KubeCon | CloudNativeCon

North America 2018

Navigating Workload Identity in Kubernetes

Mike Danese & Spike Curtis
KubeCon North America 2018

Mike Danese

GKE Identity

Co-Chair/TL of Kubernetes SIG Auth

Spike Curtis

TIGERA

Senior
Software Engineer

Core Maintainer

Co-chair
Istio Security
Working Group

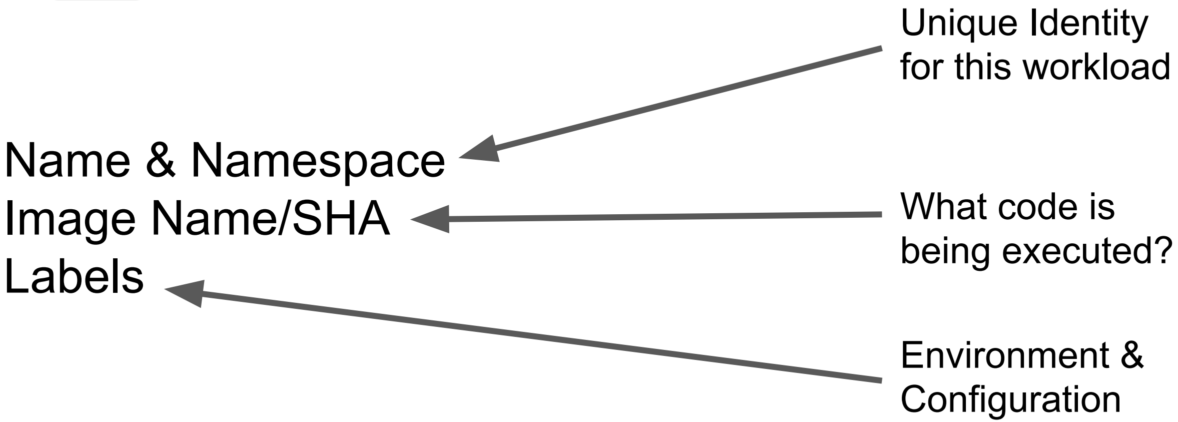
SPIFFE Standards
Maintainer

What is workload identity?

Workload Identity

Workload - instances of running code that do “work” for your application.

Pod
Container



Name & Namespace
Image Name/SHA
Labels

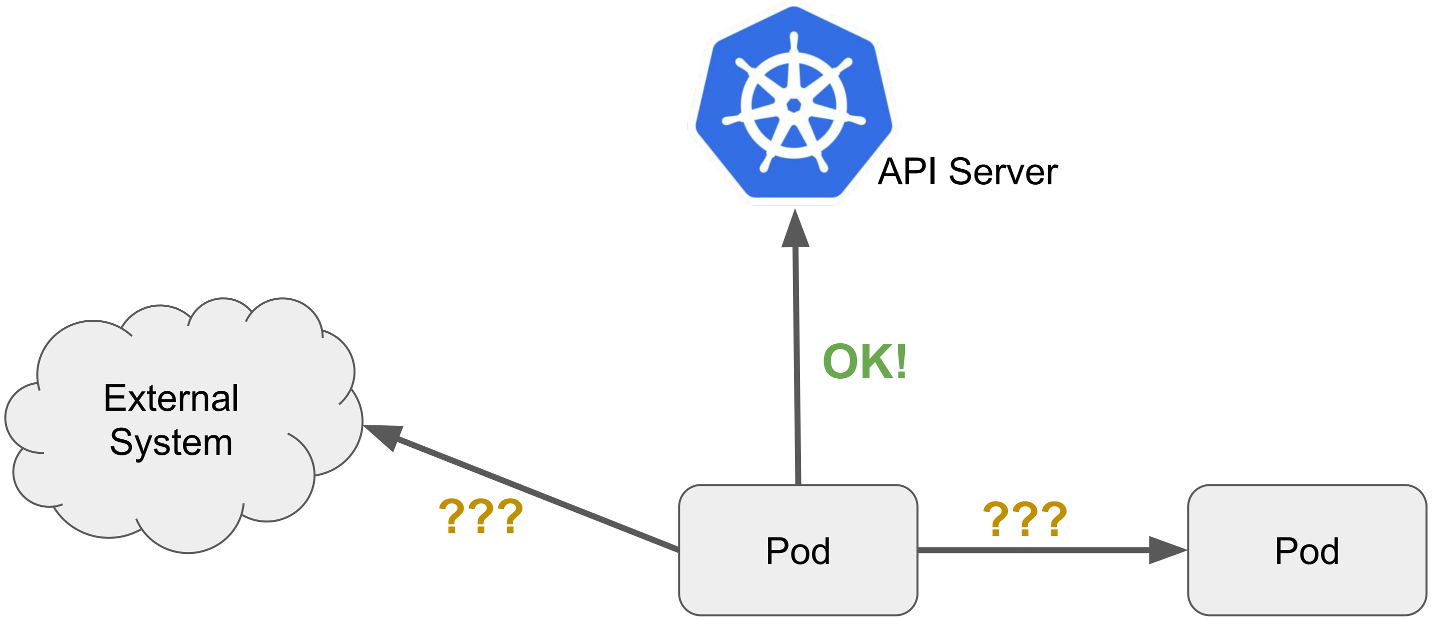
Unique Identity for this workload

What code is being executed?

Environment & Configuration

How does a workload prove its identity?

Use cases for workload identity



Desirable Properties

Desirable Properties

- Strongly Authenticated
- Prevent Escalations
- Good UX for Users, Integrators, Cluster Admins
- Performant and Available

Options for Workload ID

In this talk, we will cover 4 options you should consider

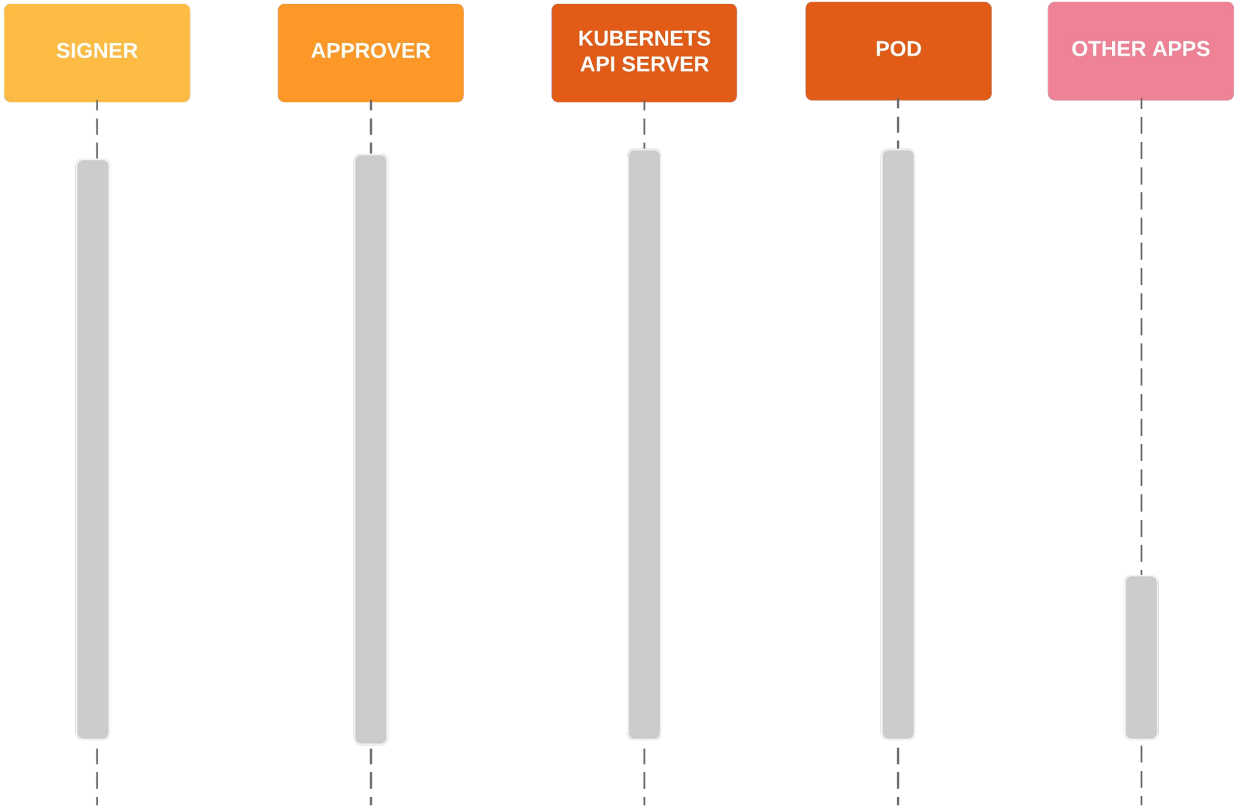
- Kubernetes Certificates API
- Kubernetes Service Account Tokens
- Istio
- SPIRE

Kubernetes Certificates API

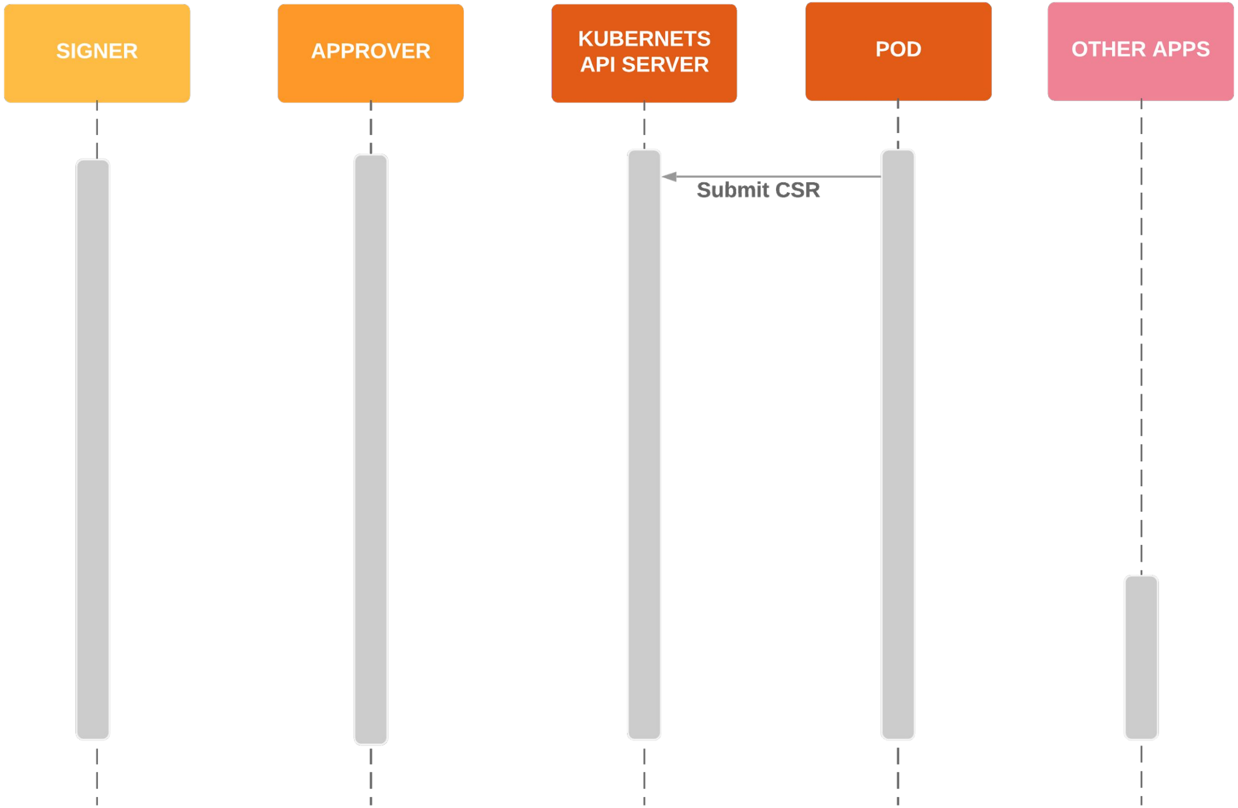
Design of Certificate Provisioning

- Multiple asynchronous actors are required to process a CSR.
- Communication flows through the Kubernetes API.
- This pattern looks a lot like any other Kubernetes control process.

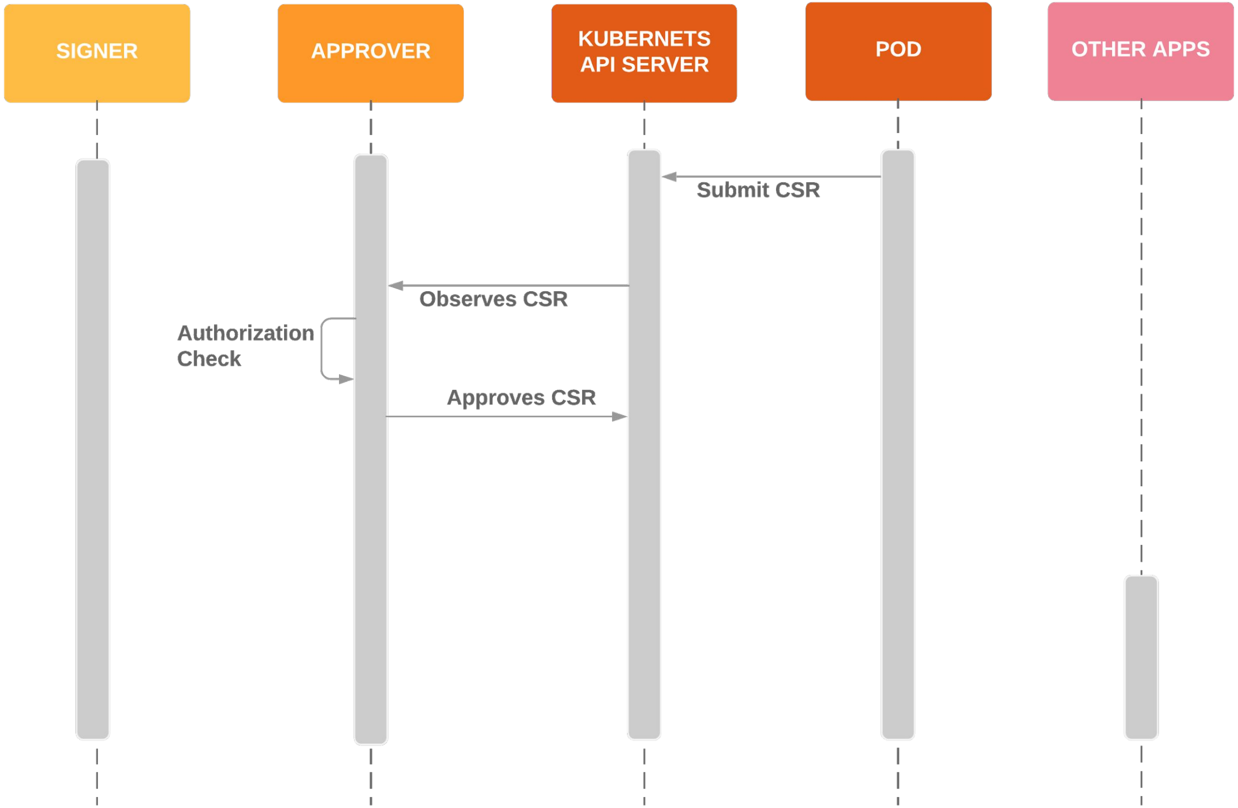
Step 0



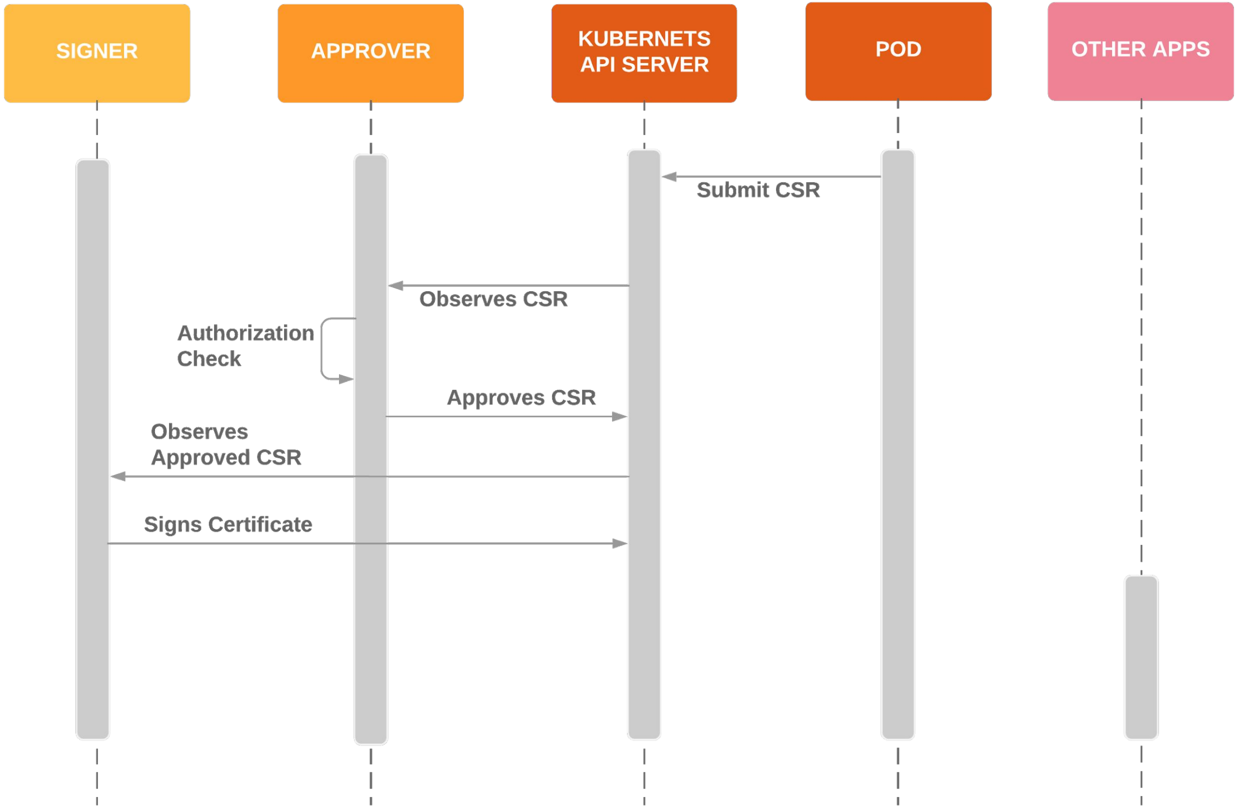
Step 1: Pod submits CSR



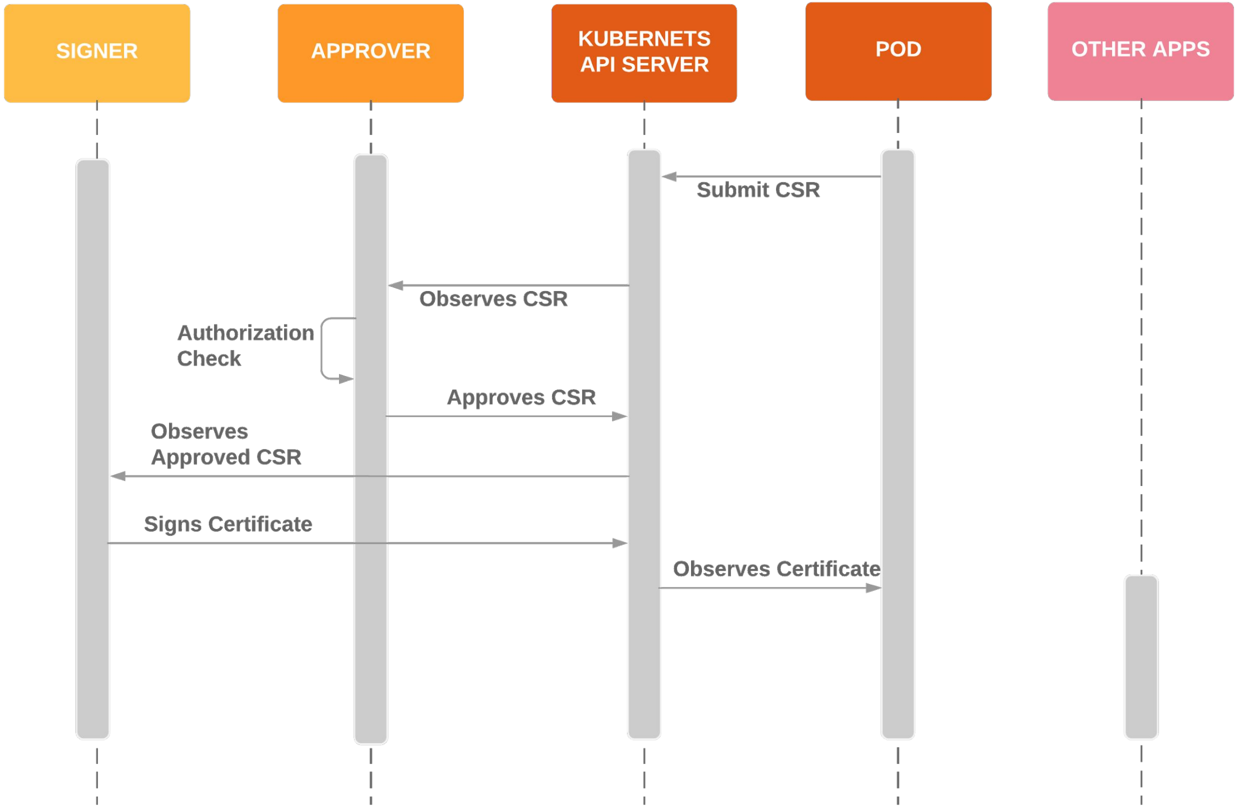
Step 2: CSR Approval



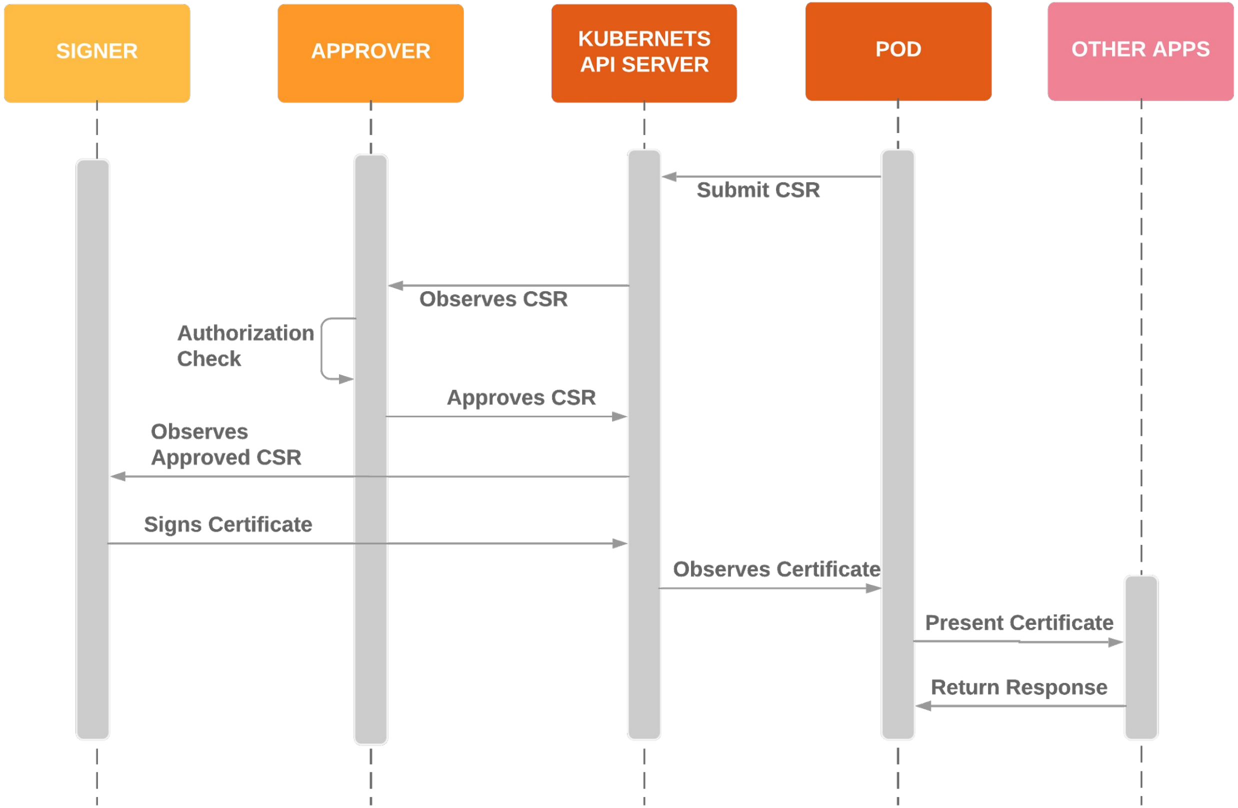
Step 3: CSR Signing



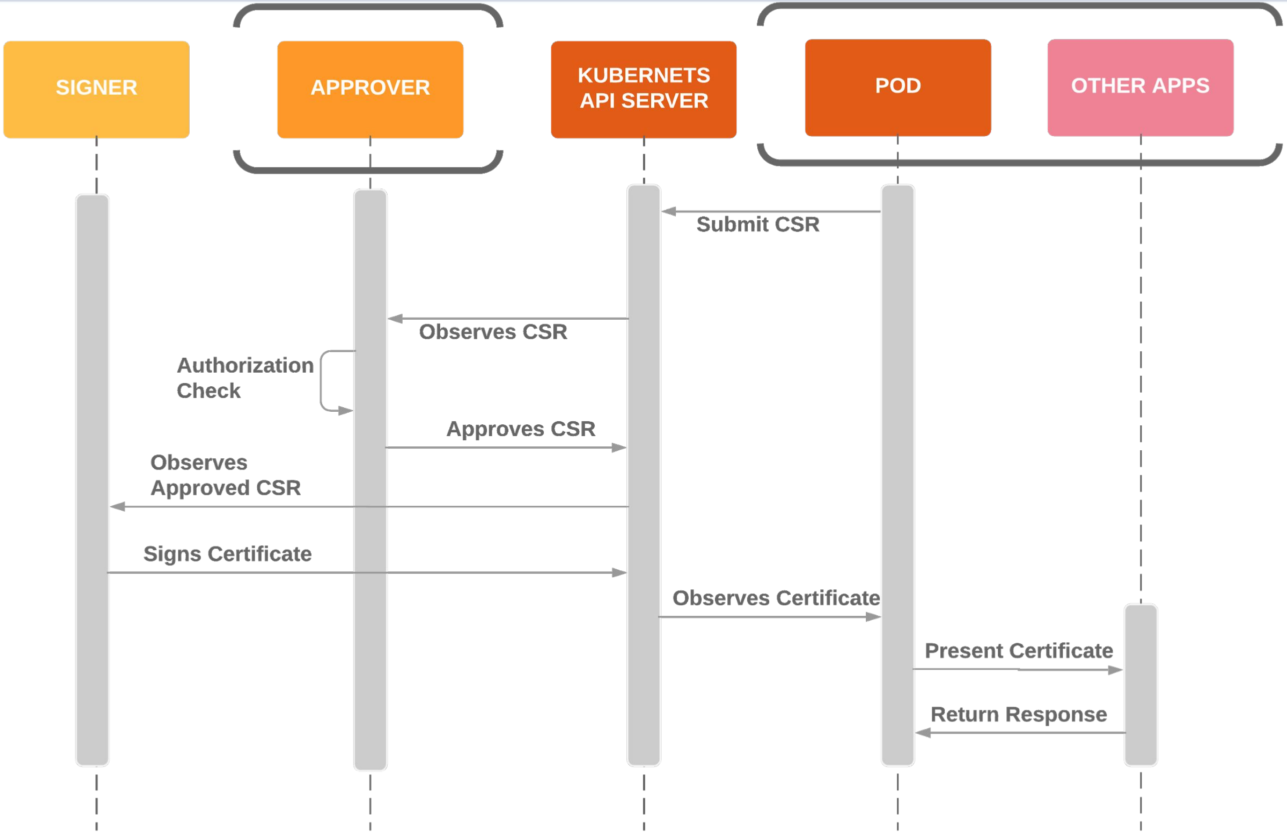
Step 4: Pod receives Certificate



The End


SIGNER
APPROVER
KUBERNETS API SERVER
POD
OTHER APPS
Submit CSR
Observes CSR
Authorization Check
Approves CSR
Observes Approved CSR
Signs Certificate
Observes Certificate
Present Certificate
Return Response

What YOU are responsible for



Approver’s Duty

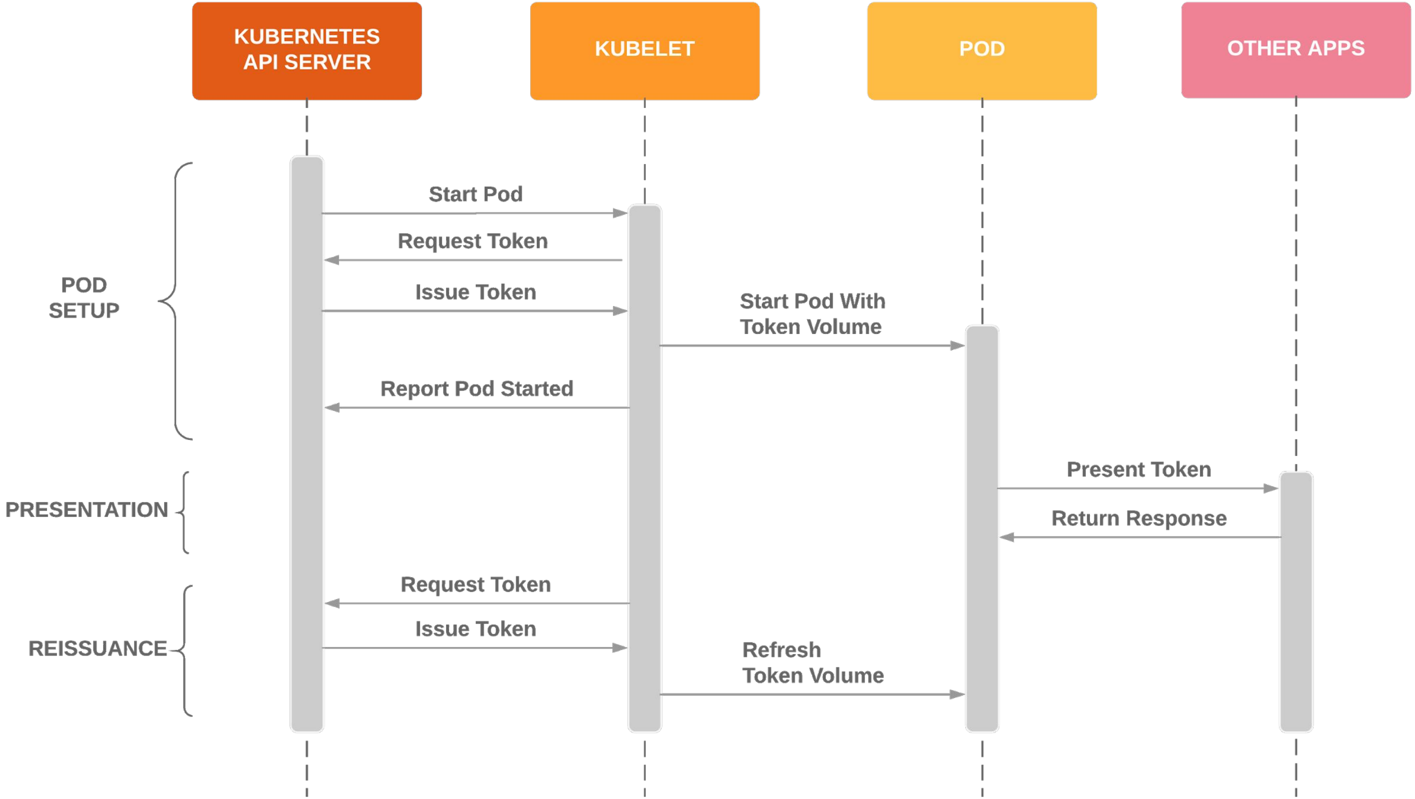
The approver is responsible for verifying the CSR satisfies two requirements:

- Subject of the CSR is the origin of the CSR.
- Subject of the CSR is authorized to act in the request context.

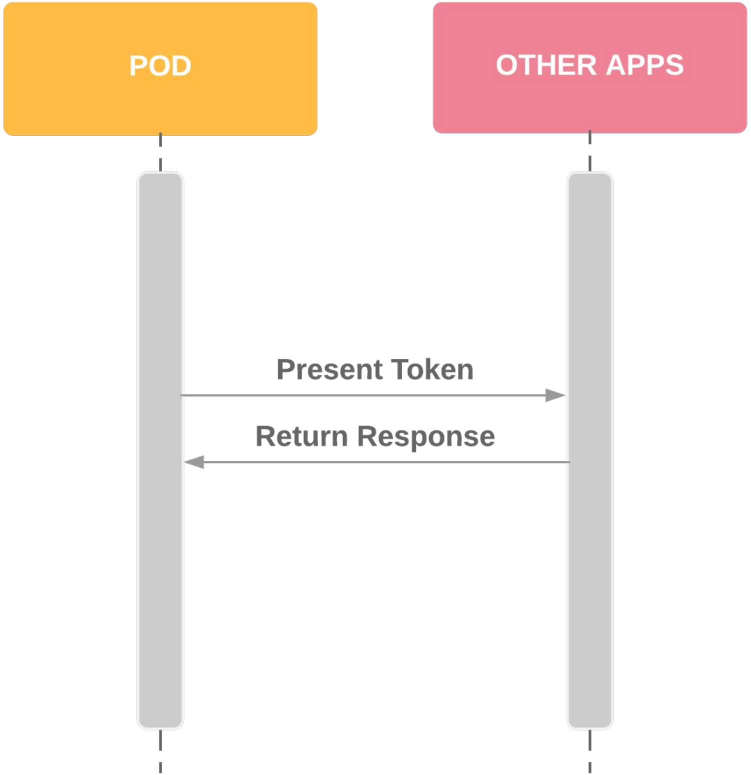
Summary?

Kubernetes
Service Account Token

Provisioning a token to a pod



What the user interacts with



Token Volume Config

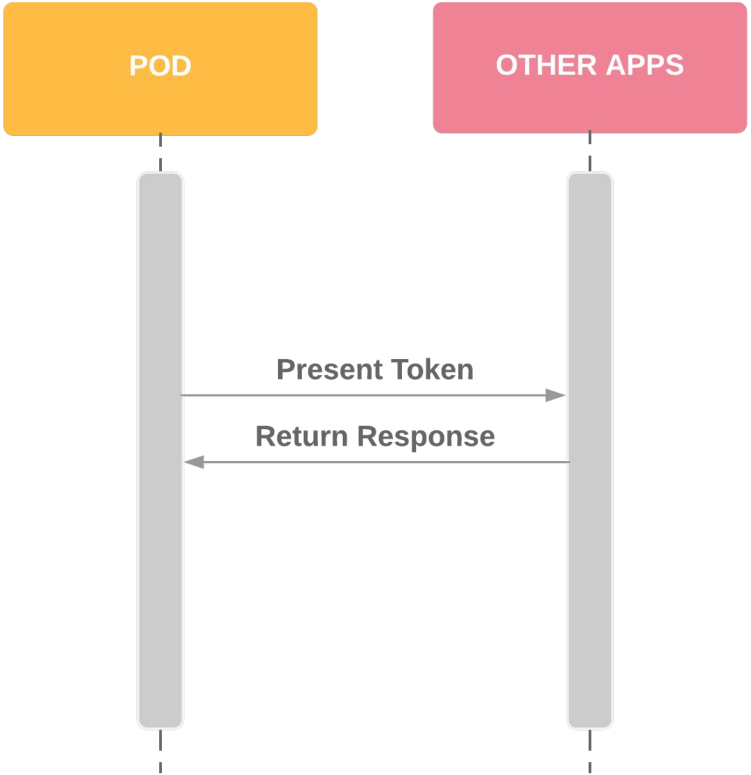
Token Volume Config

```
- serviceAccountToken:
    path: token
    audience: spike@example.com   # Kube API by default
    expirationSeconds: 1800       # an hour by default
```

Zoom Out

```
kind: Pod
spec:
  containers:
  - name: my-app
    volumeMounts:
    - name: spike-token
      mountPath: /var/talk-to-spike
  volumes:
  - name: spike-token
    projected:
      sources:
      - serviceAccountToken:
          path: token
          audience: spike@example.com
          expirationSeconds: 1800
```

What do other apps need to do?



Token Validation

Kubernetes Token Assertions

Standard Claims:

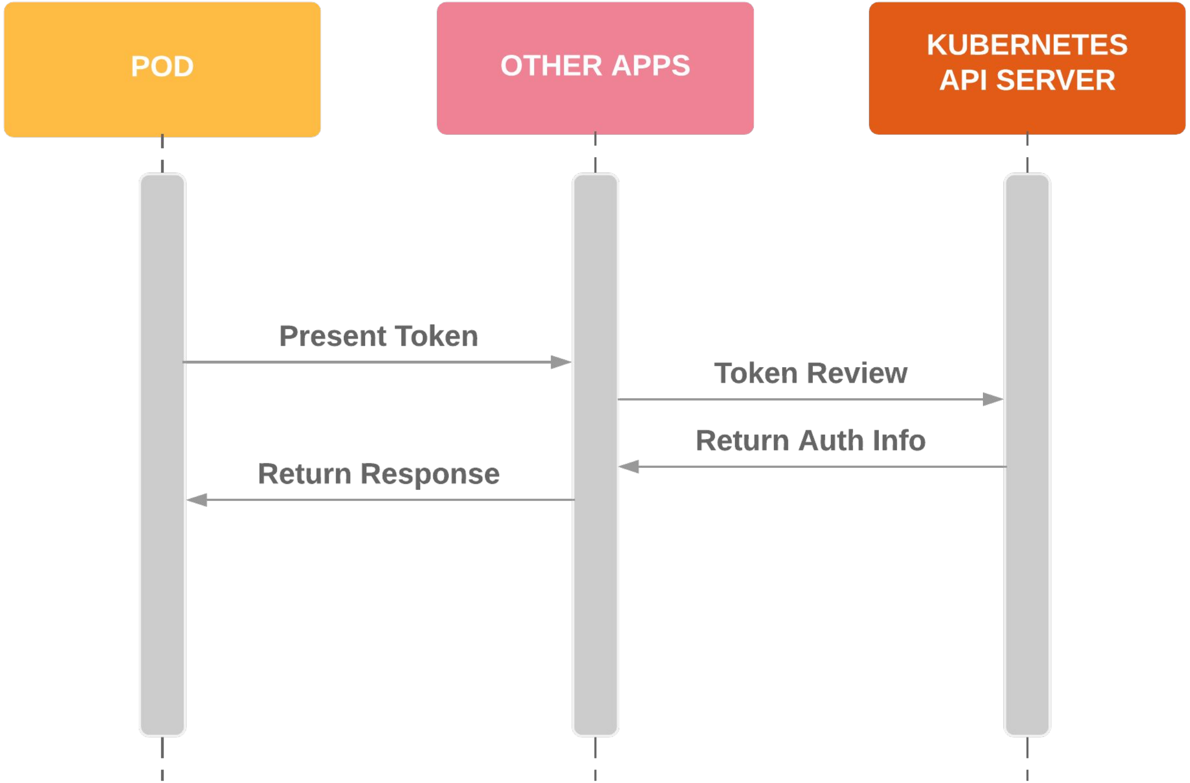
- Issuer
- Subject
- Audience
- Expiration

Custom Kubernetes Claims:

- Cluster metadata
- Pod metadata
- Node metadata derivable

```
{
  "iss": "https://foo.bar.example.com",
  "sub": "system:serviceaccount:myns:test-svcacct",
  "iat": 1536353560,
  "nbf": 1536353560,
  "exp": 1536357160,
  "aud": [
    "spike@example.com"
  ],
  "kubernetes.io": {
    "namespace": "myns",
    "pod": {
      "name": "test-pod",
      "uid": "f580d0cf-b2df-11e8-ab2c-480fcf3c8889"
    },
    "serviceaccount": {
      "name": "test-svcacct",
      "uid": "f57f5588-b2df-11e8-ab2c-480fcf3c8889"
    }
  }
}
```

Token Validation with TokenReview



POD

OTHER APPS

KUBERNETES API SERVER

Present Token

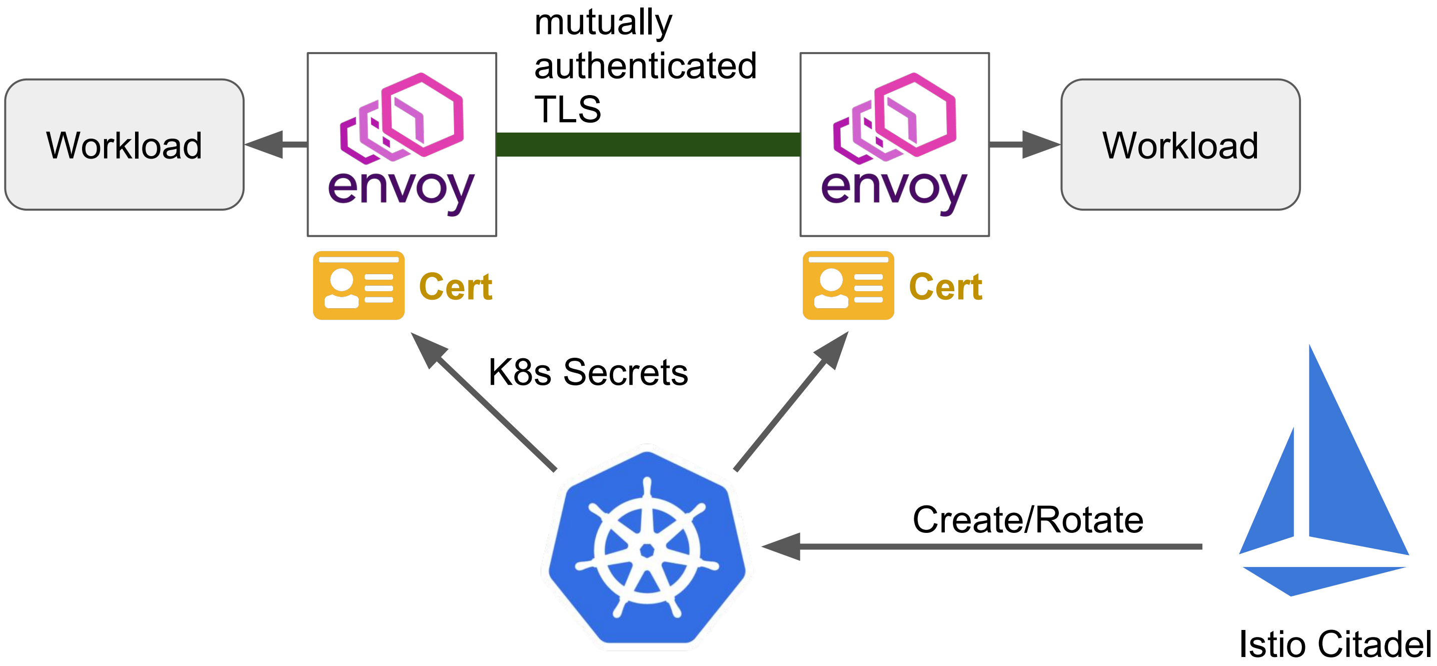
Token Review

Return Auth Info

Return Response

Summary?

Istio



mutually authenticated TLS

Workload

envoy

Cert

envoy

Cert

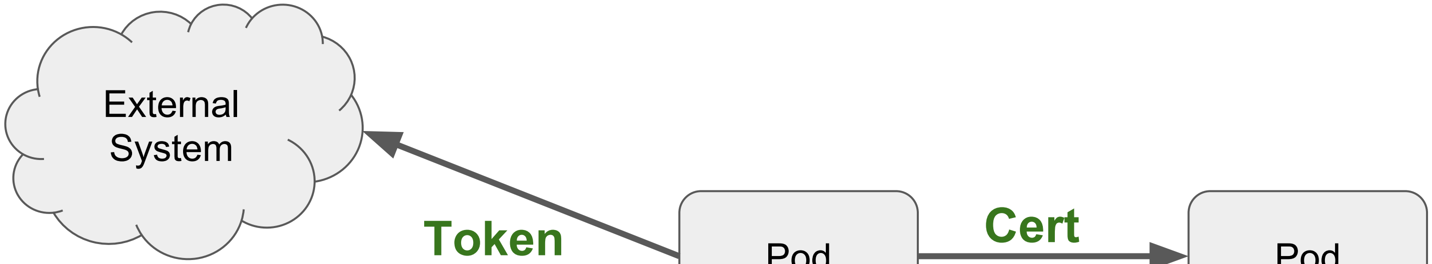
Workload

K8s Secrets

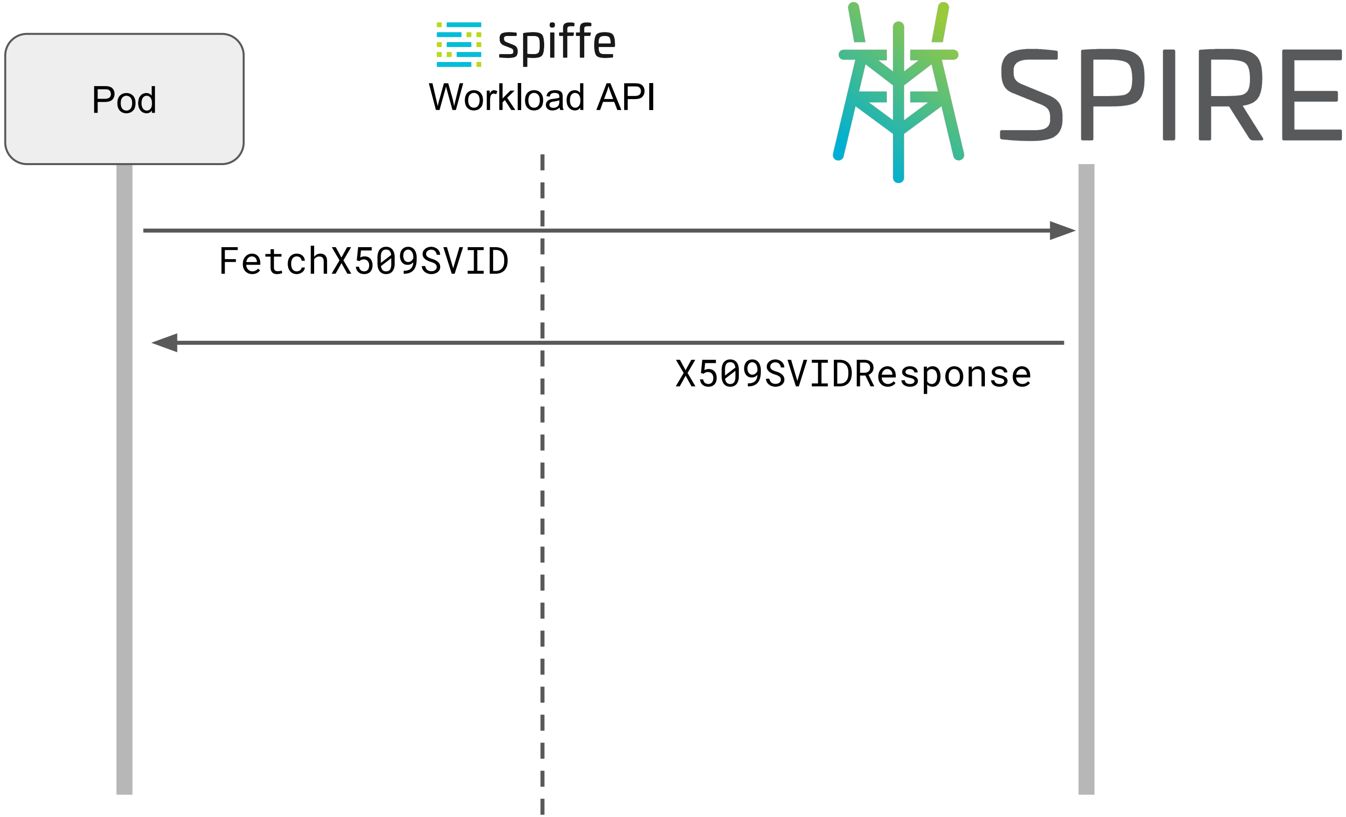
Create/Rotate

Istio Citadel

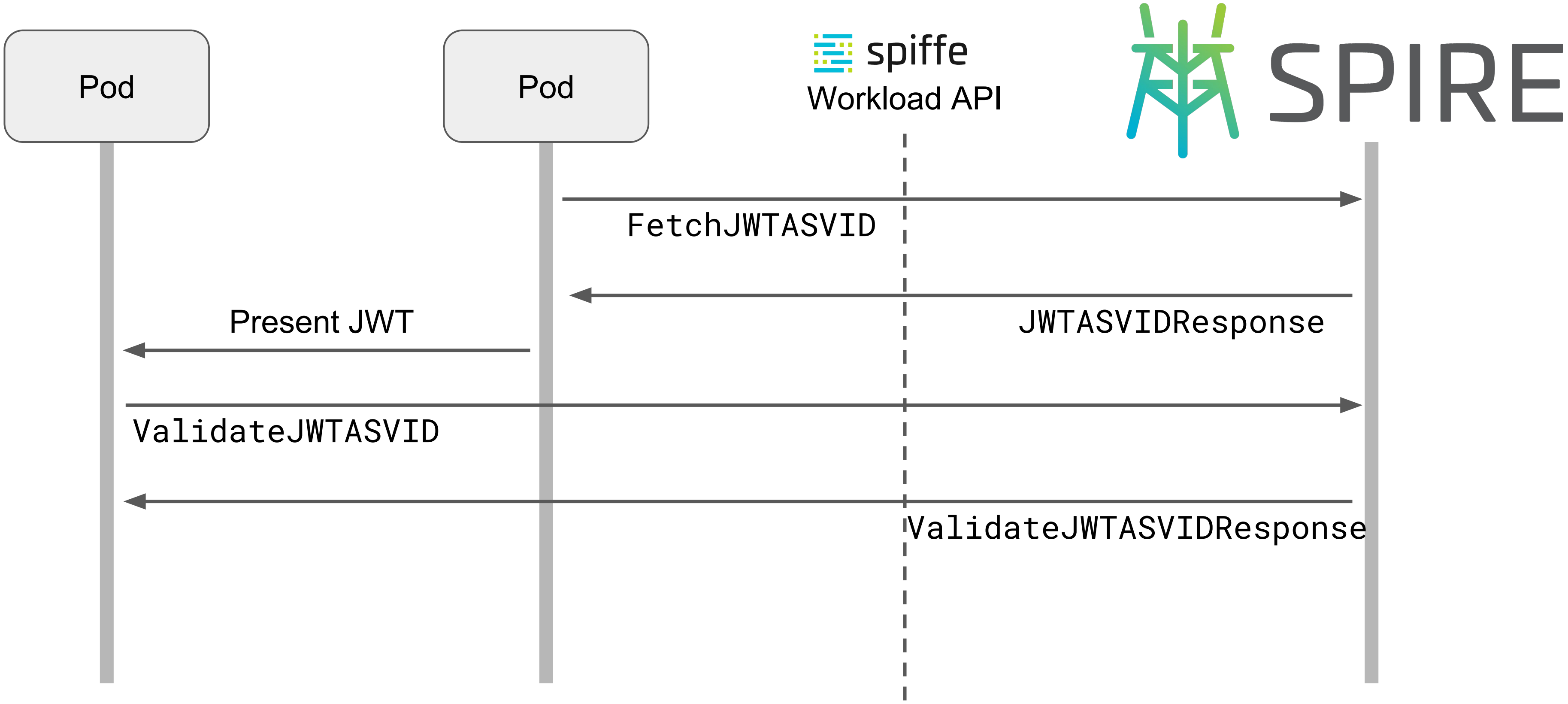
SPIRE


External System
Token
Pod
Cert
Pod

SPIFFE Workload API



SPIFFE Workload API

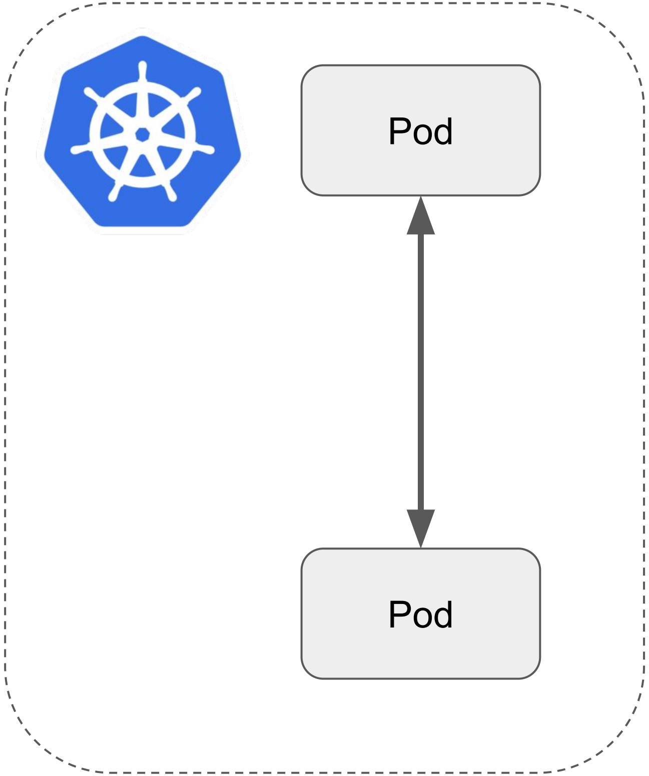


Which to choose?

Disclaimers

- There are more to these systems than can fit in a 30 minute talk
- Requirements and tradeoffs vary
- Expect all these systems to evolve in the future
- These opinions do not represent Tigera or Google
- Your mileage may vary

Which to choose?

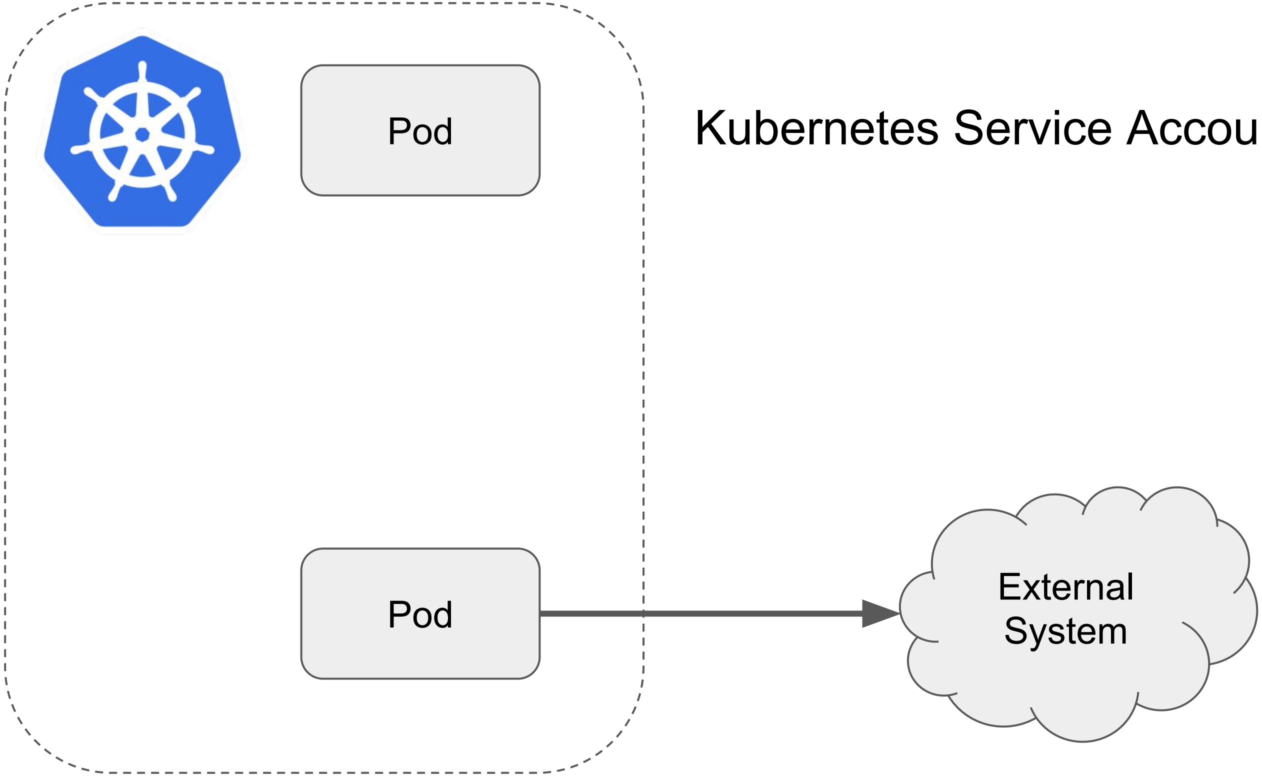


Kubernetes Certificates API

or

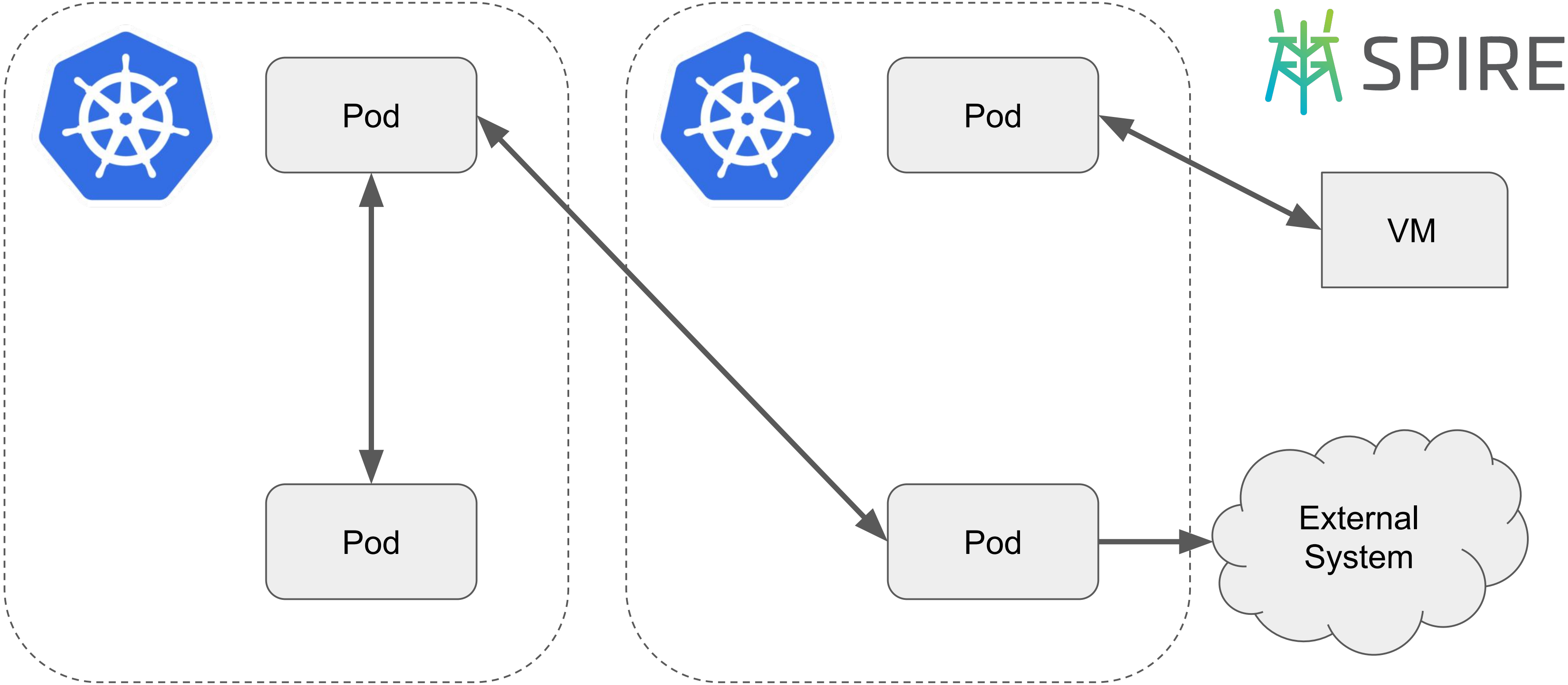
Istio

Which to choose?



Kubernetes Service Account Token

Which to choose?



Q & A