cert-manager can do SPIFFE?

Solving multi-cloud workload identity using a de facto standard tool

Thomas Meadows, Solutions Engineer, Jetstack

Josh van Leeuwen, Software Engineer, Diagrid

Nicole Geri, Unsplash

Your connection is not private

Attackers might be trying to steal your information from **www** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

☐ Help improve Safe Browsing by sending some system information and page content to Google.

Privacy policy

HIDE ADVANCED

Back to safety

KubeCon | CloudNativeCon

Europe 2023

```
Name:         managed-cert
Namespace:    default
API Version:  networking.gke.io/v1
Kind:         ManagedCertificate
(...)
Spec:
 Domains:
   spiffe.kubecon.cncf.io
   cert-manager.kubecon.cncf.io
Status:
 CertificateStatus: Provisioning
Domain Status:
 Domain: spiffe.kubecon.cncf.io
 Status: FailedNotVisible
(...)
```

```
Name:          managed-cert
Namespace:     default
API Version:   networking.gke.io/v1
Kind:          ManagedCertificate
(...)
Spec:
 Domains:
   spiffe.kubecon.cncf.io
   cert-manager.kubecon.cncf.io
Status:
 CertificateStatus: Provisioning
Domain Status:
 Domain: spiffe.kubecon.cncf.io
 Status: FailedNotVisible
(...)
```

KubeCon | CloudNativeCon

Europe 2023

CONTOUR

Getting Started Documentation Community Resources Blog

Deploying HTTPS services with Contour and cert-manager

This tutorial shows you how to securely deploy an HTTPS web application on a Kubernetes cluster, using:

→ Kubernetes

→ Contour, as the Ingress controller

→ **JetStack's cert-manager** to provision TLS certificates from **the Let's Encrypt project**

Prerequisites

CONTOUR

Getting Started Documentation Community Resources Blog

Deploying HTTPS services with Contour and cert-manager

This tutorial shows you how to securely deploy an HTTPS web application on a Kubernetes cluster, using:

→ Kubernetes

→ Contour, as the Ingress controller

→ **JetStack's cert-manager** to provision TLS certificates from **the Let's Encrypt project**

Prerequisites

```
$ kubectl describe certificate quickstart-example-tls
Status:
 Conditions:
   Last Transition Time:  2019-01-09T13:57:52Z
   Message:               Certificate is up to date and has not expired
   Reason:                Ready
   Status:                True
   Type:                  Ready
 Not After:               2019-04-09T12:57:50Z
Events:
 Type    Reason         Age                From          Message
 ----    ------         ----               ----          -------
 Normal  Generated      11m                cert-manager  Generated new
private key
 Normal  OrderCreated   11m                cert-manager  Created Order
resource "quickstart-example-tls-889745041"
 Normal  OrderComplete  10m                cert-manager  Order "quickstart-
example-tls-889745041" completed successfully
```

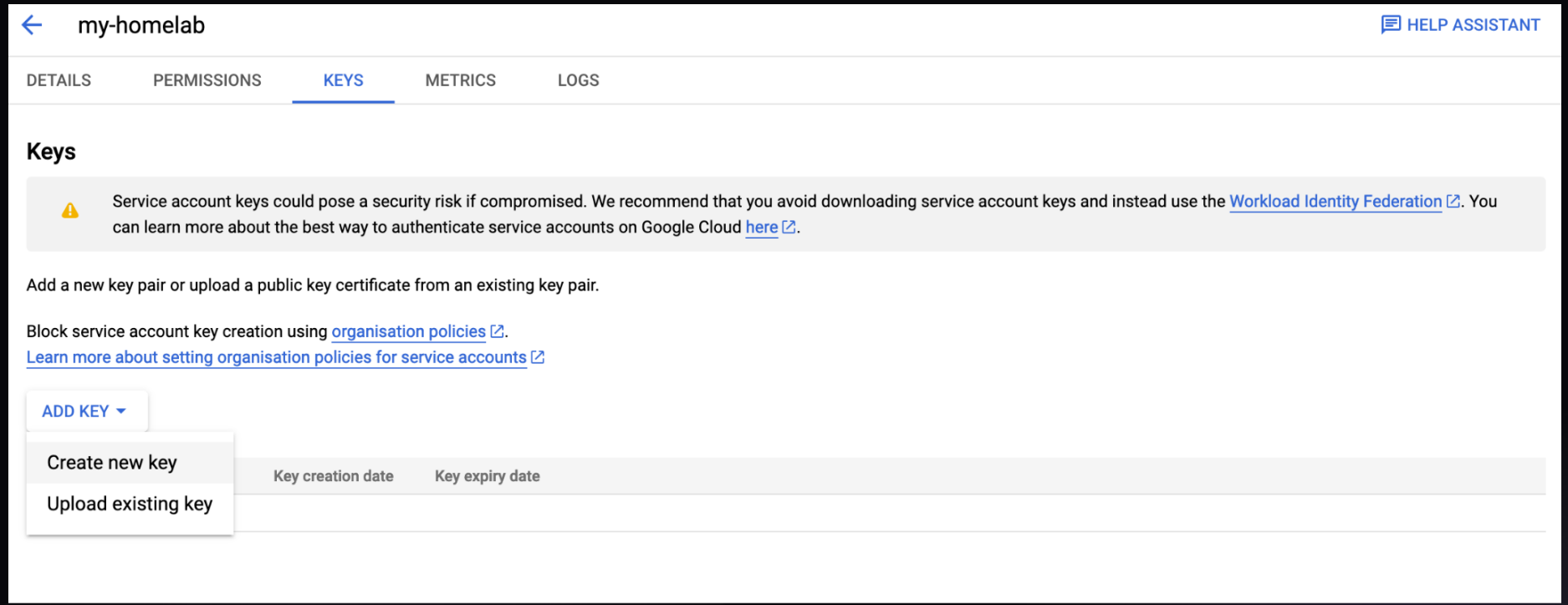
KubeCon | CloudNativeCon

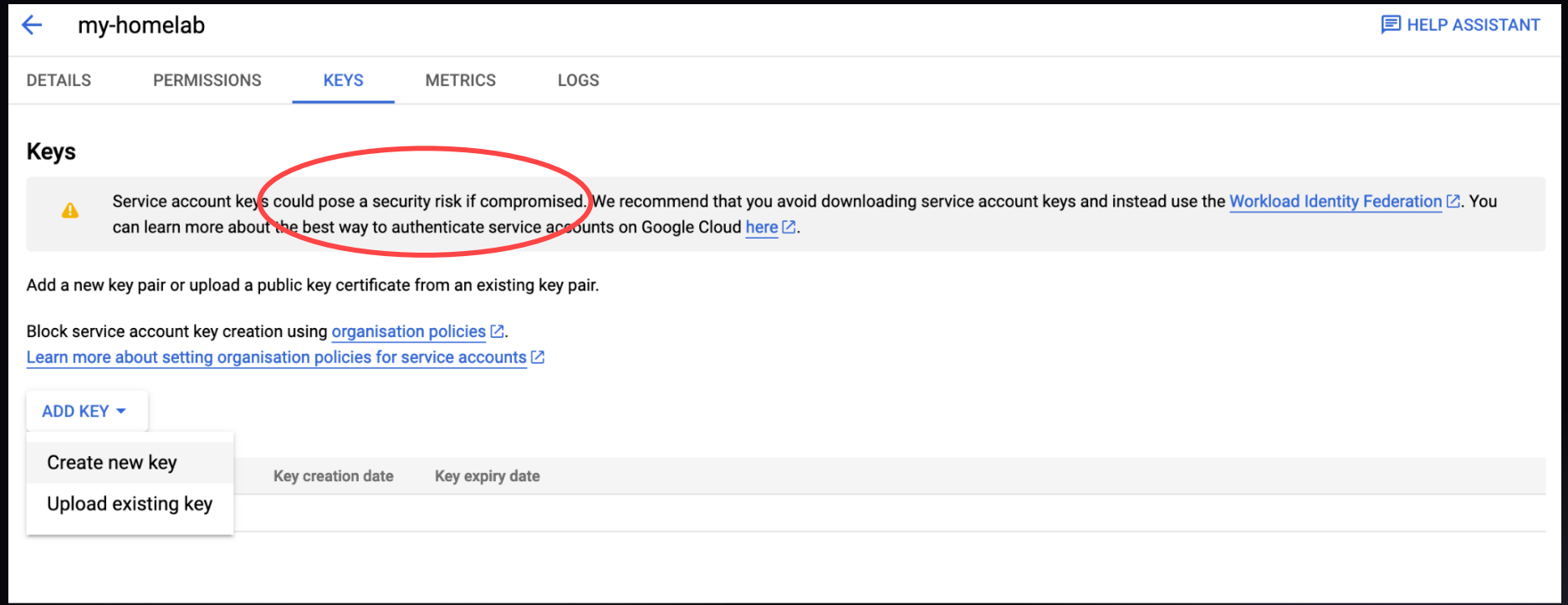
Europe 2023

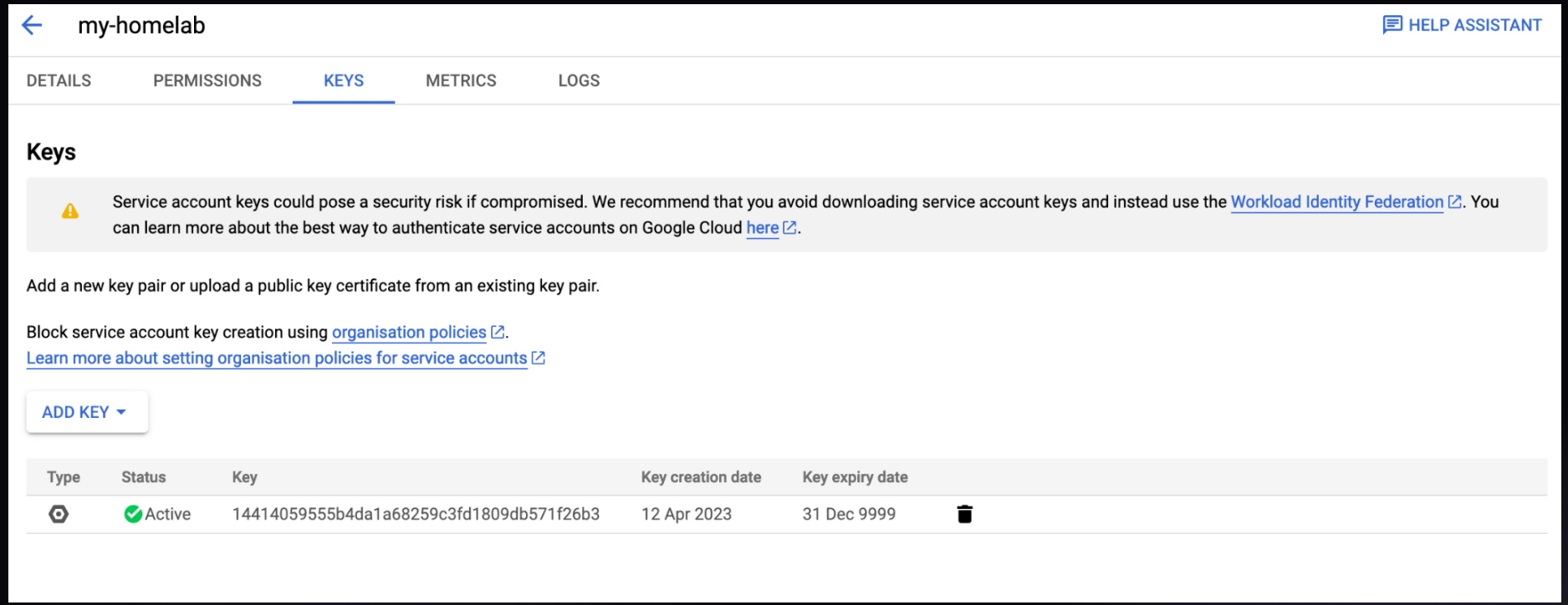
Let's Encrypt

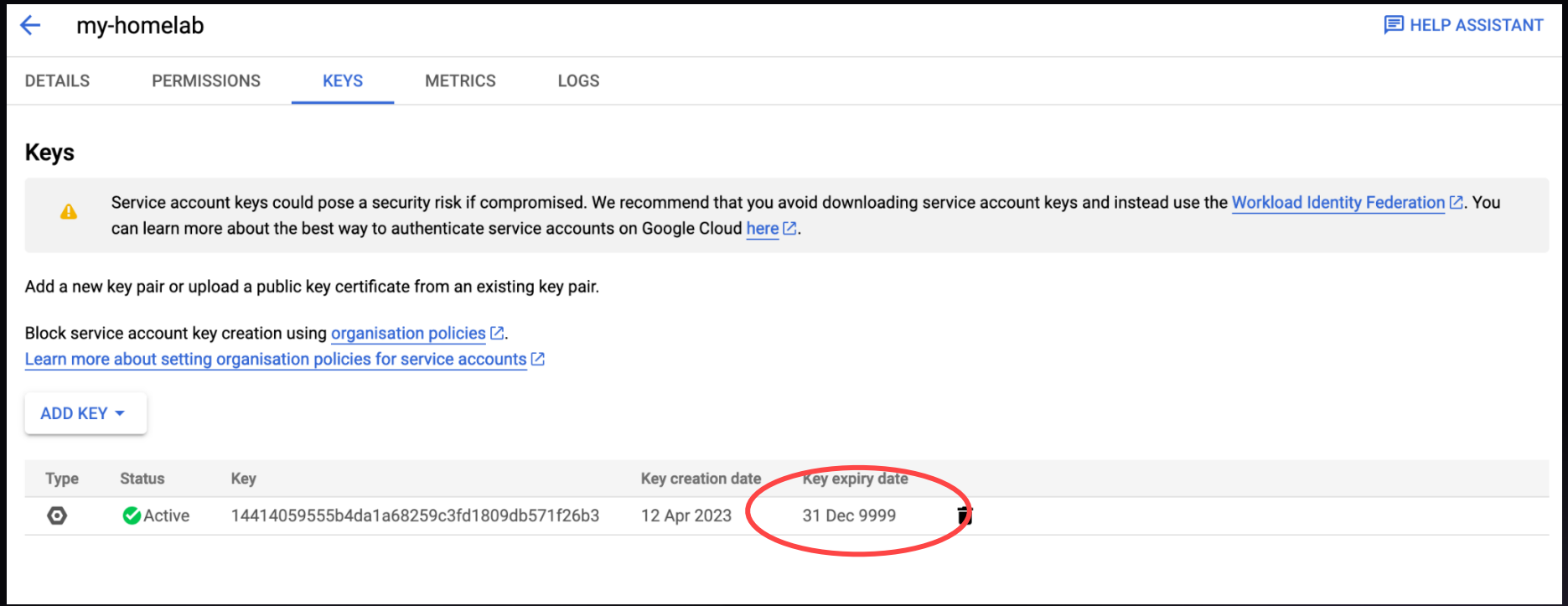
Authentication

What about it?


my-homelab
HELP ASSISTANT
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts
ADD KEY
Create new key
Upload existing key
Key creation date
Key expiry date


my-homelab
HELP ASSISTANT
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts
ADD KEY
Create new key
Upload existing key
Key creation date
Key expiry date


my-homelab
HELP ASSISTANT
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts
ADD KEY
Type
Status
Key
Key creation date
Key expiry date
Active
14414059555b4da1a68259c3fd1809db571f26b3
12 Apr 2023
31 Dec 9999


my-homelab
HELP ASSISTANT
DETAILS
PERMISSIONS
KEYS
METRICS
LOGS
Keys
Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.
Add a new key pair or upload a public key certificate from an existing key pair.
Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts
ADD KEY
Type
Status
Key
Key creation date
Key expiry date
Active
14414059555b4da1a68259c3fd1809db571f26b3
12 Apr 2023
31 Dec 9999

my-homelab

HELP ASSISTANT

DETAILS | PERMISSIONS | KEYS | METRICS | LOGS

Keys

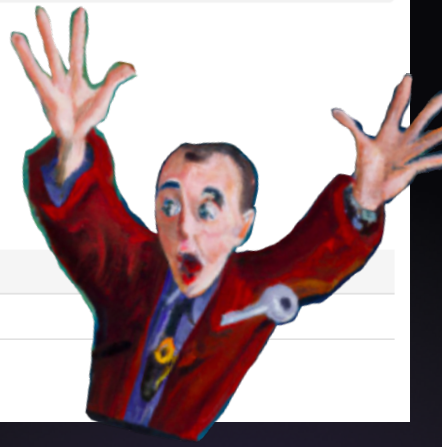
Service account keys could pose a security risk if compromised. We recommend that you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organisation policies.
Learn more about setting organisation policies for service accounts

ADD KEY

Type	Status	Key	Key creation date	Key expiry date
	Active	14414059555b4da1a68259c3fd1809db571f26b3	12 Apr 2023	31 Dec 9999



KubeCon CloudNativeCon Europe 2023

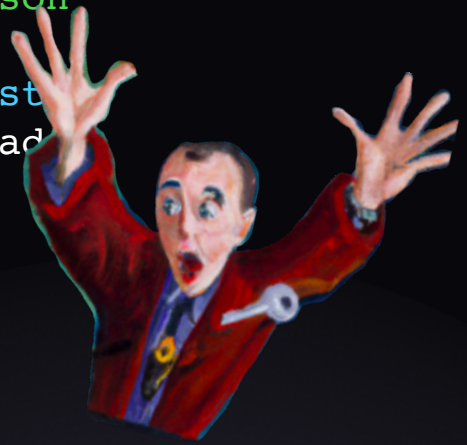
```
mic-test …
→ ls
Dockerfile  README.md  bin  go.mod  main.go  my-service-account-
keys.json

mic-test …
→ git add .
```

KubeCon CloudNativeCon Europe 2023

```
mic-test …
→ ls
Dockerfile  README.md  bin  go.mod  main.go  my-service-account-
keys.json

mic-test
→ git ad
```



```
apiVersion: v1
kind: ServiceAccount
metadata:
 annotations:
   iam.gke.io/gcp-service-account: my-homelab@my-
project.iam.gserviceaccount.com
 name: test
 namespace: default
```

```
→ kubectl run --serviceaccount=my-homelab -i --tty test3 --
image gcr.io/cloud-builders/gsutil ls gs://workload-identity-
test

→ gs://workload-identity-test/success/
```

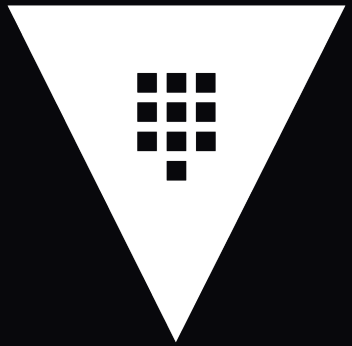
```
apiVersion: v1
kind: ServiceAccount
metadata:
 annotations:
   iam.gke.io/gcp-service-account: my-homelab@my-
project.iam.gserviceaccount.com
 name: test
 namespace: default
```

```
→ kubectl run --serviceaccount=my-homelab -i --tty test3 --
image gcr.io/cloud-builders/gsutil ls gs://workload-identity-
test

→ gs://workload-identity-test/success/
```

KubeCon CloudNativeCon Europe 2023

KubeCon | CloudNativeCon
Europe 2023



HashiCorp
Vault

> But where do I store the secret that lets me access the secrets? 😕

— Me

Surely not more long-lived static keys?

Surely not more long-lived static keys?

KubeCon | CloudNativeCon

Europe 2023

What if there was a world…

KubeCon | CloudNativeCon

Europe 2023

Where having to use secrets to authenticate was a thing of the past…

If only it was that simple.

Enter the Secure Production Identity Framework For Everyone!

Enter the **S**ecure **P**roduction **I**dentity **F**ramework
For **E**veryone!

SPIFFE


pod


?
pod


pod


pod
SVID

spiffe://trust.domain/workload

spiffe://trust.domain/workload

spiffe://trust.domain/workload

spiffe://gke.homelab/workload

spiffe://gke.homelab/workload

spiffe://gke.homelab/sa/phippy

spiffe://gke.homelab/ns/default/sa/phippy

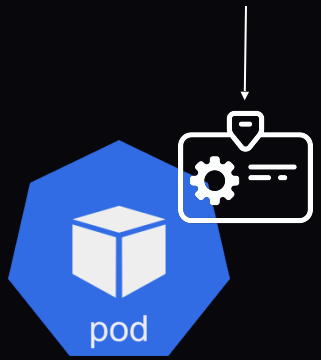
spiffe://gke.homelab/ns/default/sa/phippy

KubeCon | CloudNativeCon

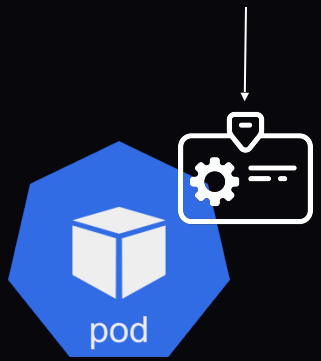
Europe 2023


pod

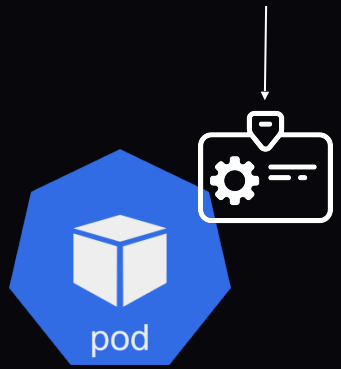
spiffe://tom.cluster/ns/default/sa/pod01



spiffe://tom.cluster/ns/default/sa/pod01

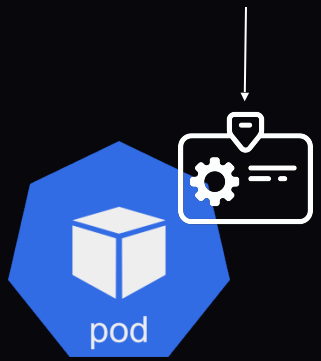


spiffe://tom.cluster/ns/default/sa/pod02

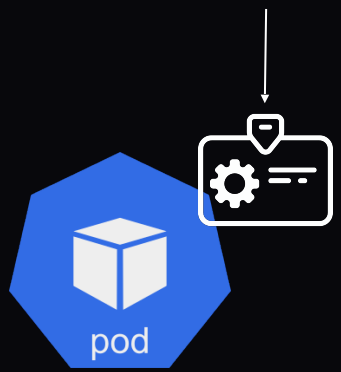



spiffe://tom.cluster/ns/default/sa/pod01
spiffe://tom.cluster/ns/default/sa/pod02
pod
pod

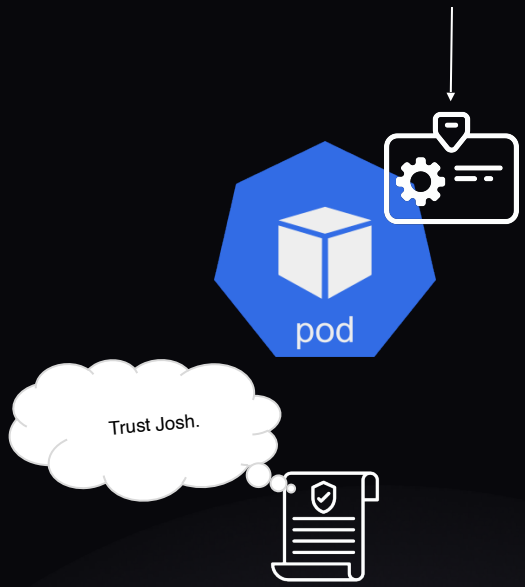
spiffe://tom.cluster/ns/default/sa/pod01



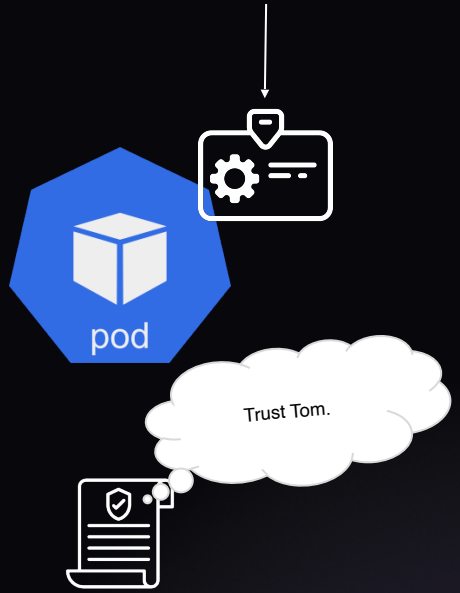
spiffe://josh.cluster/ns/default/sa/pod02

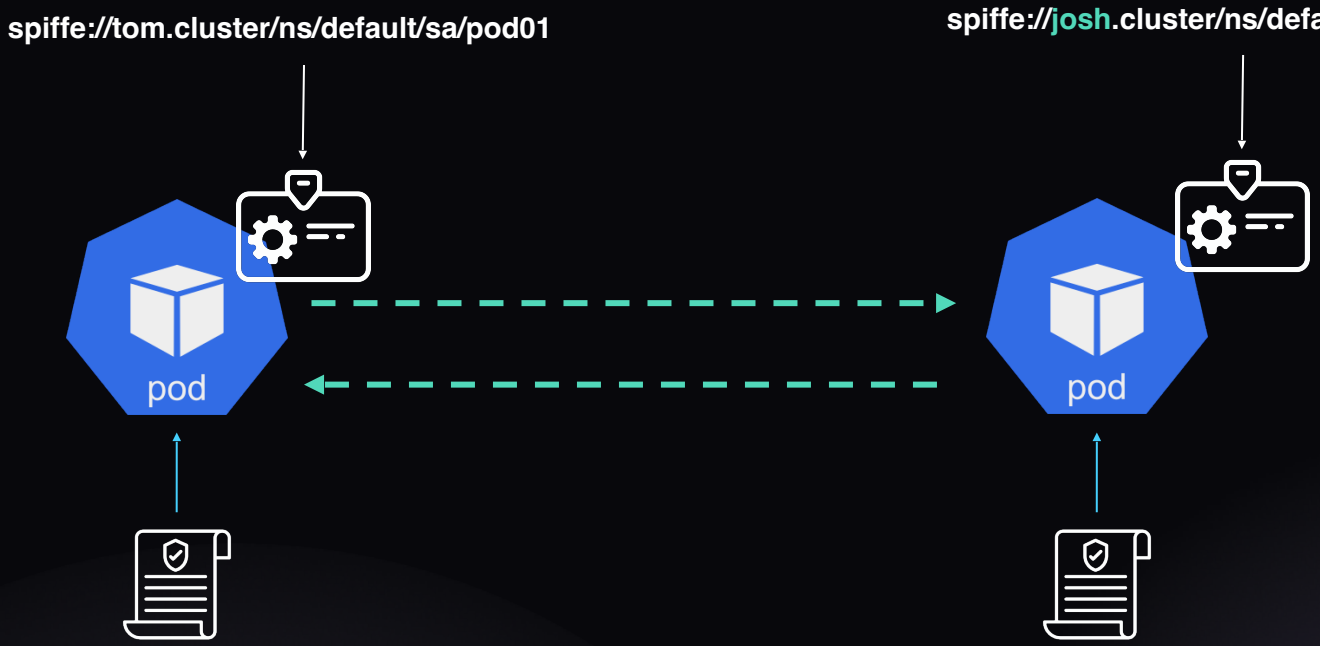


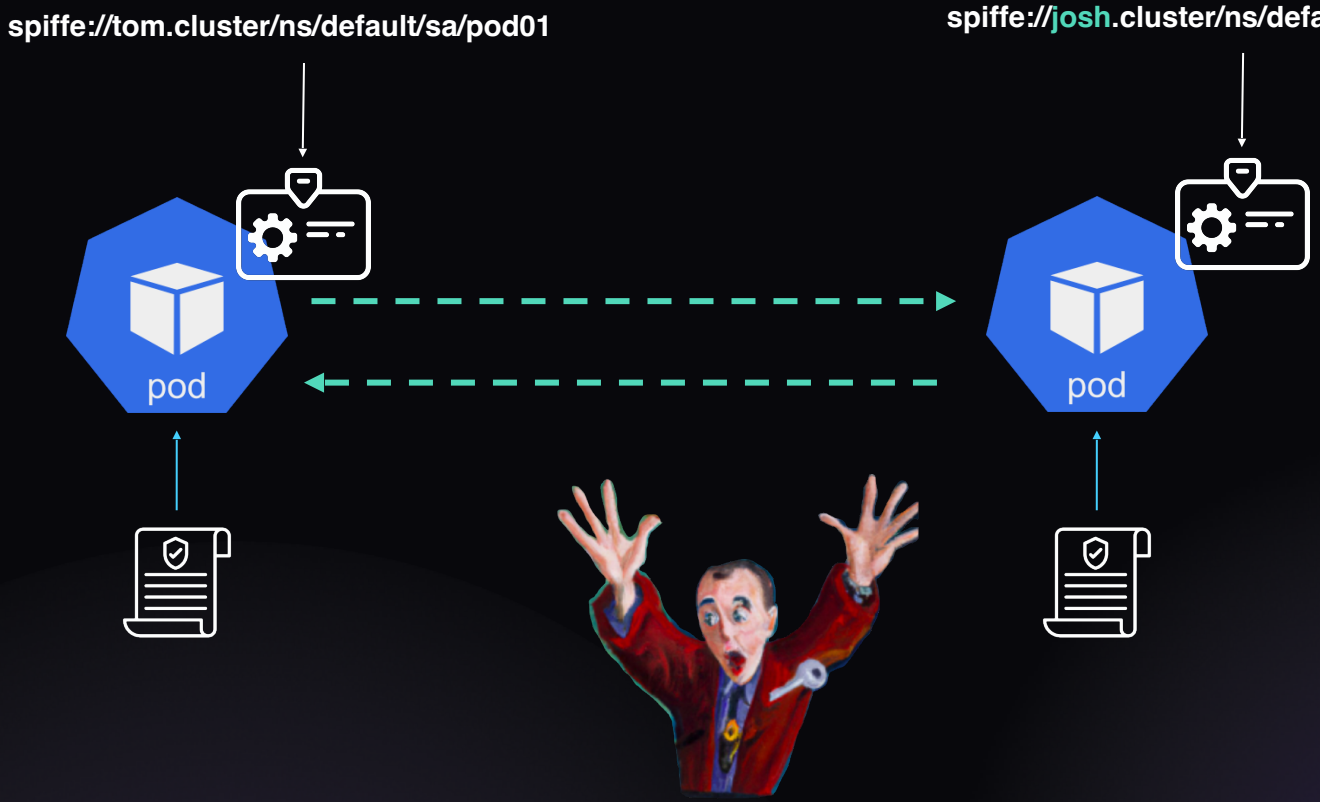
spiffe://tom.cluster/ns/default/sa/pod01



spiffe://josh.cluster/ns/default/sa/pod02

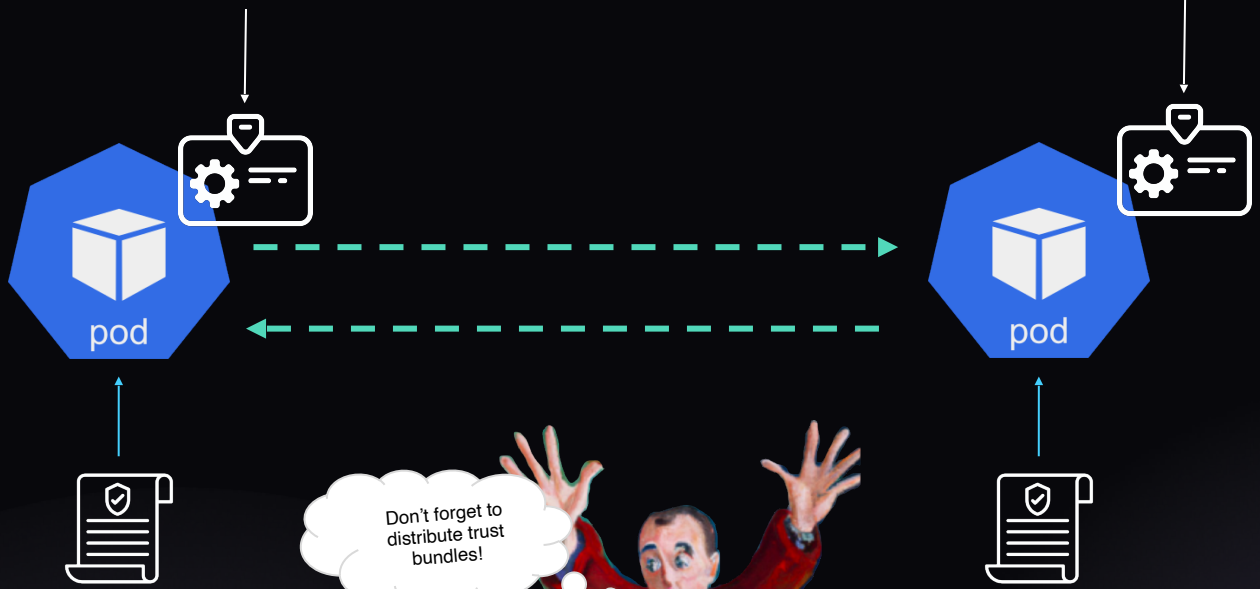



spiffe://tom.cluster/ns/default/sa/pod01
spiffe://josh.cluster/ns/default/sa/pod02
pod
pod


spiffe://tom.cluster/ns/default/sa/pod01
spiffe://josh.cluster/ns/default/sa/pod02
pod
pod

spiffe://tom.cluster/ns/default/sa/pod01

spiffe://josh.cluster/ns/default/sa/pod02

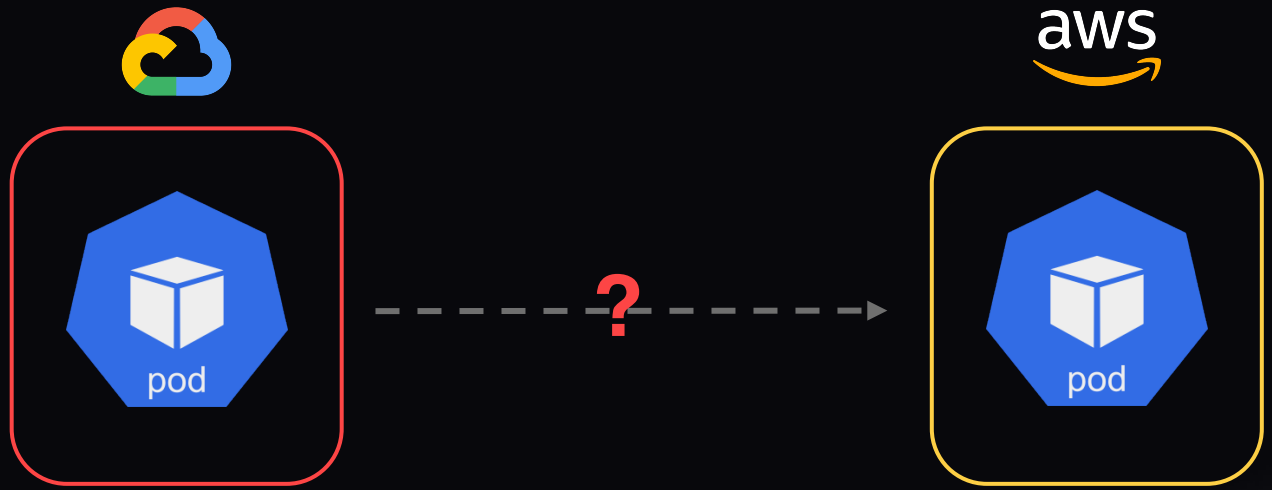


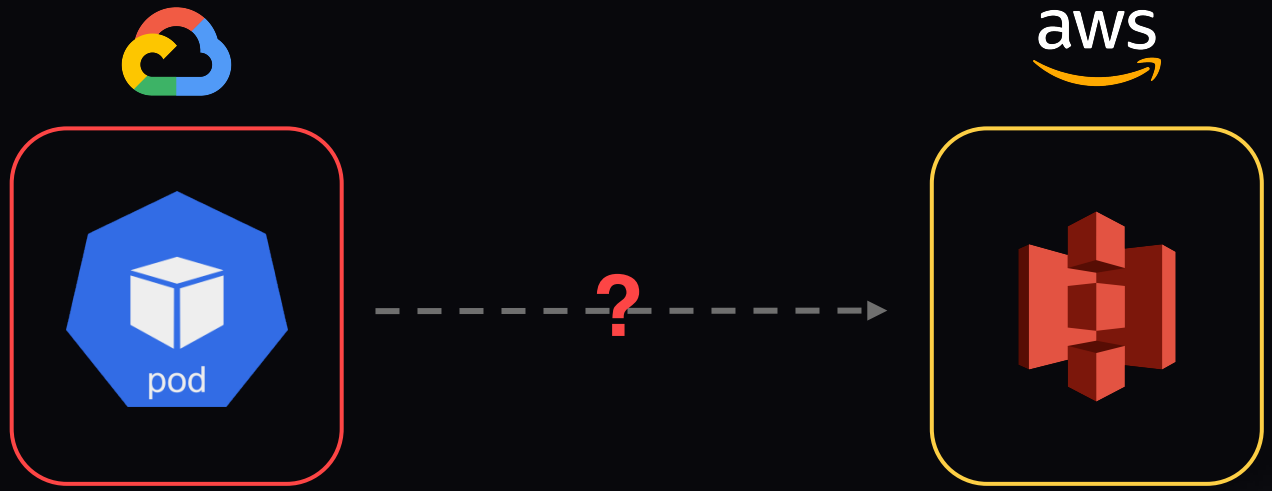

pod

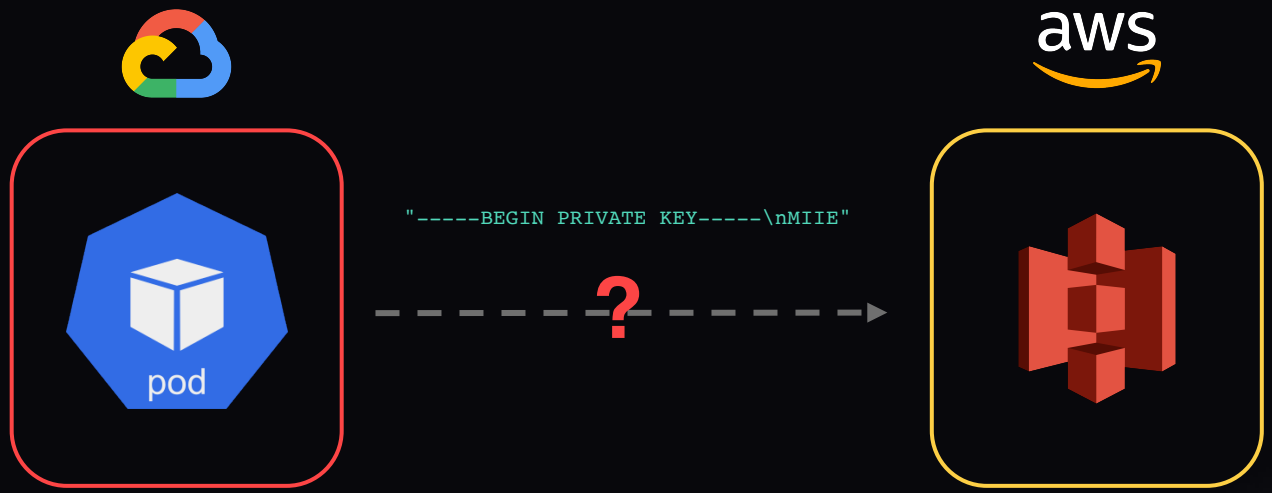

pod


pod

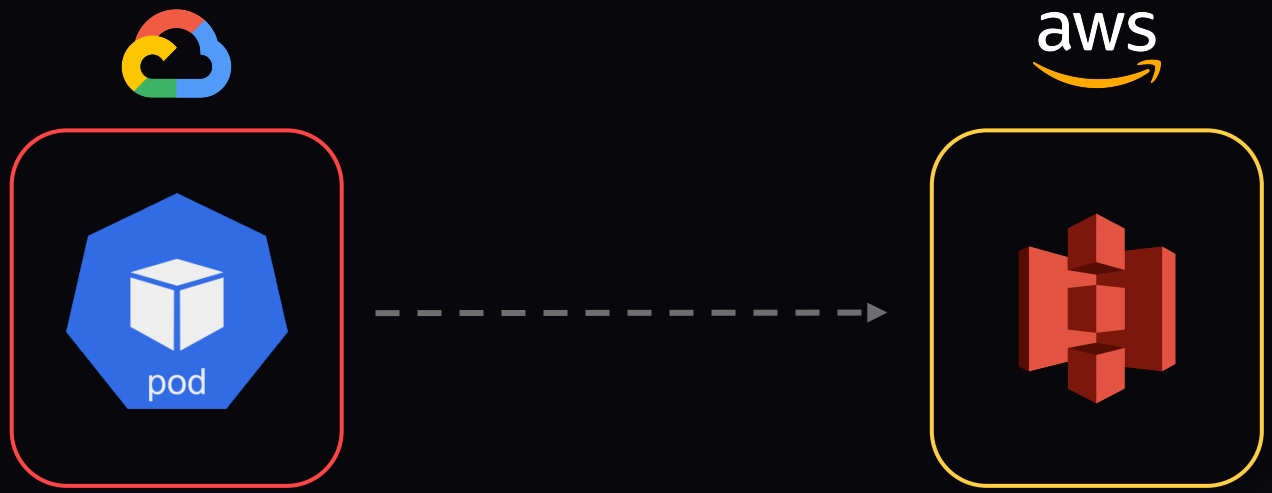

pod

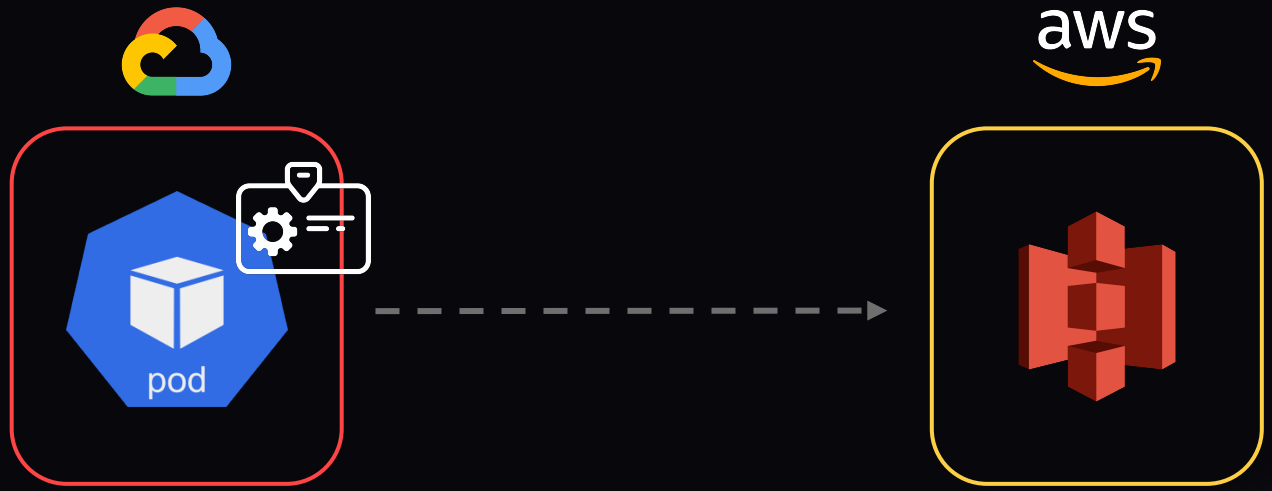

aws
pod
?
pod


aws
pod
?

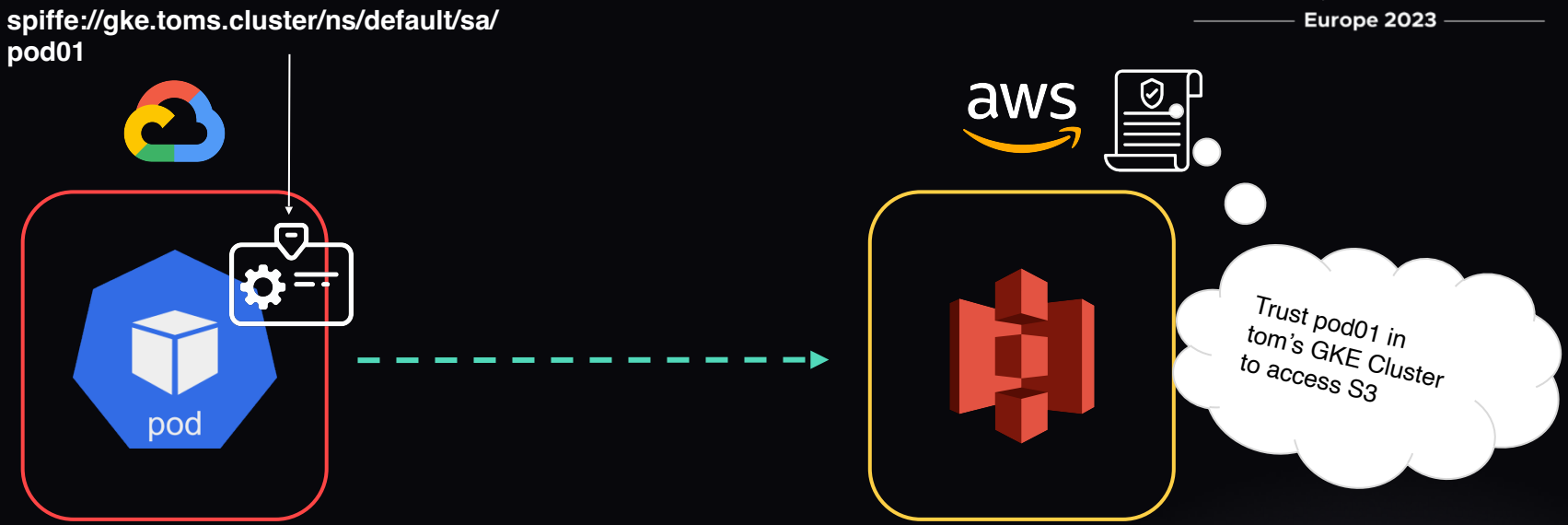

aws
pod
"-----BEGIN PRIVATE KEY-----\nMIIE"
?


aws
pod
"-----BEGIN PRIVATE KEY-----\nMIIE"
?


aws
pod


aws
pod


spiffe://gke.toms.cluster/ns/default/sa/
pod01
aws
pod


spiffe://gke.toms.cluster/ns/default/sa/pod01
pod
aws
Trust pod01 in tom's GKE Cluster to access S3


This is awesome!


How do I get started?

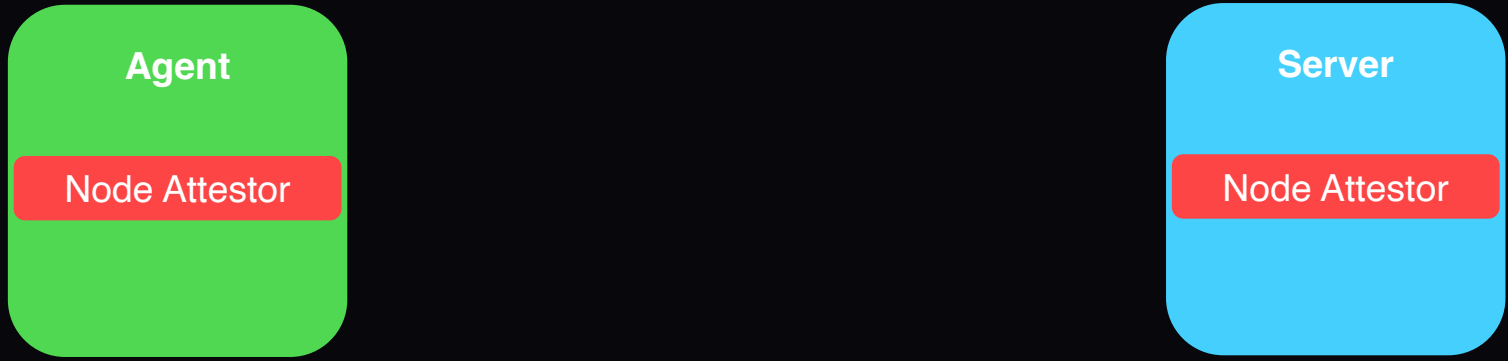
KubeCon | CloudNativeCon

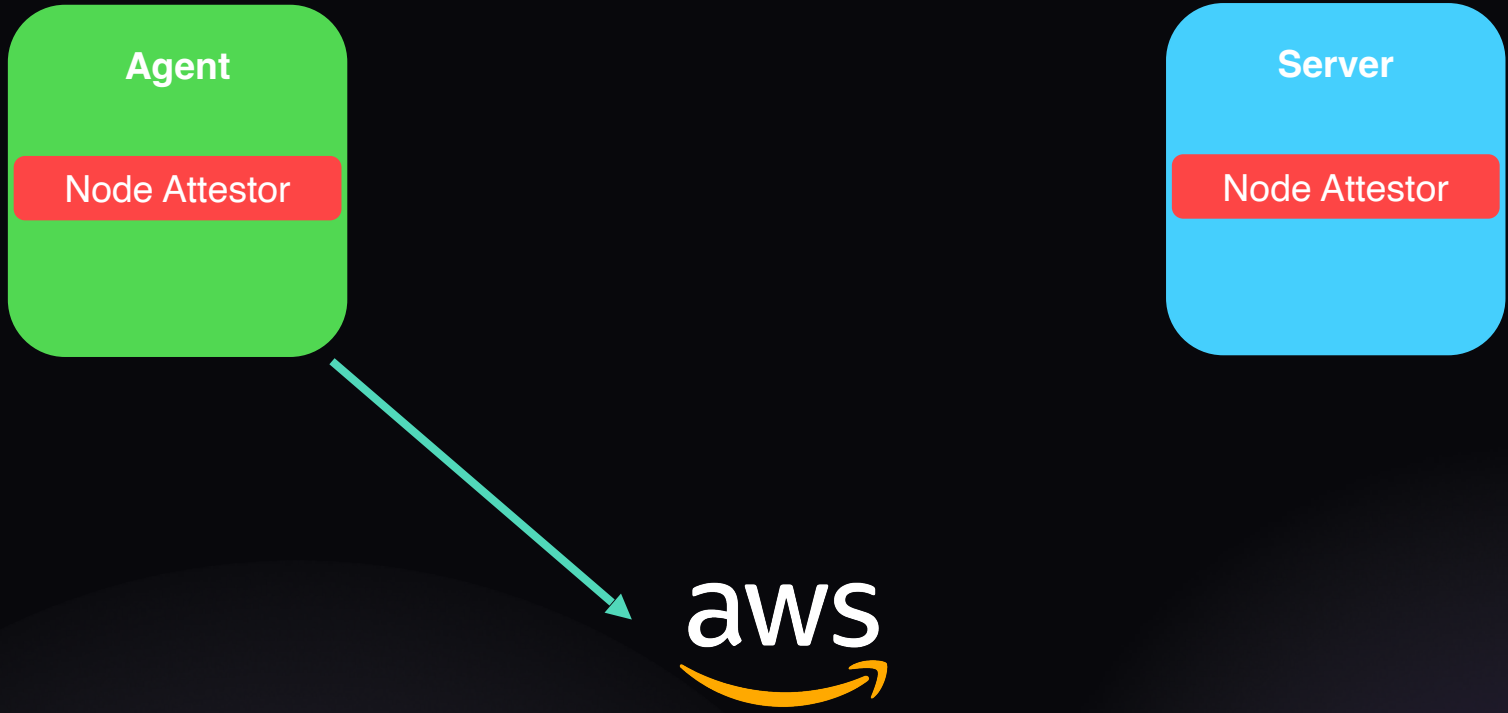
Europe 2023

SPIRE


Agent


Server


Agent
Node Attestor
Server
Node Attestor


Agent
Node Attestor
Server
Node Attestor
aws


Agent
Node Attestor
Server
Node Attestor
aws


Agent
Node Attestor
Server
Node Attestor
aws
This is the bottom turtle!


Agent
Node Attestor
Server
Node Attestor
aws


Agent
Node Attestor
Server
Node Attestor
JWT/X509
aws

KubeCon CloudNativeCon Europe 2023

Allows the secure issuance of SVID documents in both JWT and X.509 formats.

KubeCon | CloudNativeCon

Europe 2023

- Allows the secure issuance of SVID documents in both JWT and X.509 formats.
- Can verify SVIDs of other workloads

KubeCon | CloudNativeCon

Europe 2023

- Allows the secure issuance of SVID documents in both JWT and X.509 formats.
- Can verify SVIDs of other workloads
- Has an emerging ecosystem of plugins to integrate with other tools and services

Calling SPIRE needs changes to your app

KubeCon CloudNativeCon Europe 2023

Calling SPIRE needs changes to your app

For enterprises, it’s another point of required integration with private PKI

Calling SPIRE needs changes to your app

For enterprises, it’s another point of required integration with private PKI

It is another stateful service to maintain. In HA configurations that usually means a dedicated database.

KubeCon | CloudNativeCon

Europe 2023

Hold on…

KubeCon | CloudNativeCon
Europe 2023

Could we just use cert-manager?

KubeCon | CloudNativeCon
Europe 2023

cert-manager makes the world of distributing identity documents more easy, accessible and safe on Kubernetes.

KubeCon CloudNativeCon Europe 2023

- cert-manager makes the world of distributing identity documents more easy, accessible and safe on Kubernetes.
- It provides those identity documents in X.509 format, and rotating them is automated and simple.

- cert-manager makes the world of distributing identity documents more easy, accessible and safe on Kubernetes.
- It provides those identity documents in X.509 format, and rotating them is automated and simple.
- It supports a wide variety of certificate issuers (both private and public).

csi-driver-spiffe

Introducing csi-driver-spiffe!

csi-driver-spiffe

- Container Storage Interface (CSI) driver plugin for Kubernetes.
- Creates, delivers and renews X.509 SVIDs for pods.

csi-driver-spiffe

- Container Storage Interface (CSI) driver plugin for Kubernetes.
- Creates, delivers and renews X.509 SVIDs for pods.

The private key for the SVID never leaves the node's memory (tmpfs).

csi-driver-spiffe

- Container Storage Interface (CSI) driver plugin for Kubernetes.
- Creates, delivers and renews X.509 SVIDs for pods.

The private key for the SVID never leaves the node's memory (tmpfs).

No extra CRDs.

csi-driver-spiffe

- Container Storage Interface (CSI) driver plugin for Kubernetes.
- Creates, delivers and renews X.509 SVIDs for pods.

- The private key for the SVID never leaves the node's memory (tmpfs).
- No extra CRDs.
- No extra databases.

csi-driver-spiffe

cert-manager can only do X.509

csi-driver-spiffe

Thank god it’s better than JWT 😉

csi-driver-spiffe

- X.509 private keys are never shared ("passwordless")
- SPIFFE authorization incorporated during TLS handshake

csi-driver-spiffe

Why?

csi-driver-spiffe

X.509 private keys are never shared ("passwordless")

csi-driver-spiffe

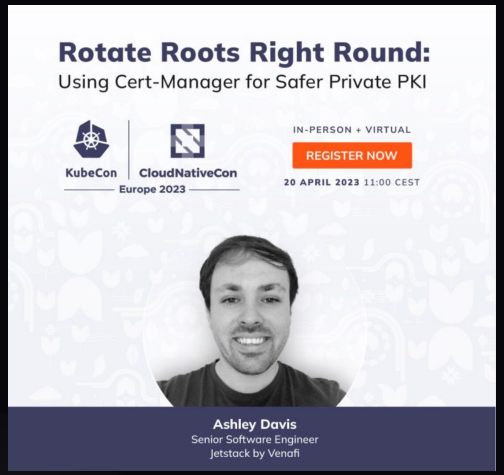
- X.509 private keys are never shared ("passwordless")
- SPIFFE authorization incorporated during TLS handshake

csi-driver-spiffe

- ✅ X.509 private keys are never shared ("passwordless")
- ✅ SPIFFE authorization incorporated during TLS handshake

- ❌ You do have to handle the distribution of trust bundles 😔

🎉 trust-manager



❌ You do have to handle the distribution of trust bundles 😔

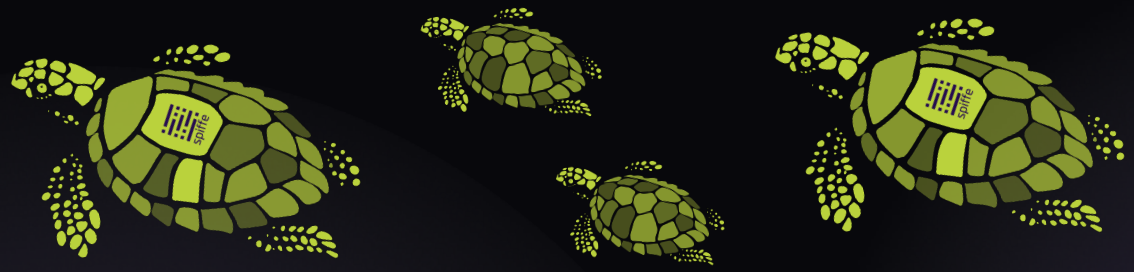
csi-driver-spiffe

csi-driver-spiffe

What's the bottom turtle?

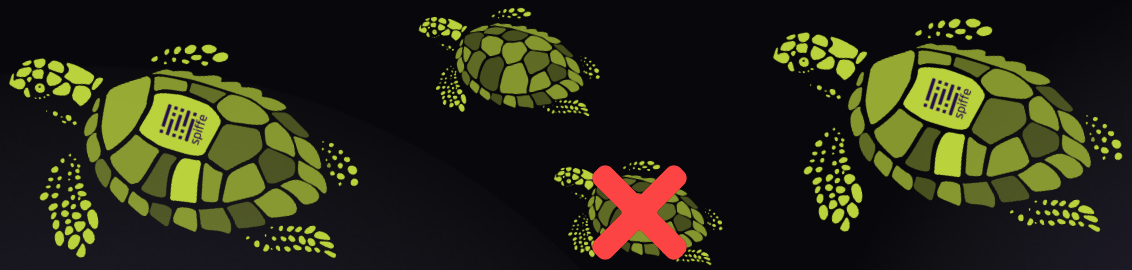
csi-driver-spiffe

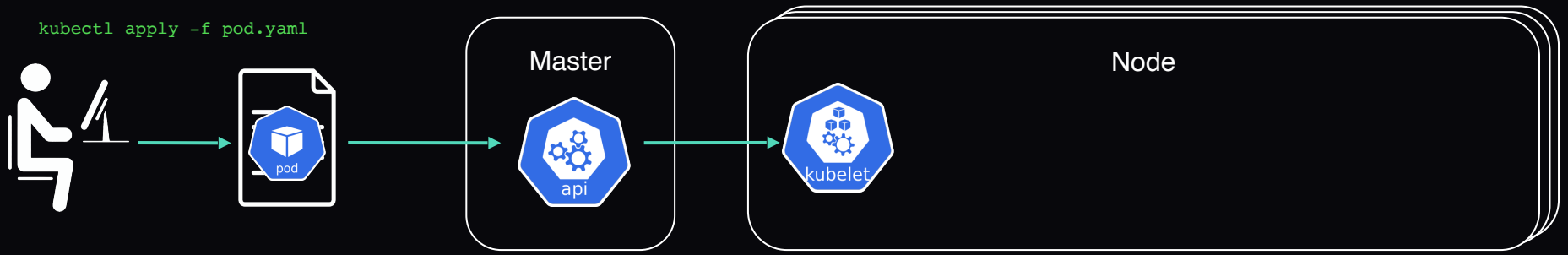
What's the bottom turtle?

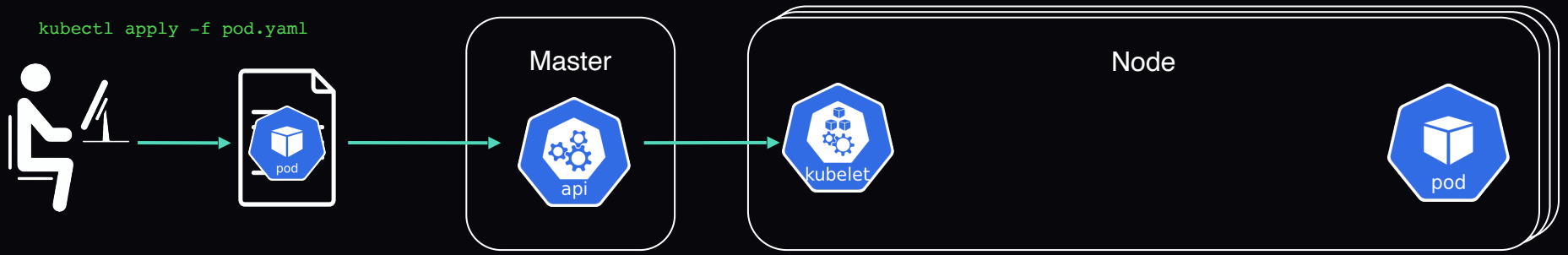


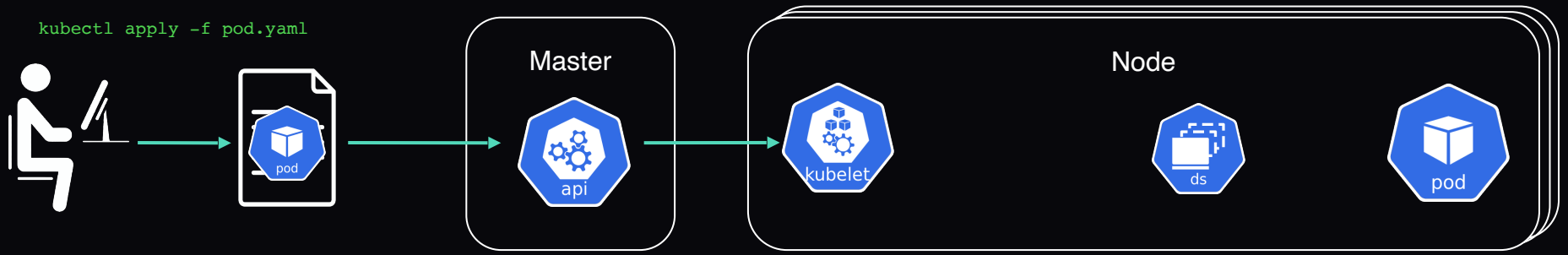
csi-driver-spiffe

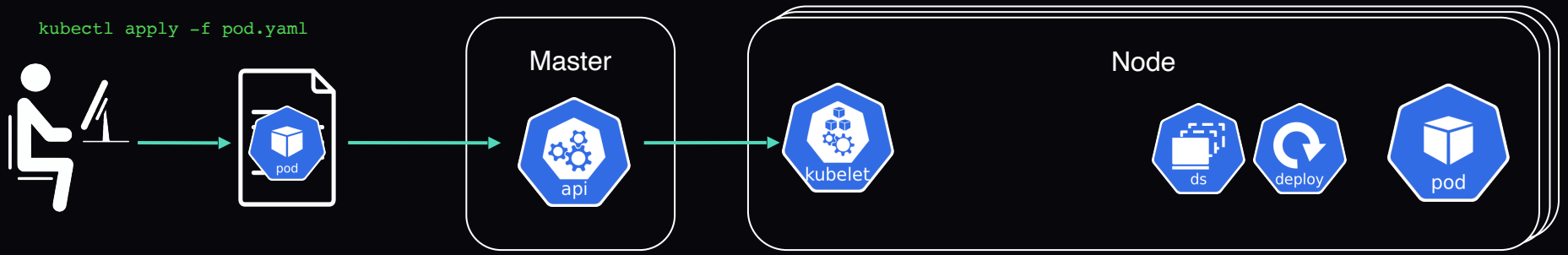
What's the bottom turtle?

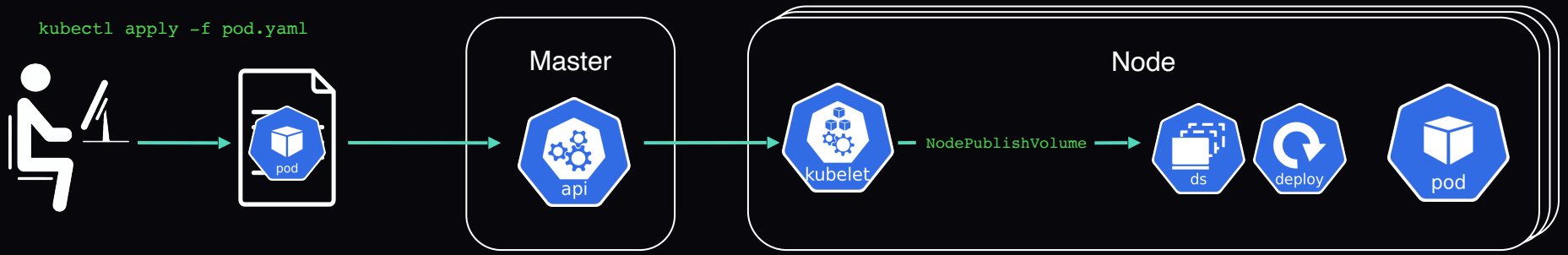


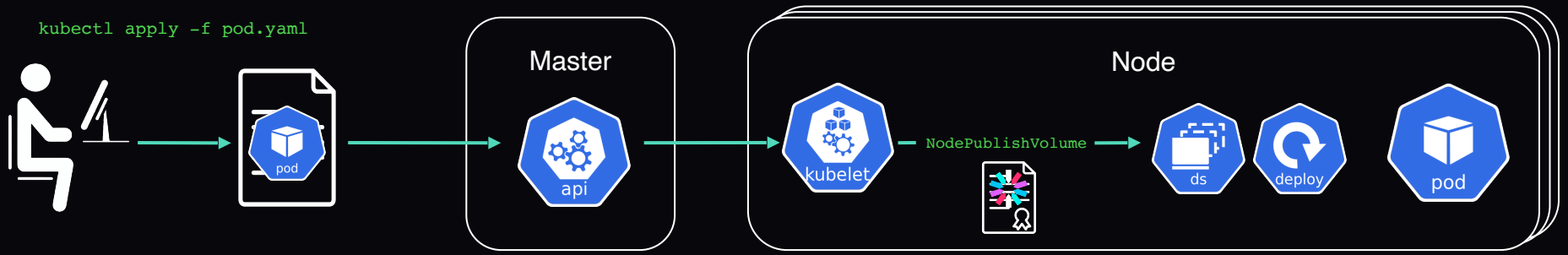

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet

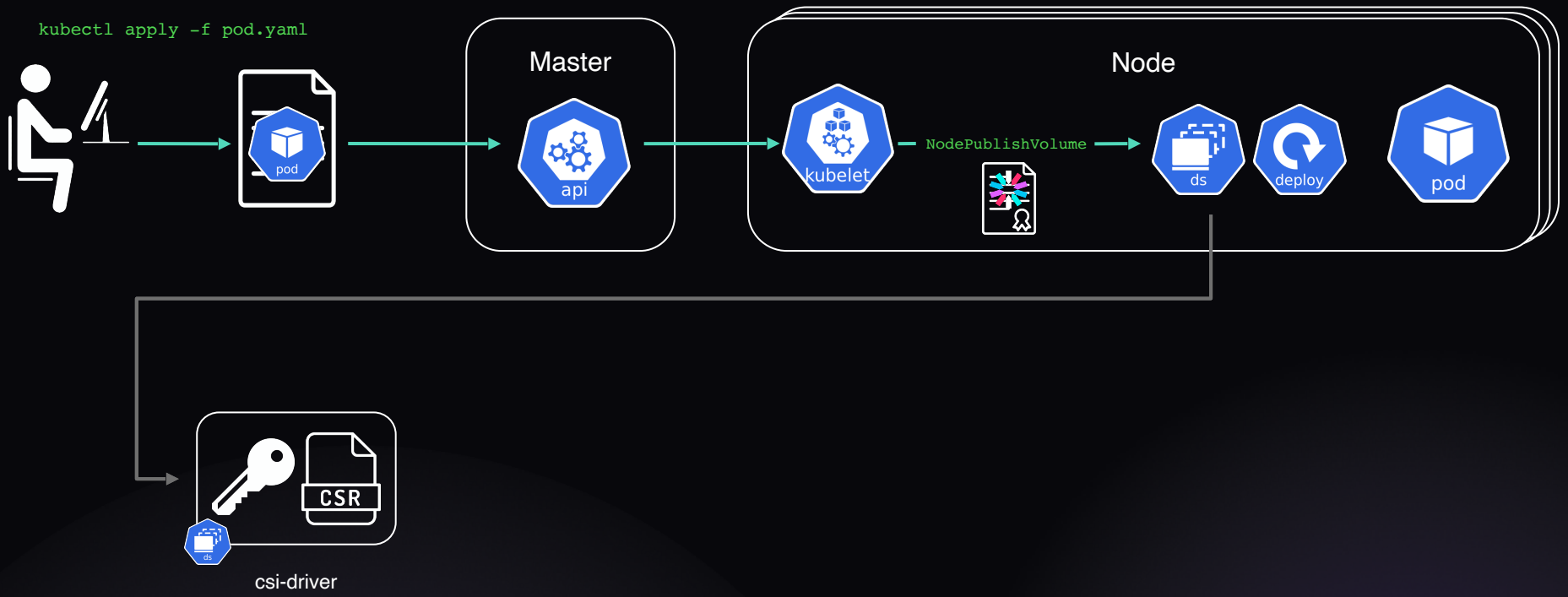

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
pod

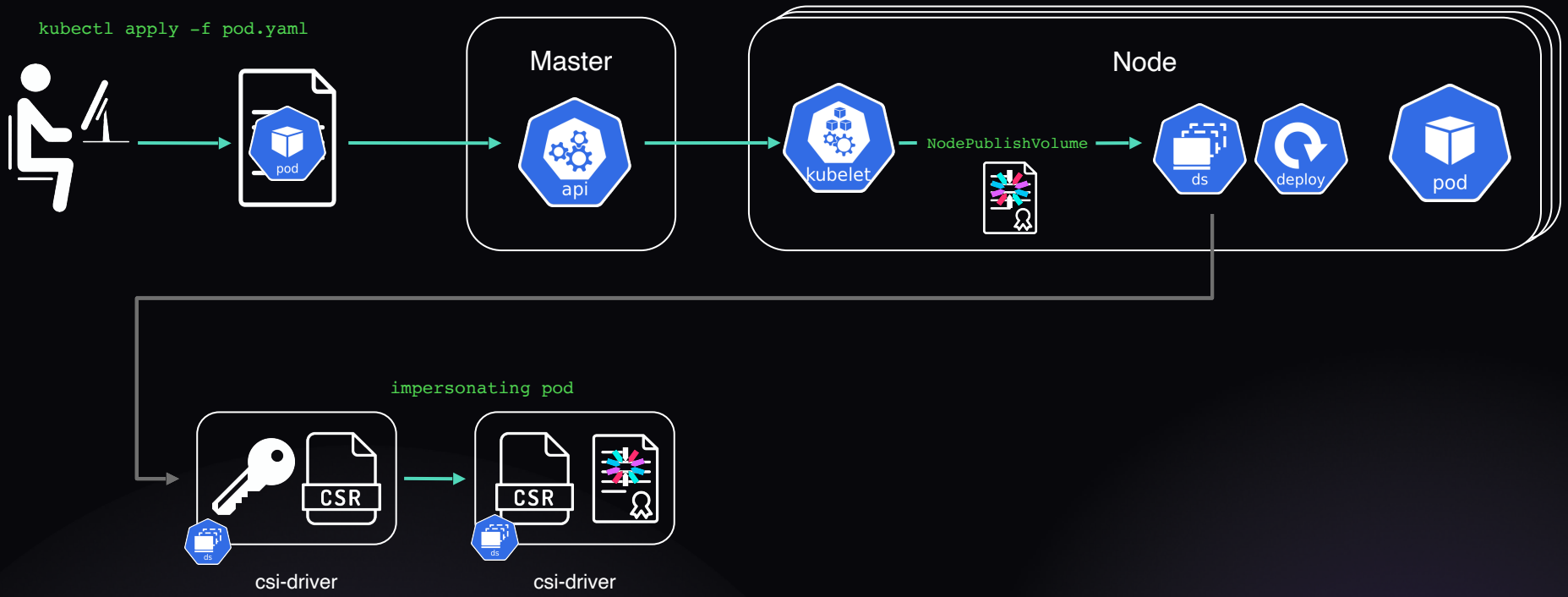

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
ds
pod

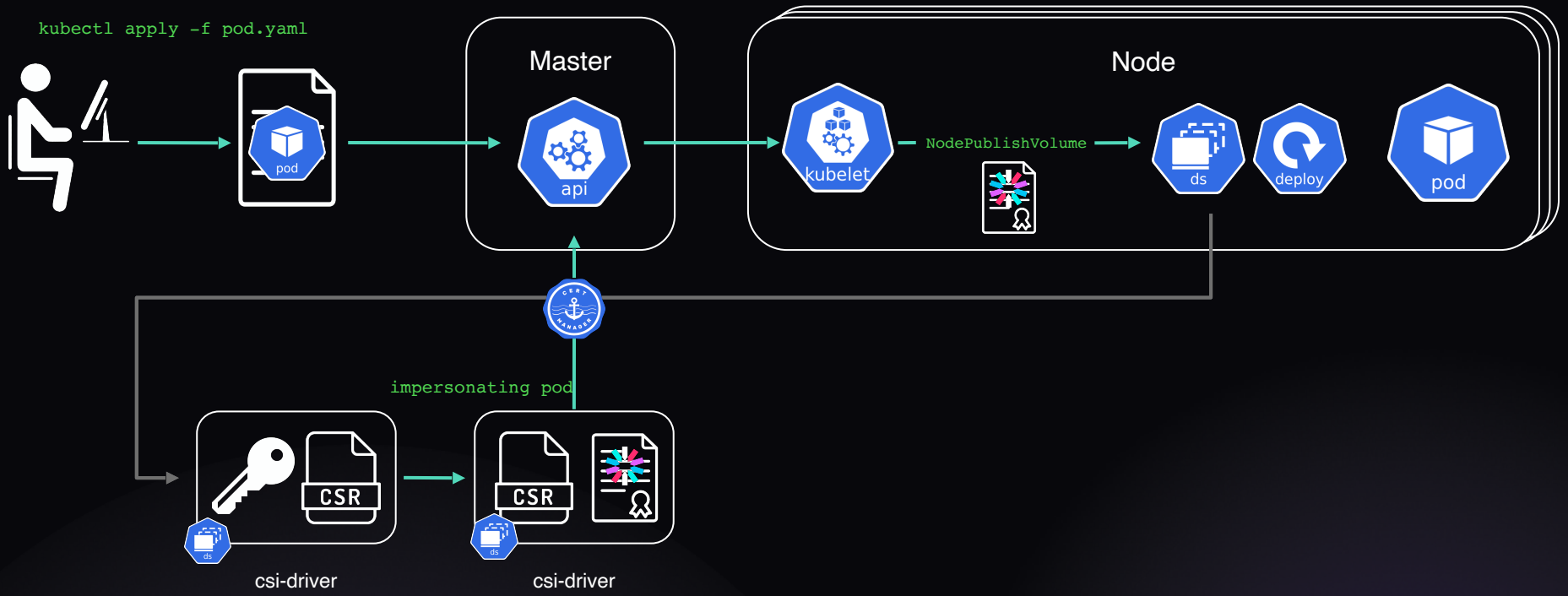

kubectl apply -f pod.yaml
pod
Master
api
kubelet
Node
ds
deploy
pod

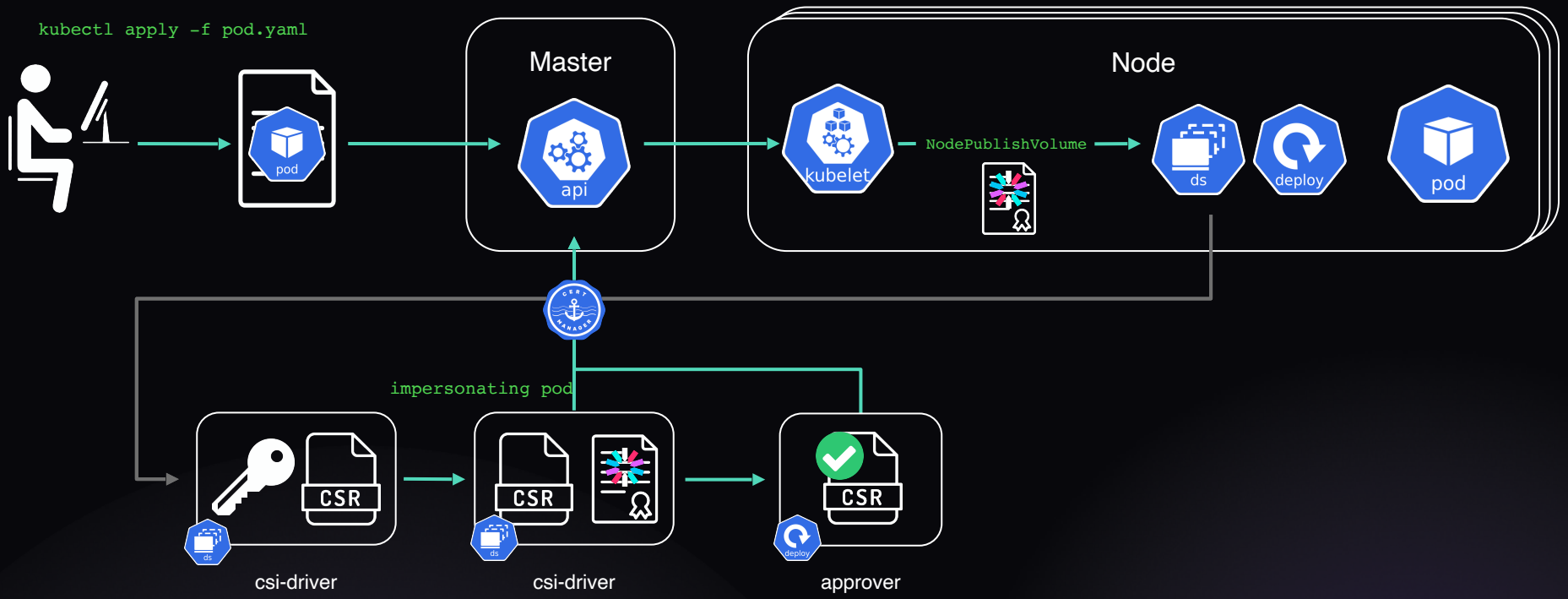

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod

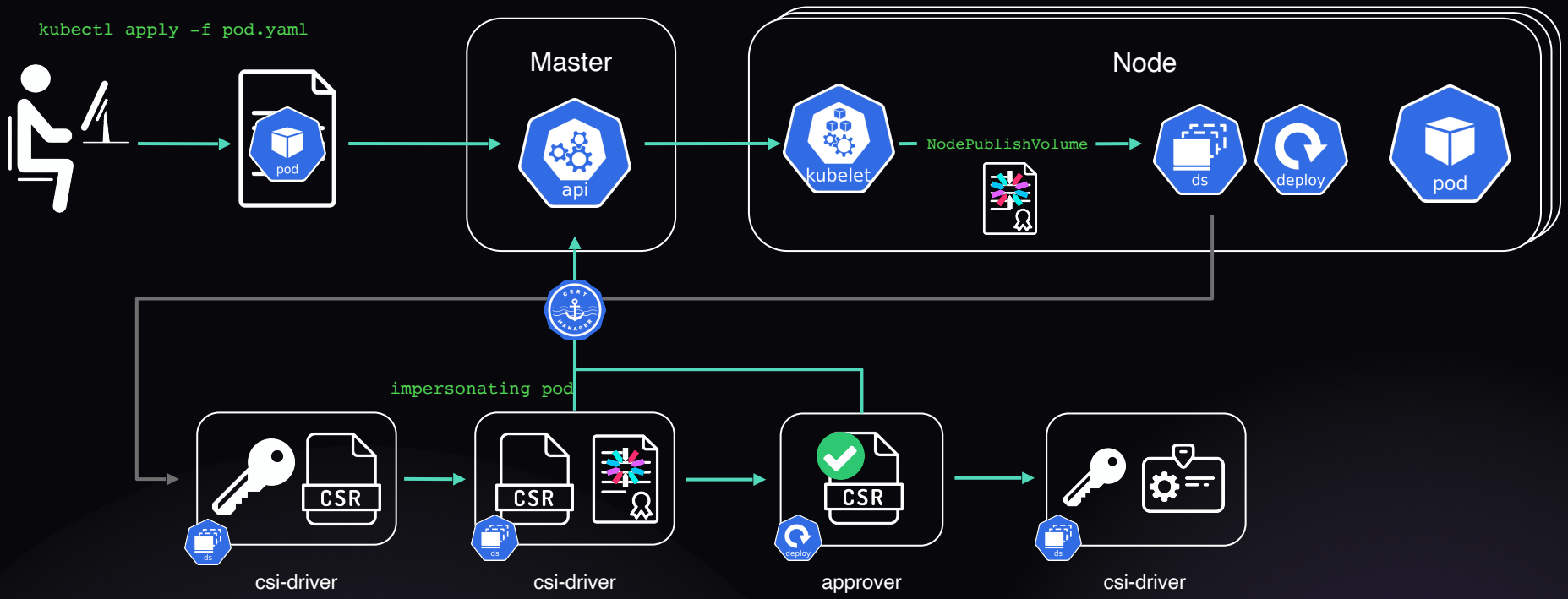

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod

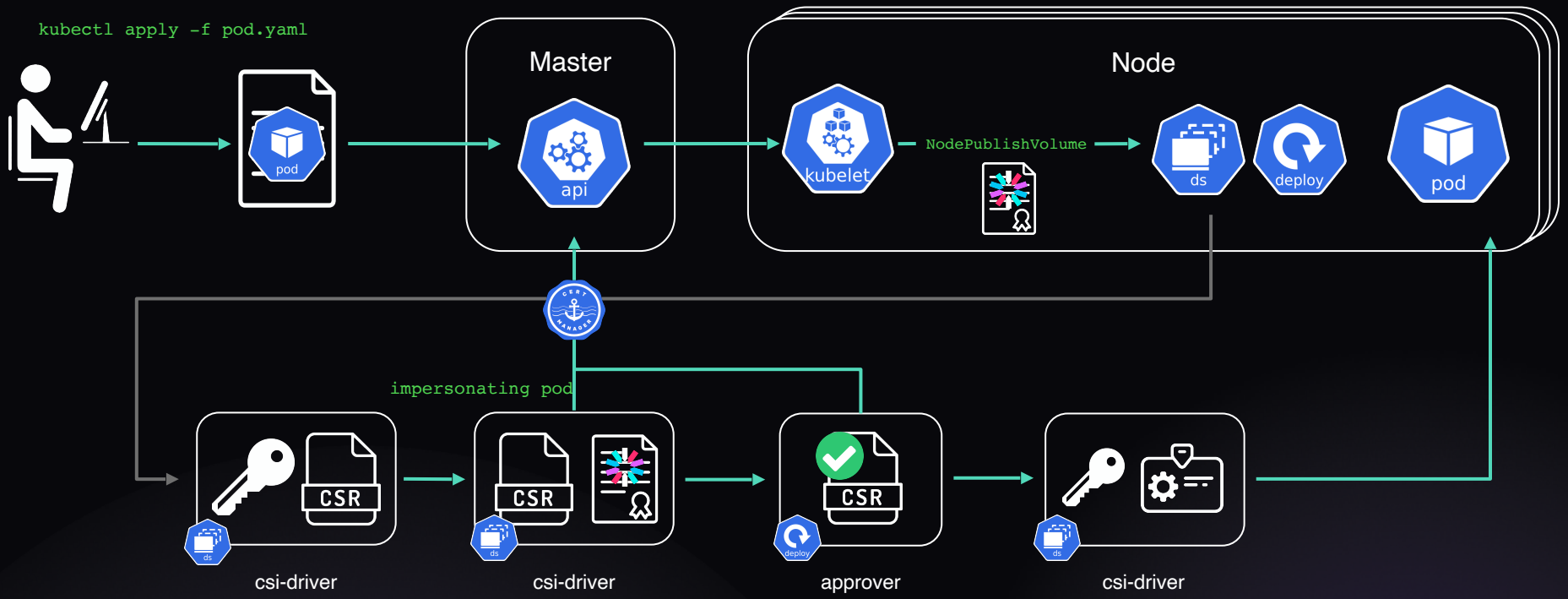

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
CSR
ds
csi-driver

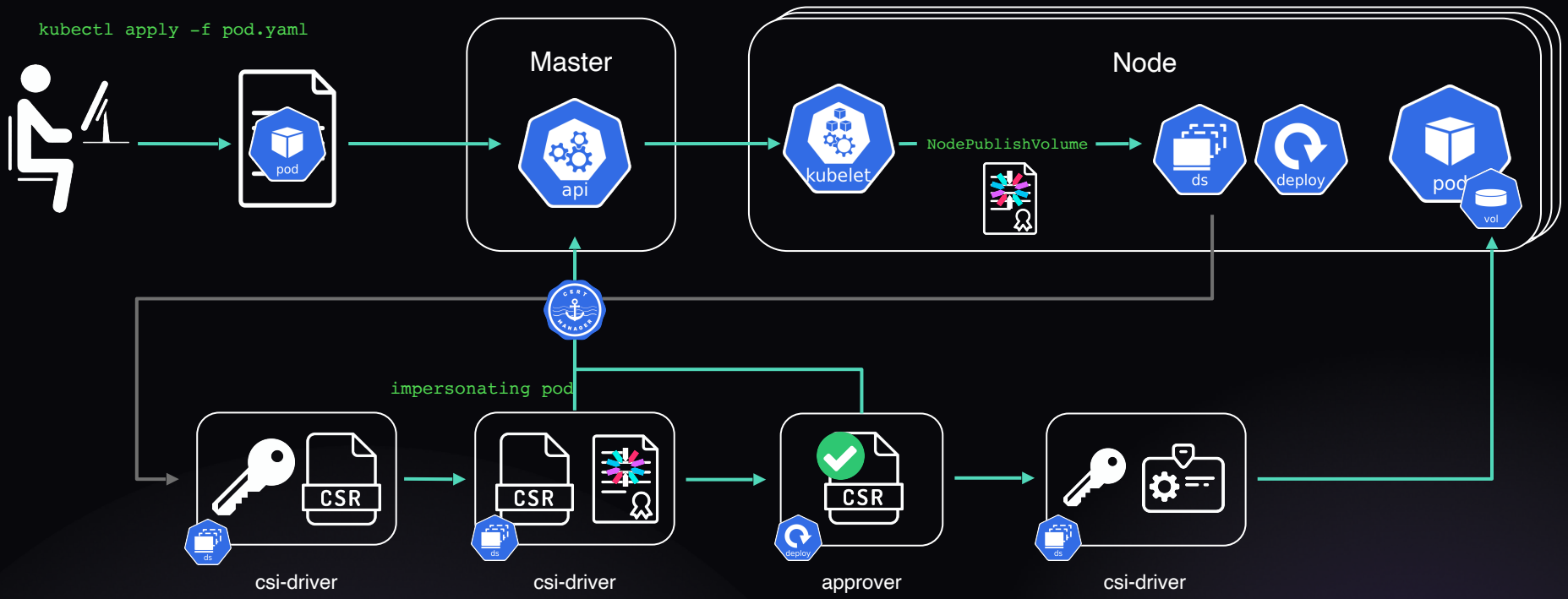

kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
impersonating pod
CSR
CSR
ds
ds
csi-driver
csi-driver


kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
impersonating pod
CSR
CSR
csi-driver
csi-driver


kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
impersonating pod
CSR
CSR
CSR
csi-driver
csi-driver
approver


kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
impersonating pod
CSR
CSR
CSR
csi-driver
csi-driver
approver
csi-driver


kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
impersonating pod
CSR
CSR
CSR
csi-driver
csi-driver
approver
csi-driver


kubectl apply -f pod.yaml
pod
Master
api
Node
kubelet
NodePublishVolume
ds
deploy
pod
vol
impersonating pod
CSR
CSR
CSR
csi-driver
csi-driver
approver
csi-driver

csi-driver-spiffe

Please stop with the slides.

Show me the demo already 🙄

csi-driver-spiffe

Having said all this…

csi-driver-spiffe

csi-driver-spiffe might not always be the right fit

csi-driver-spiffe

csi-driver-spiffe might not always be the right fit

But SPIRE might!

KubeCon | CloudNativeCon

Europe 2023

Fully supports JWT document format for SVIDs

KubeCon | CloudNativeCon

Europe 2023

SPIRE

- Fully supports JWT document format for SVIDs
- Enables workload attestation for not just Kubernetes but beyond

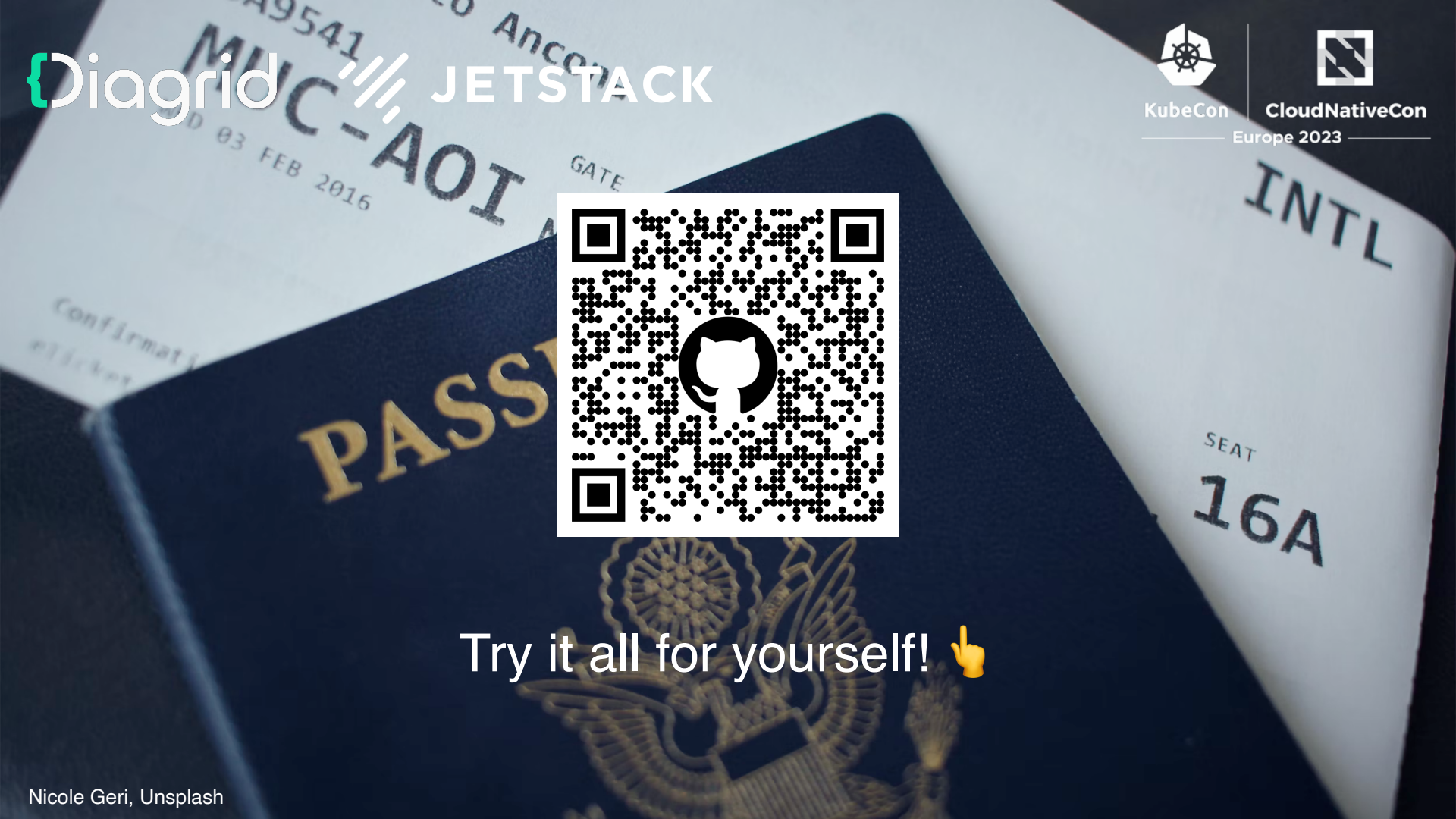
KubeCon | CloudNativeCon

Europe 2023

SPIRE

- Fully supports JWT document format for SVIDs
- Enables workload attestation for not just Kubernetes but beyond
- Implements workload APIs

However you do authentication, use SPIFFE!


Diagrid
JETSTACK
KubeCon
CloudNativeCon
Europe 2023
Try it all for yourself! 👆
Nicole Geri, Unsplash