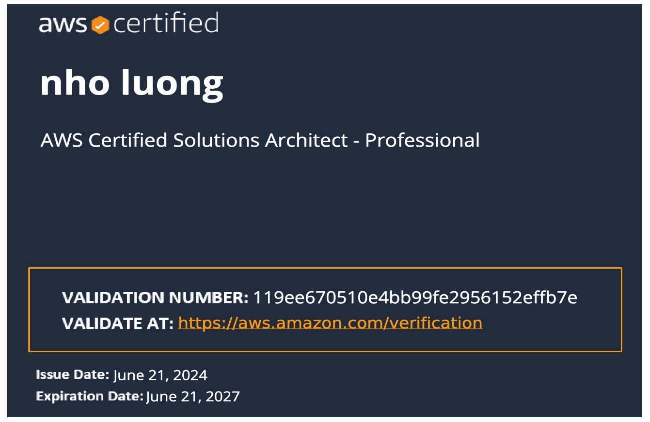
Earned on: June 14, 2024

Expires on: June 15, 2025

✓ Online Verifiable

Satya Narayana Nadella

Microsoft CERTIFIED
EXPERT



aws certified

**nho luong**

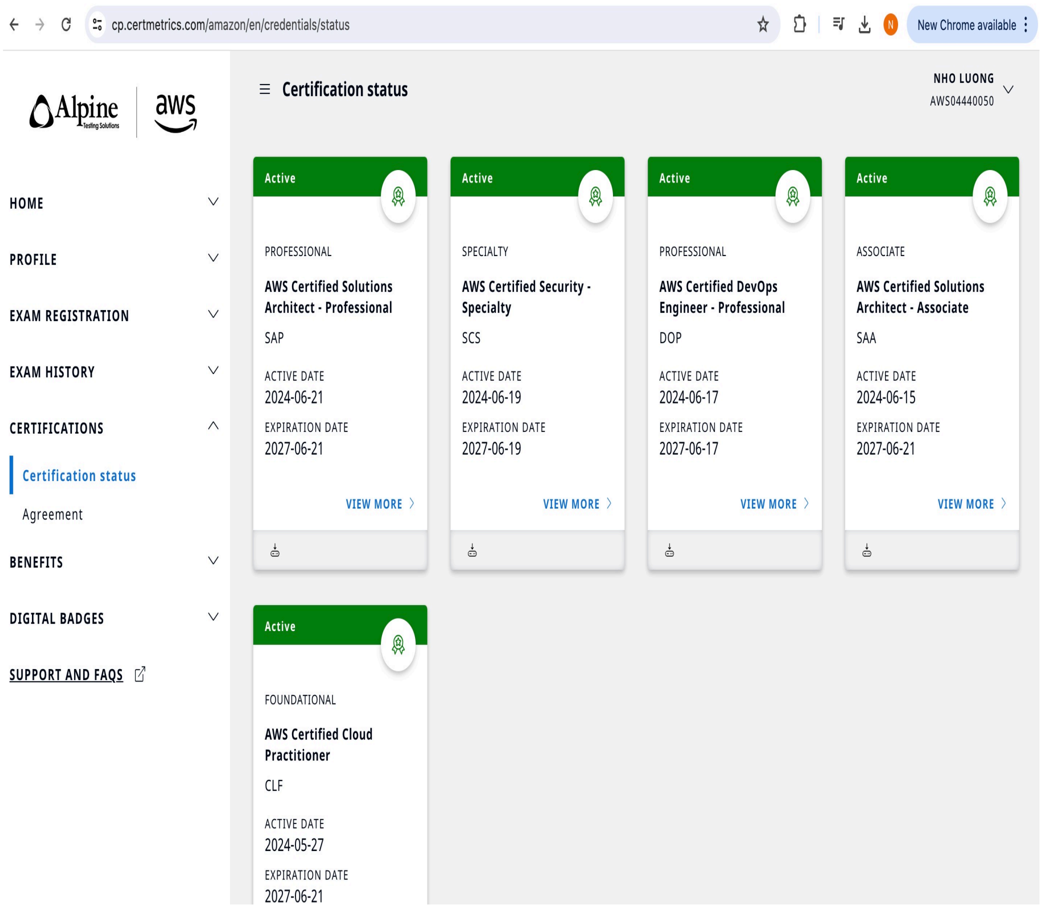
AWS Certified Solutions Architect - Professional

**VALIDATION NUMBER:** 119ee670510e4bb99fe2956152effb7e

**VALIDATE AT:** https://aws.amazon.com/verification

**Issue Date:** June 21, 2024

**Expiration Date:** June 21, 2027



cp.certmetrics.com/amazon/en/credentials/status

Certification status

NHO LUONG
AWS04440050

Active

PROFESSIONAL

AWS Certified Solutions Architect - Professional

SAP

ACTIVE DATE
2024-06-21

EXPIRATION DATE
2027-06-21

VIEW MORE

Active

SPECIALTY

AWS Certified Security - Specialty

SCS

ACTIVE DATE
2024-06-19

EXPIRATION DATE
2027-06-19

VIEW MORE

Active

PROFESSIONAL

AWS Certified DevOps Engineer - Professional

DOP

ACTIVE DATE
2024-06-17

EXPIRATION DATE
2027-06-17

VIEW MORE

Active

ASSOCIATE

AWS Certified Solutions Architect - Associate

SAA

ACTIVE DATE
2024-06-15

EXPIRATION DATE
2027-06-21

VIEW MORE

Active

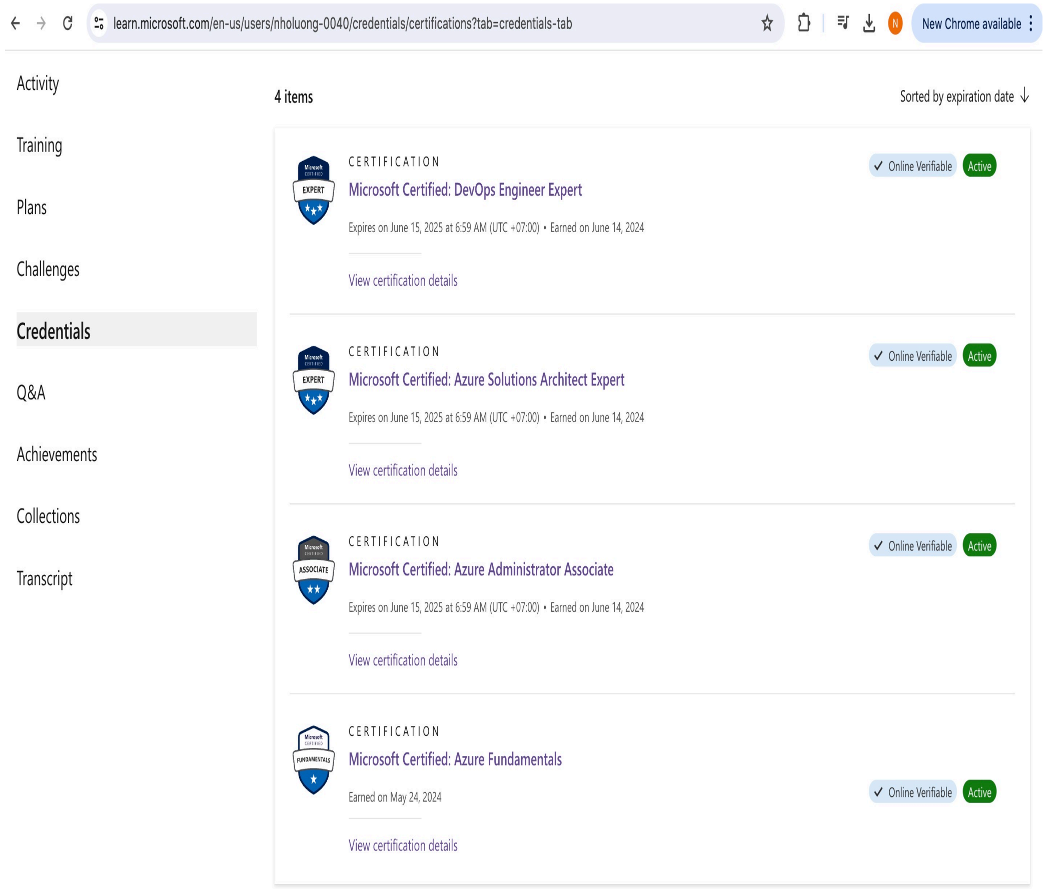
FOUNDATIONAL

AWS Certified Cloud Practitioner

CLF

ACTIVE DATE
2024-05-27

EXPIRATION DATE
2027-06-21



learn.microsoft.com/en-us/users/nholuong-0040/credentials/certifications?tab=credentials-tab

4 items

Sorted by expiration date ↓

CERTIFICATION

Microsoft Certified: DevOps Engineer Expert

✓ Online Verifiable Active

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details

CERTIFICATION

Microsoft Certified: Azure Solutions Architect Expert

✓ Online Verifiable Active

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details

CERTIFICATION

Microsoft Certified: Azure Administrator Associate

✓ Online Verifiable Active

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details

CERTIFICATION

Microsoft Certified: Azure Fundamentals

Earned on May 24, 2024

✓ Online Verifiable Active

View certification details

Security is hard.

Containers are faster,  but less secure?

How do you sign off on a release before it goes to production?

Not who, but what

How do you make sure that only trusted code runs in your production environments?

What about the bad guys?

Author: Nho Luong
Skill: DevOps Engineer Lead

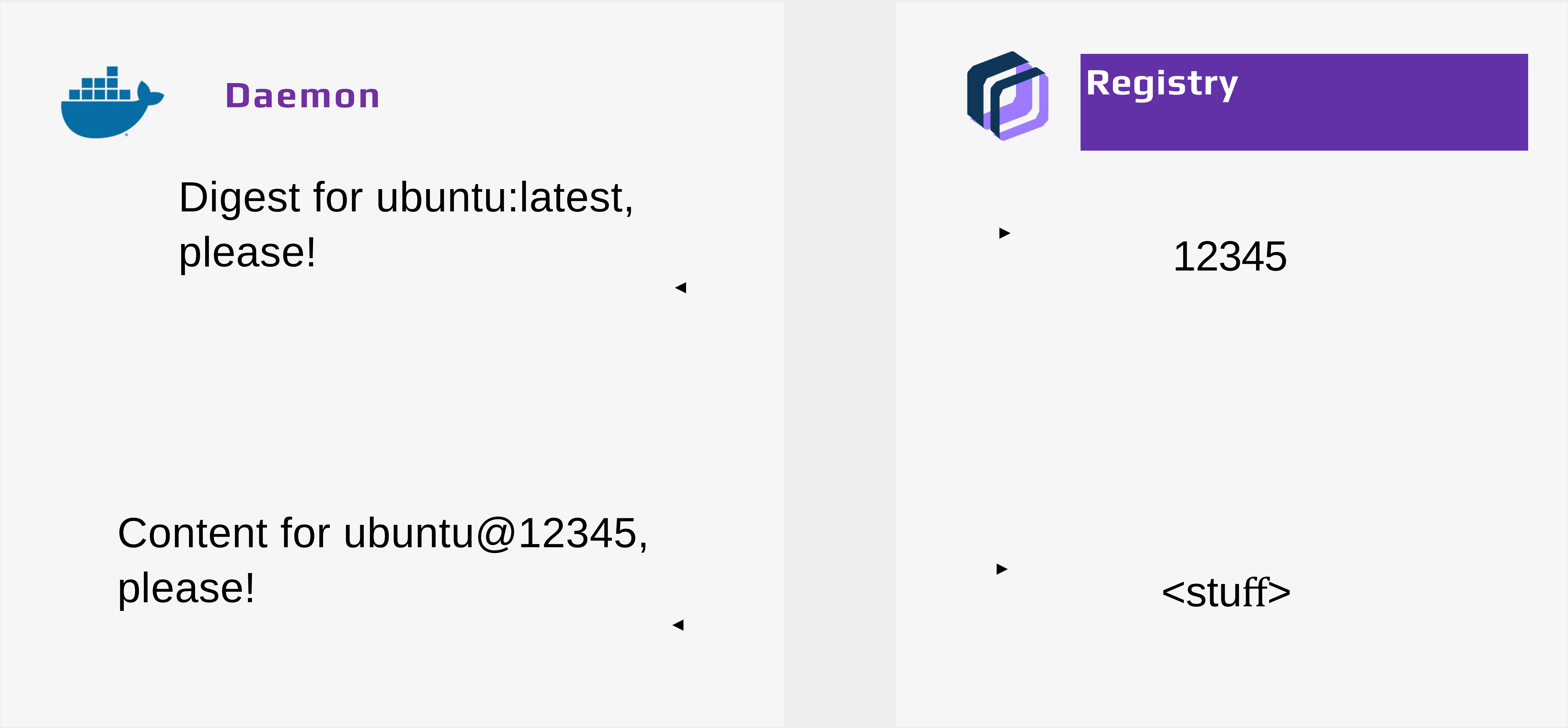
## Digitally sign it!
## But how do you sign a Docker image?

Enter Notary

Implements The Update Framework (TUF) Stores

trusted data ... such as Docker image digests

Author: Nho Luong
Skill: DevOps Engineer Lead



Daemon

Registry

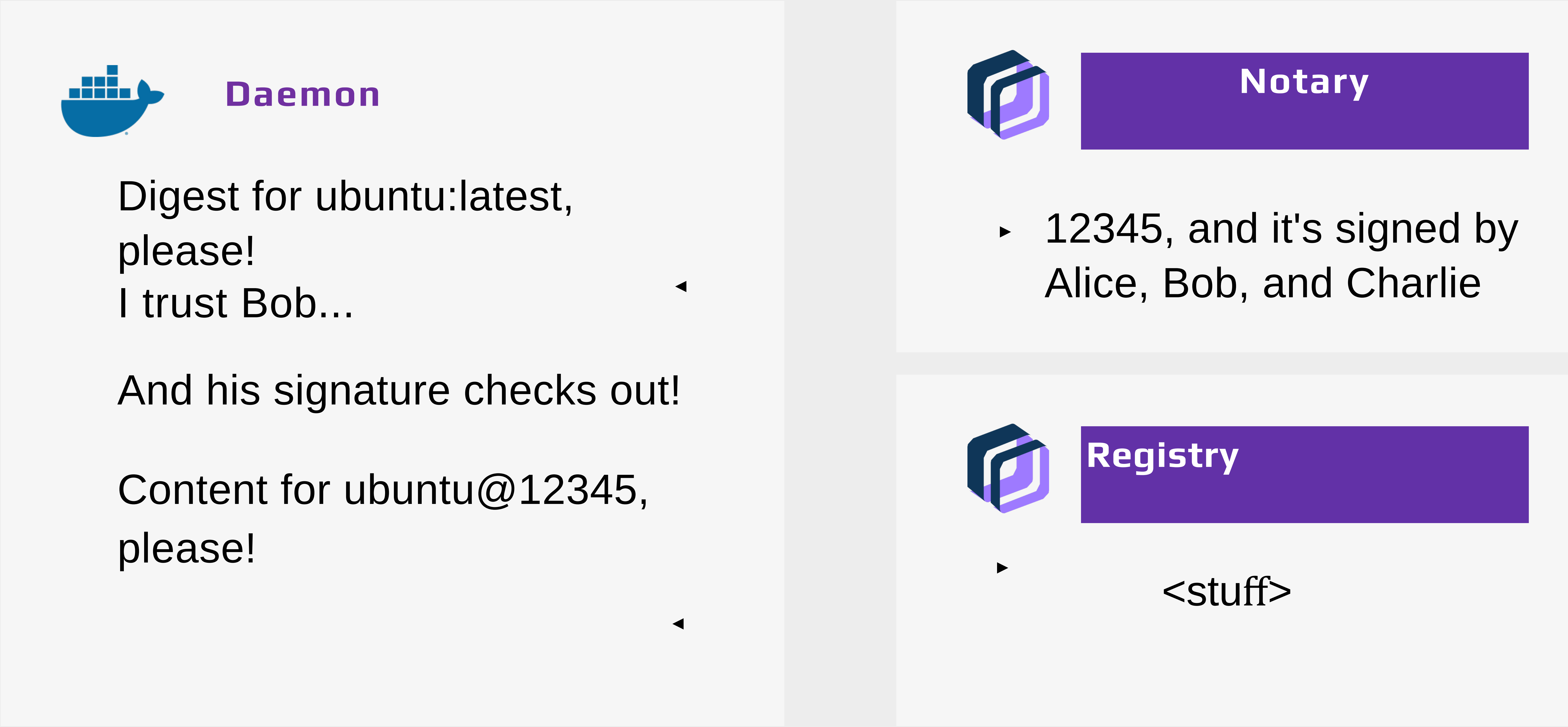
Digest for ubuntu:latest, please!

12345

Content for ubuntu@12345, please!

<stuff>

Author: Nho Luong
Skill: DevOps Engineer Lead



Daemon

Digest for ubuntu:latest, please!
I trust Bob...

And his signature checks out!

Content for ubuntu@12345, please!

Notary

12345, and it's signed by Alice, Bob, and Charlie

Registry

<stuff>

# Why not use Docker Content Trust in your cluster?
# Who else do you trust?
# What about the kubelet images?

Kubernetes deserves powerful trust management

Admission Controllers

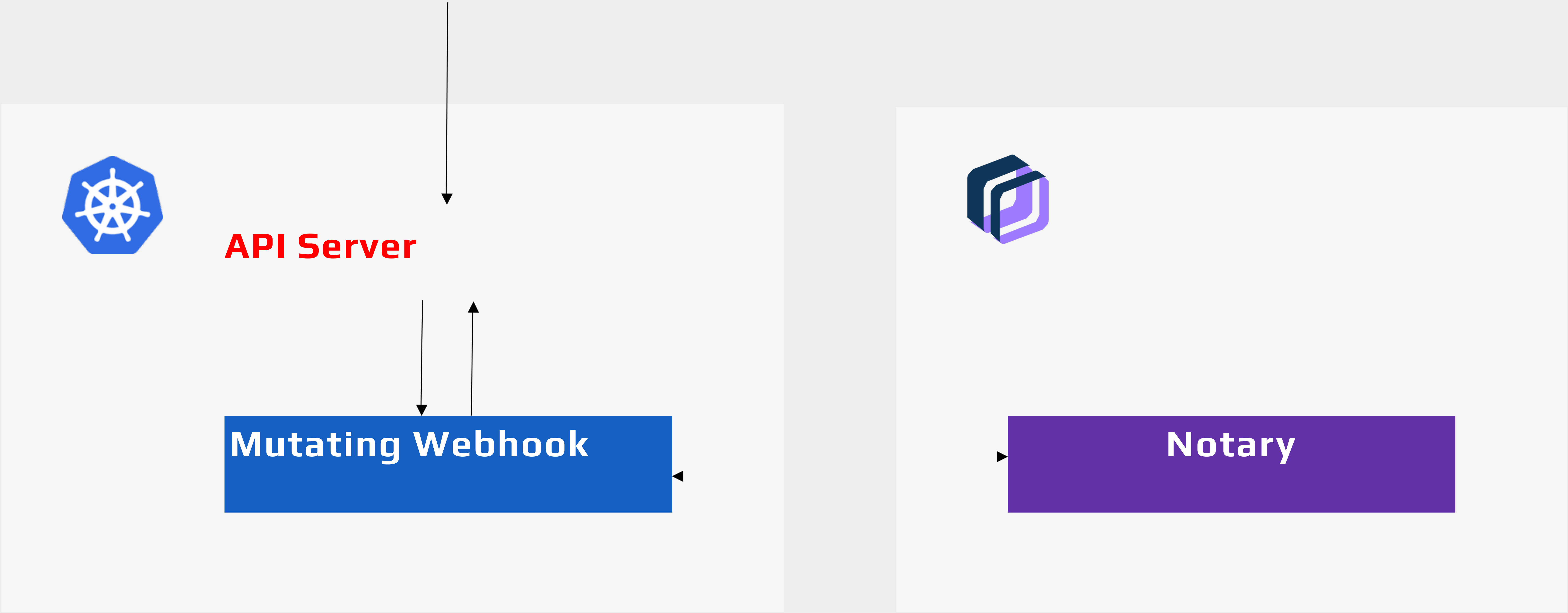
Author: Nho Luong
Skill: DevOps Engineer Lead

# Validating Admission Webhook
# Mutating Admission Webhook

Author: Nho Luong
Skill: DevOps Engineer Lead

```
liamwhite/kubecon@sha256:4bd87a5758f80eedb01335676a9e47347801fc...
```

Author: Nho Luong
Skill: DevOps Engineer Lead



API Server

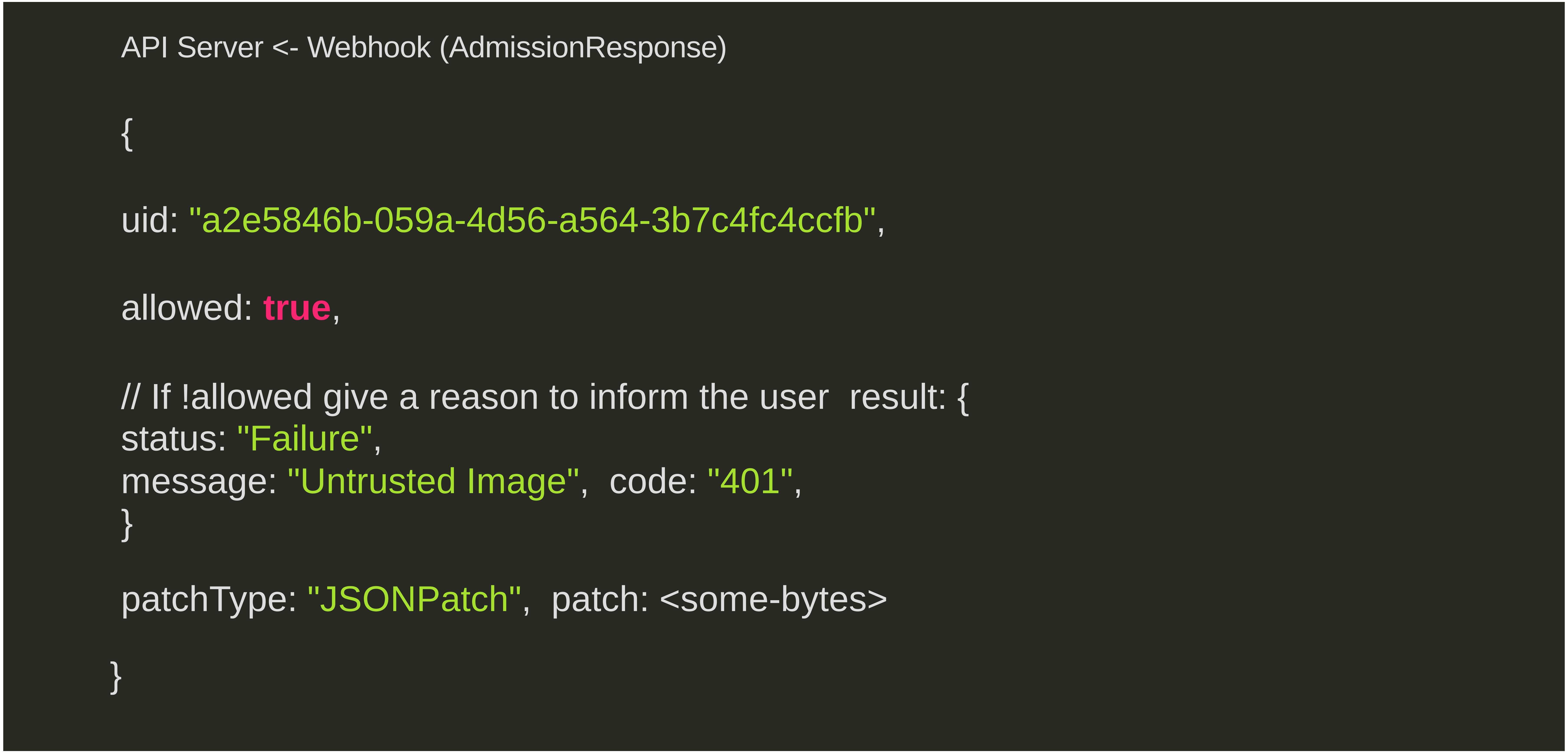
Mutating Webhook

Notary

Author: Nho Luong
Skill: DevOps Engineer Lead

## API Server -> Webhook (AdmissionRequest)

```
{
uid: "a2e5846b-059a-4d56-a564-3b7c4fc4ccfb",

kind: {
group: "",
version: "v1",
kind: "Pod",
},

resource: {
group: "",
version: "v1",  resource: "pods",
},

namespace: "default",  operation: "CREATE",  object: <lots-of-bytes>
}
```



API Server <- Webhook (AdmissionResponse)

```
{

uid: "a2e5846b-059a-4d56-a564-3b7c4fc4ccfb",

allowed: true,

// If !allowed give a reason to inform the user  result: {
status: "Failure",
message: "Untrusted Image",  code: "401",
}

patchType: "JSONPatch",  patch: <some-bytes>

}
```

Author: Nho Luong
Skill: DevOps Engineer Lead

```
API Server <- Webhook (Patch)

{


operation: "replace",

path: "/spec/containers/0/image",

value: "liamwhite/kubecon@sha256:4bd87a5758f80eedb01335676a9e47347801fc",


}
```

# PORTIERIS

github.com/ibm/portieris

Author: Nho Luong
Skill: DevOps Engineer Lead

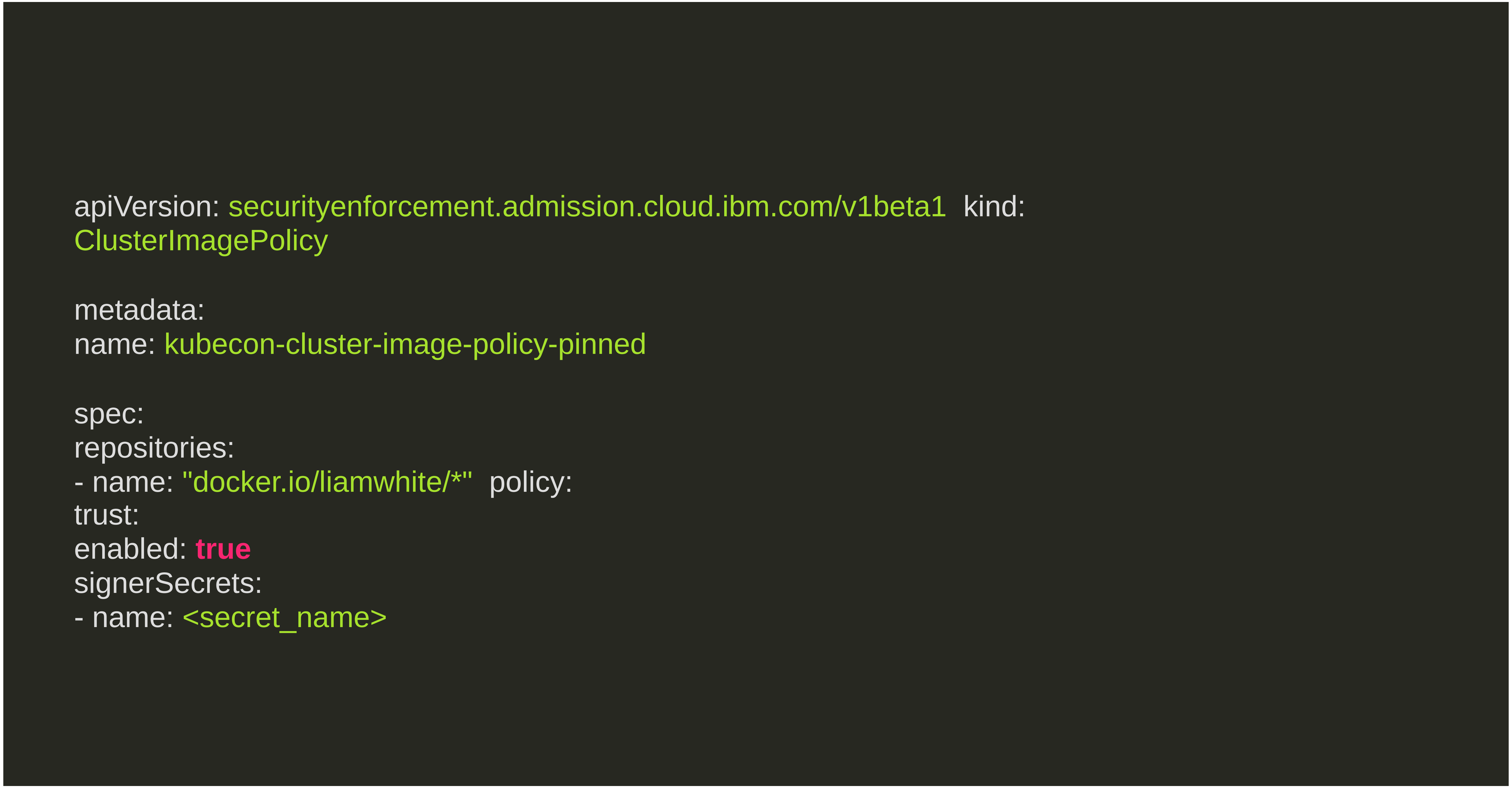
Whitelist Images
Fail Closed

Namespace or Cluster Wide Policies

Extensible

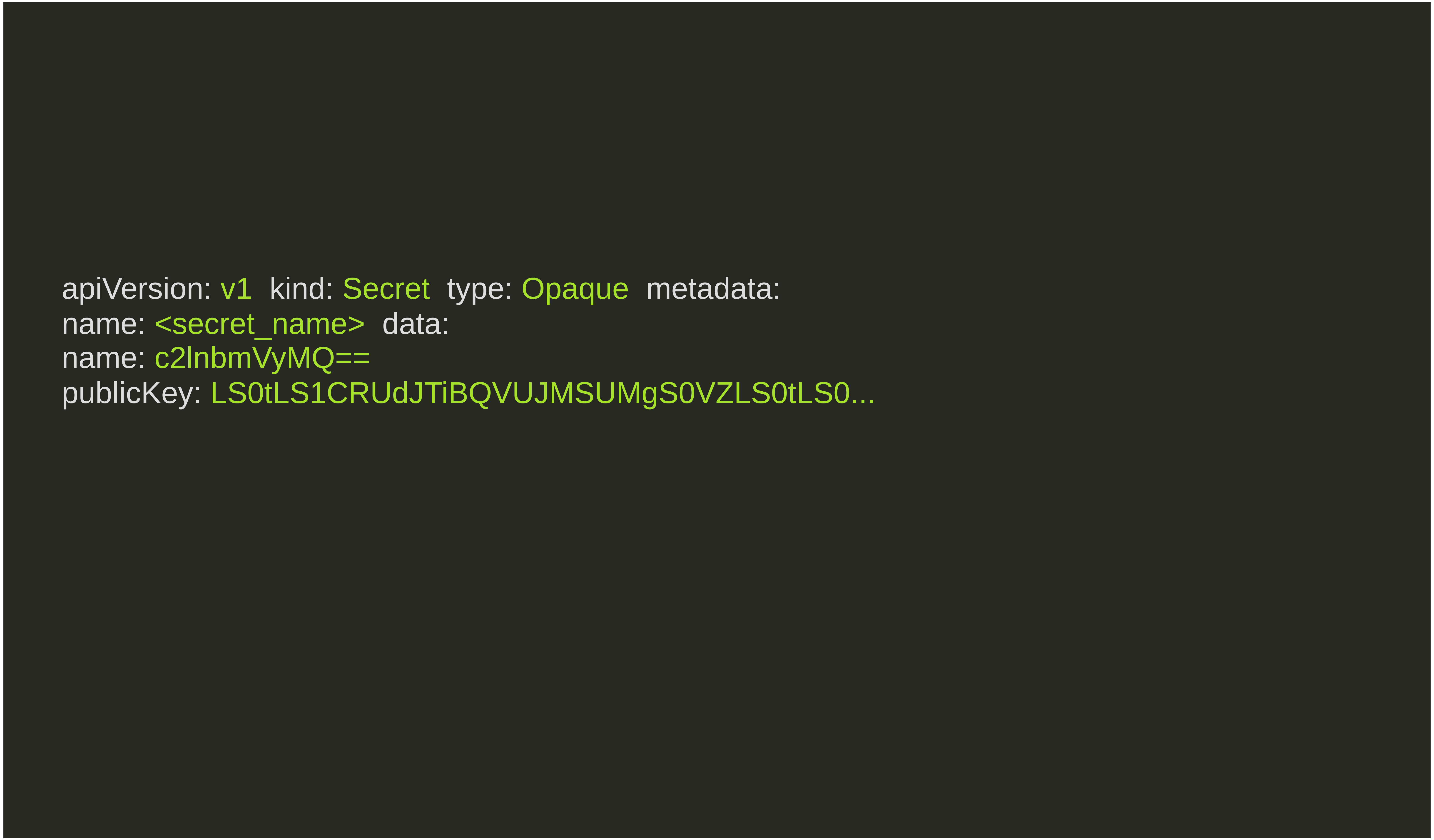
Author: Nho Luong
Skill: DevOps Engineer Lead

```
apiVersion: securityenforcement.admission.cloud.ibm.com/v1beta1  kind:
ClusterImagePolicy

metadata:
name: kubecon-cluster-image-policy

spec:
repositories:
- name: "docker.io/liamwhite/kubecon"  policy:
trust:
enabled: true
```



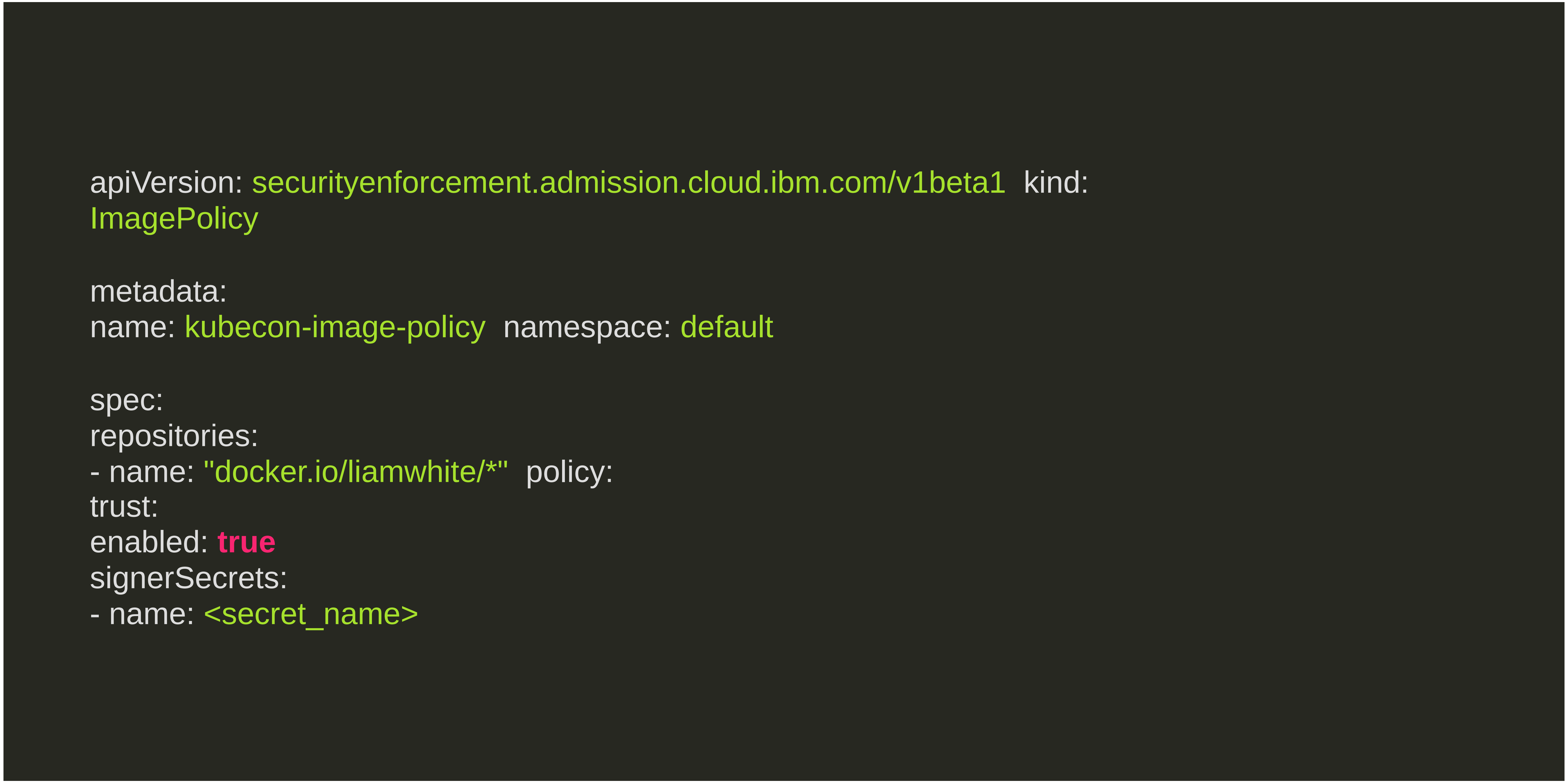
```
apiVersion: securityenforcement.admission.cloud.ibm.com/v1beta1  kind:
ClusterImagePolicy

metadata:
name: kubecon-cluster-image-policy-pinned

spec:
repositories:
- name: "docker.io/liamwhite/*"  policy:
trust:
enabled: true
signerSecrets:
- name: <secret_name>
```

Author: Nho Luong
Skill: DevOps Engineer Lead



```
apiVersion: v1  kind: Secret  type: Opaque  metadata:
name: <secret_name>  data:
name: c2lnbmVyMQ==
publicKey: LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0...
```

Author: Nho Luong
Skill: DevOps Engineer Lead



```
apiVersion: securityenforcement.admission.cloud.ibm.com/v1beta1  kind:
ImagePolicy

metadata:
name: kubecon-image-policy  namespace: default

spec:
repositories:
- name: "docker.io/liamwhite/*"  policy:
trust:
enabled: true
signerSecrets:
- name: <secret_name>
```

Author: Nho Luong
Skill: DevOps Engineer Lead

# Thank You

Author: Nho Luong
Skill: DevOps Engineer Lead