

spiffe://kubernetes/every/object

Every Kubernetes Object Deserves an Identity

The SPIFFE Broker API



ABOUT ME

Arndt Schwenkschuster

Maintainer @ SPIFFE

Contributor to OAuth & WIMSE @ IETF

Defakto Security

What SPIFFE is used for today

Service authentication

- Secretless authentication & resource access
- Service mesh identity
- Certificate & trust provisioning

Identity layer

- Across platforms
- Cross-cloud
- Cross-cluster

Bootstrap identity

- On-prem
- Hardware attestation
- Multi-factor attestation

Agent identity

- Autonomous agents
- OAuth client authentication

Secure Production Identity Framework for Everyone

FORMAT

SPIFFE ID

`spiffe://example.org/ns/prod/sa/api`

CREDENTIALS

SVID

`X.509` `JWT` `WIT`

DELIVERY

Workload API

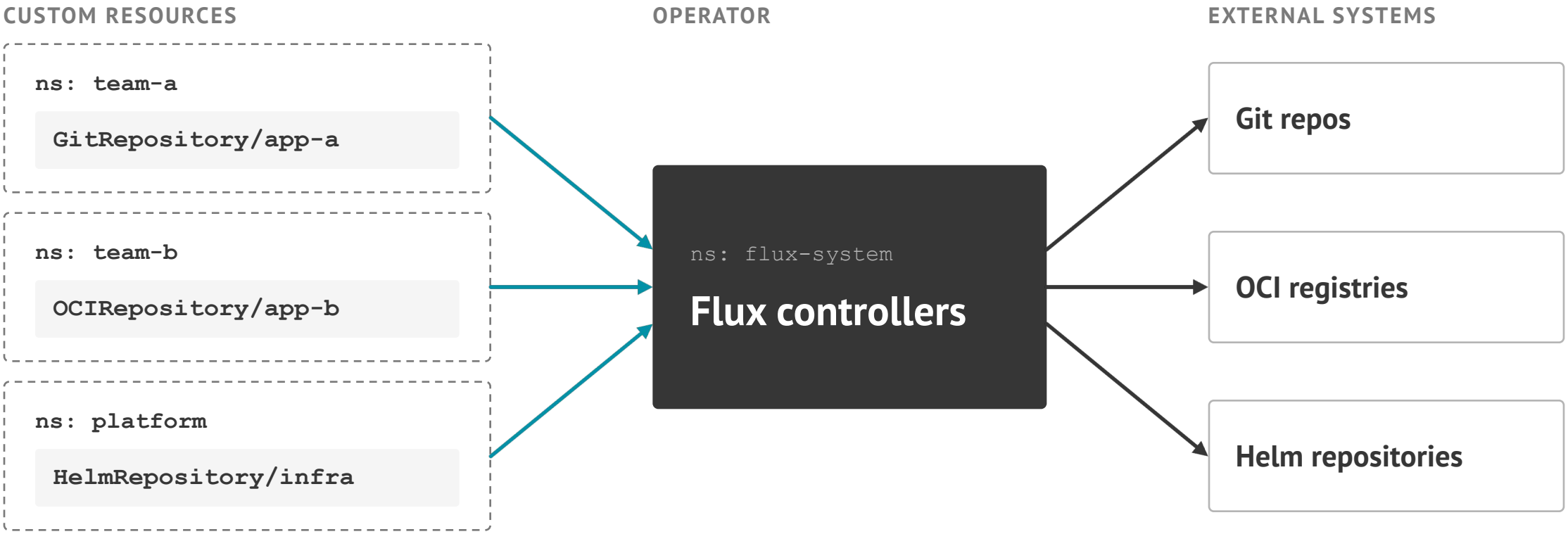
`Fetch*SVID` `Fetch*Bundle`

The Kubernetes operator pattern

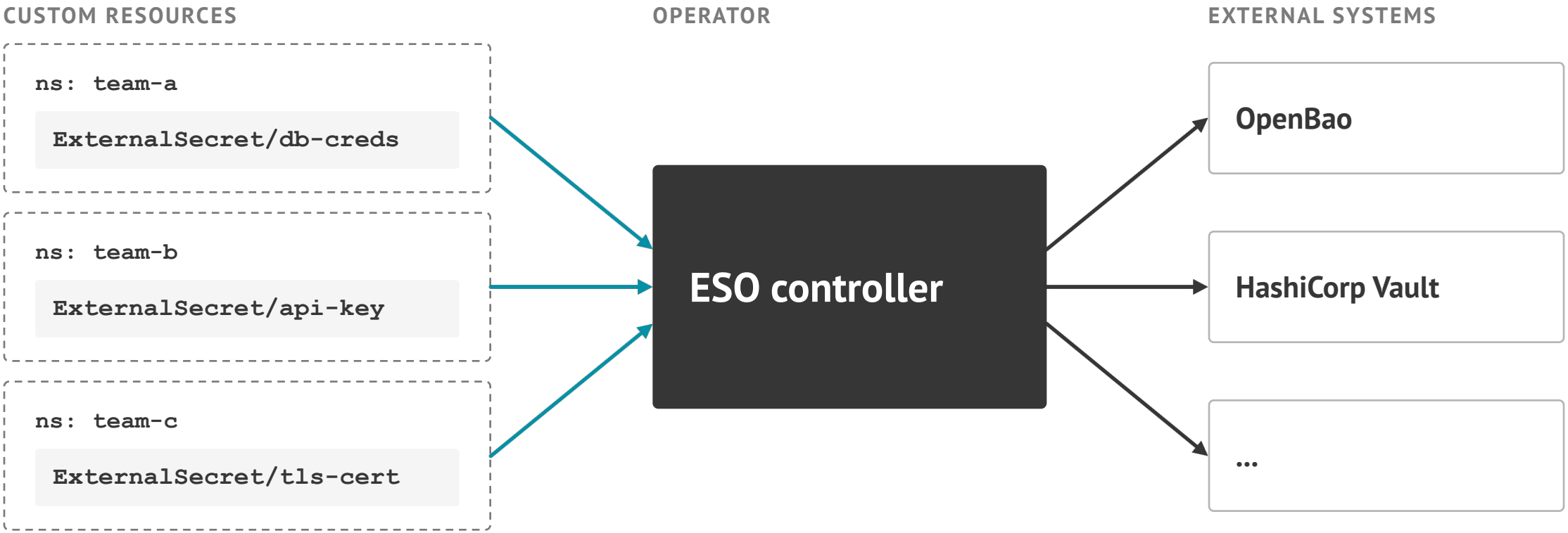




Example: Flux



Example: External Secrets Operator

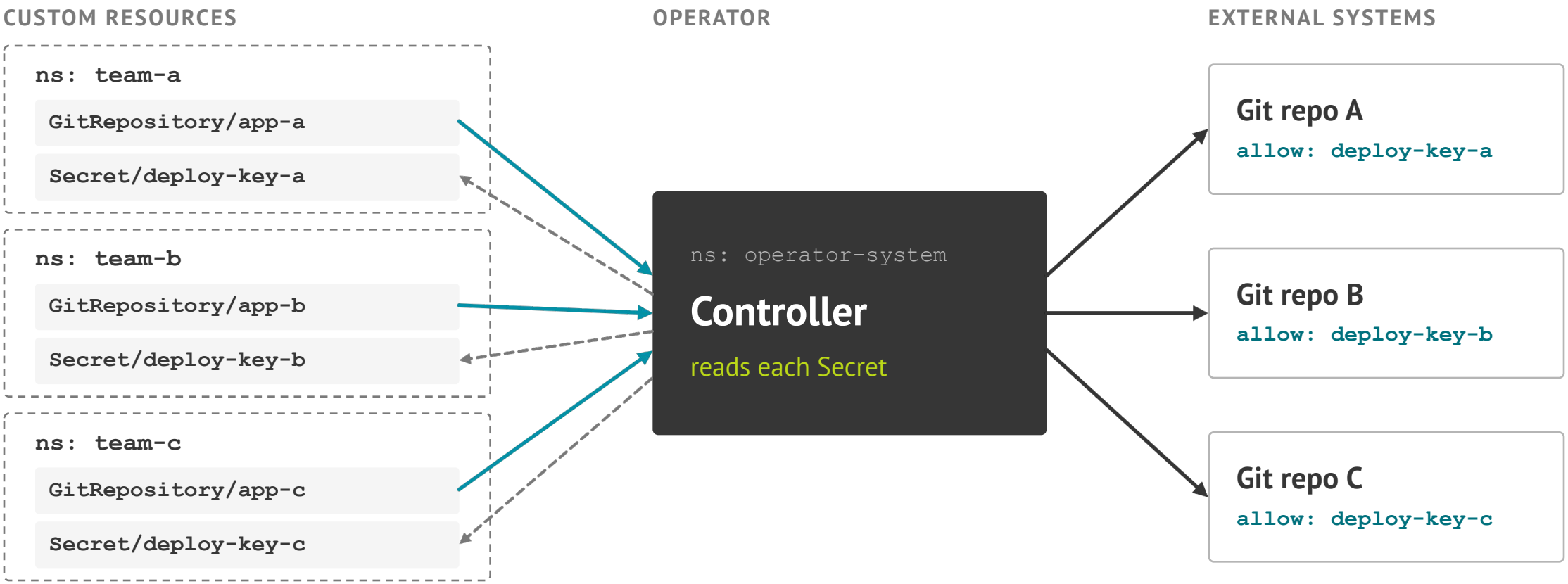


02

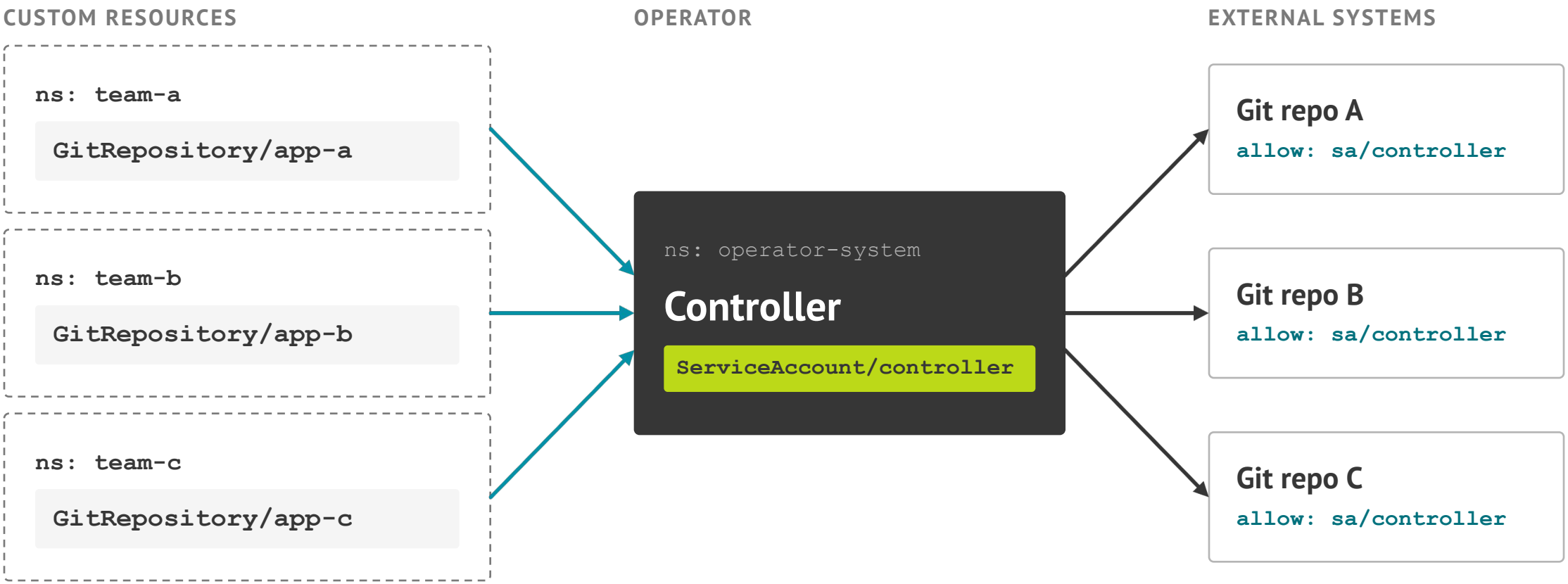
Situation today

How operators get identity for external systems

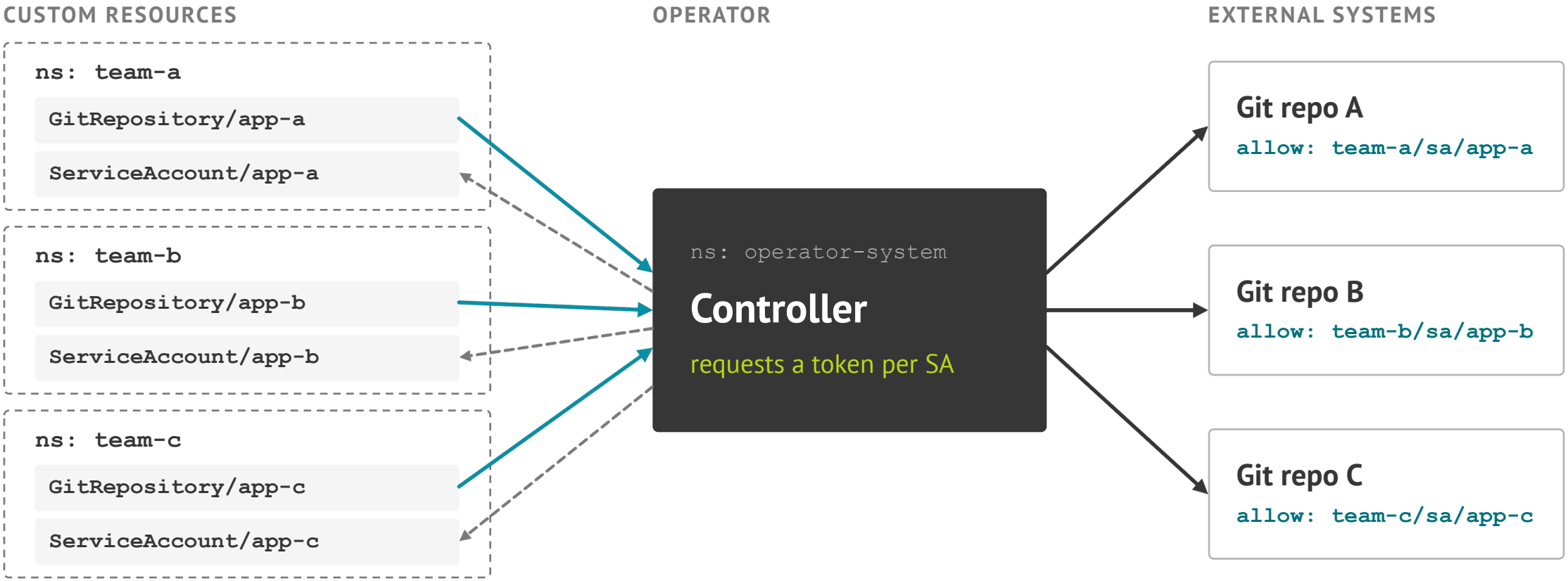
Option 1: Static keys



Option 2: The operator's Service Account



Option 3: A Service Account per object



What if the object itself got a SPIFFE ID?

GITREPOSITORY

```
spiffe://example.org/ns/team-a/gitrepository/app-a
```

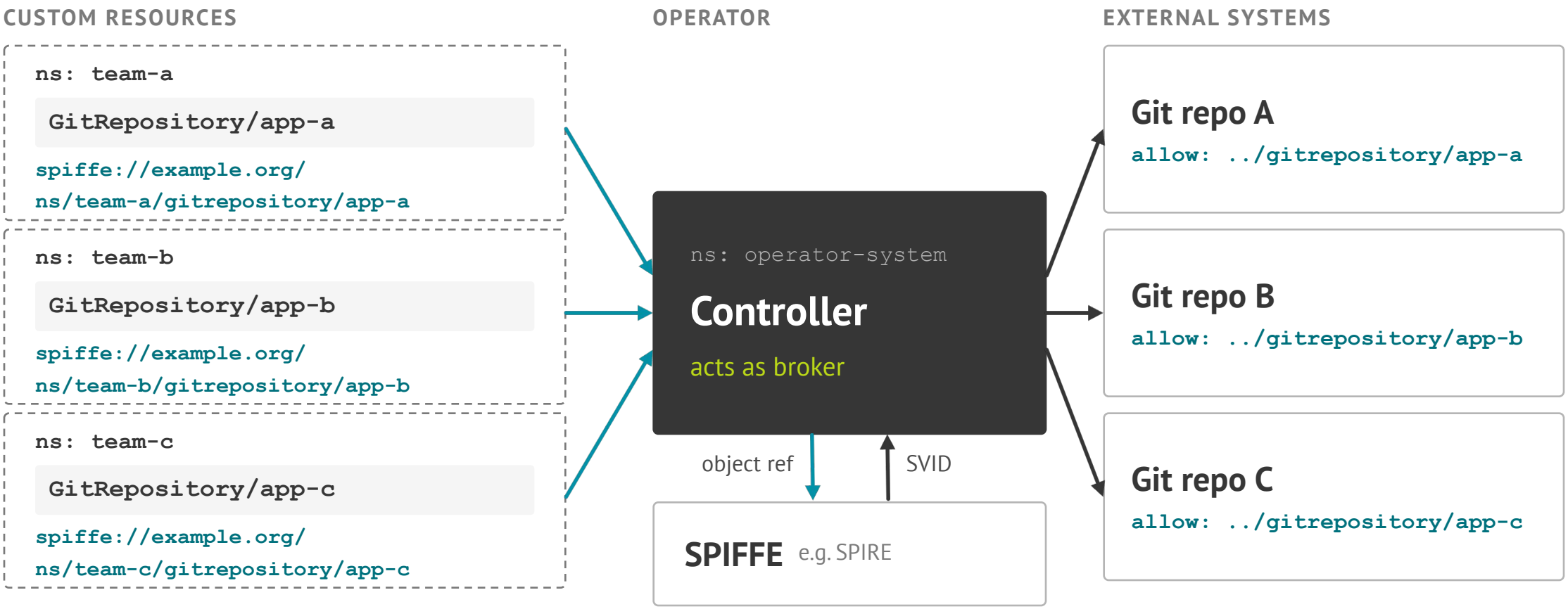
SECRET

```
spiffe://example.org/ns/team-a/secret/db-credentials
```

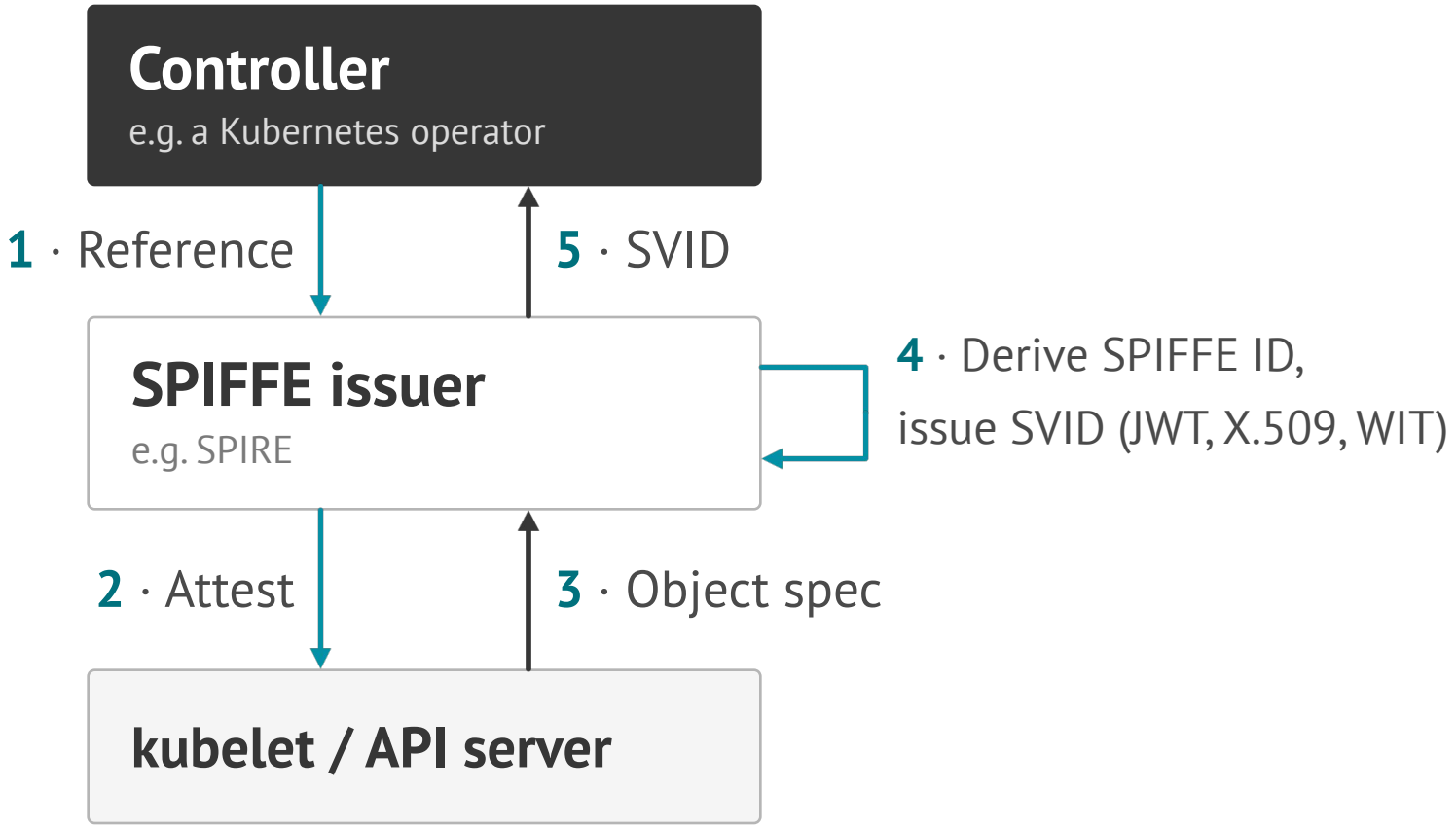
CONFIGMAP

```
spiffe://example.org/ns/team-a/configmap/feature-flags
```

The same operator, with SPIFFE IDs



The SPIFFE Broker API



Built-in reference types

```
KubernetesObjectReference
group: source.toolkit.fluxcd.io
plural: gitrepositories
namespace: team-a
name: app-a
uid: [uid]
```

```
WorkloadPIDReference
pid: 4242
```

CUSTOM REFERENCES

systemd units

Task references

Custom process orchestrators

…

05

In practice

Flux, Argo CD, Istio and External Secrets Operator

spiffe



Flux

GitRepository

`source-controller`

Git hosts

OCIRepository

`source-controller`

Container registries

HelmRepository

`source-controller`

Helm chart repositories

Others

Flux 2.10 supports the SPIFFE Broker API

spiffe



Argo CD

App source

`repo-server`

Git hosts and Helm registries

App destination

`application-controller`

Remote clusters

ApplicationSet

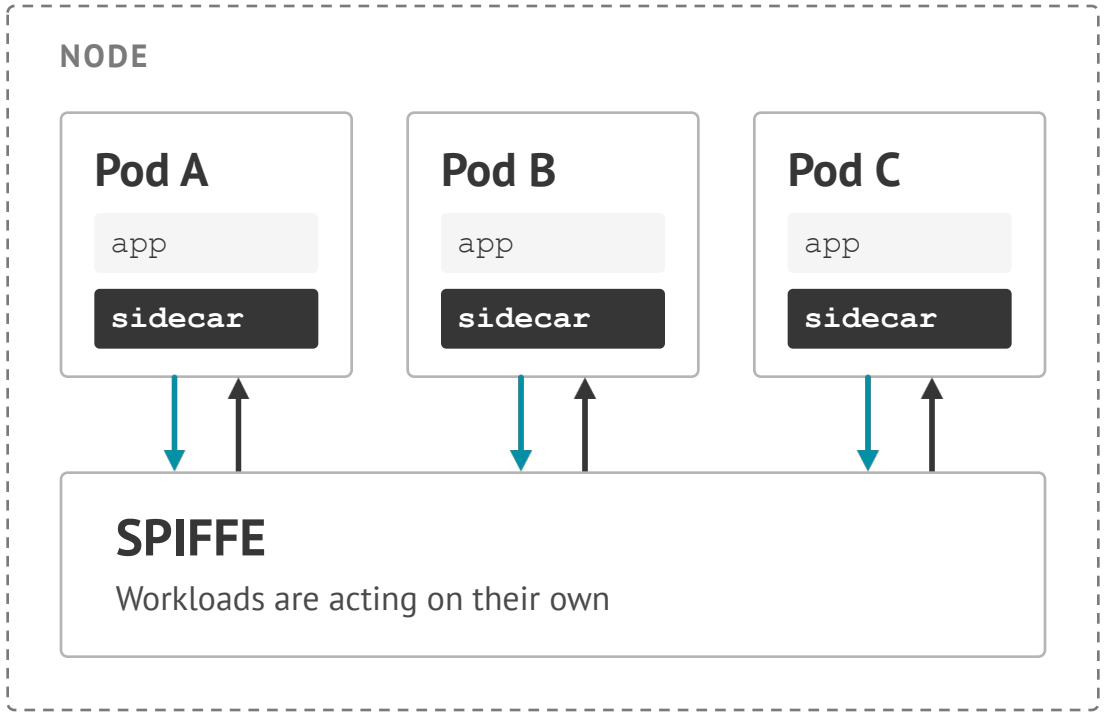
`applicationset-controller`

SCM providers for generators

Others

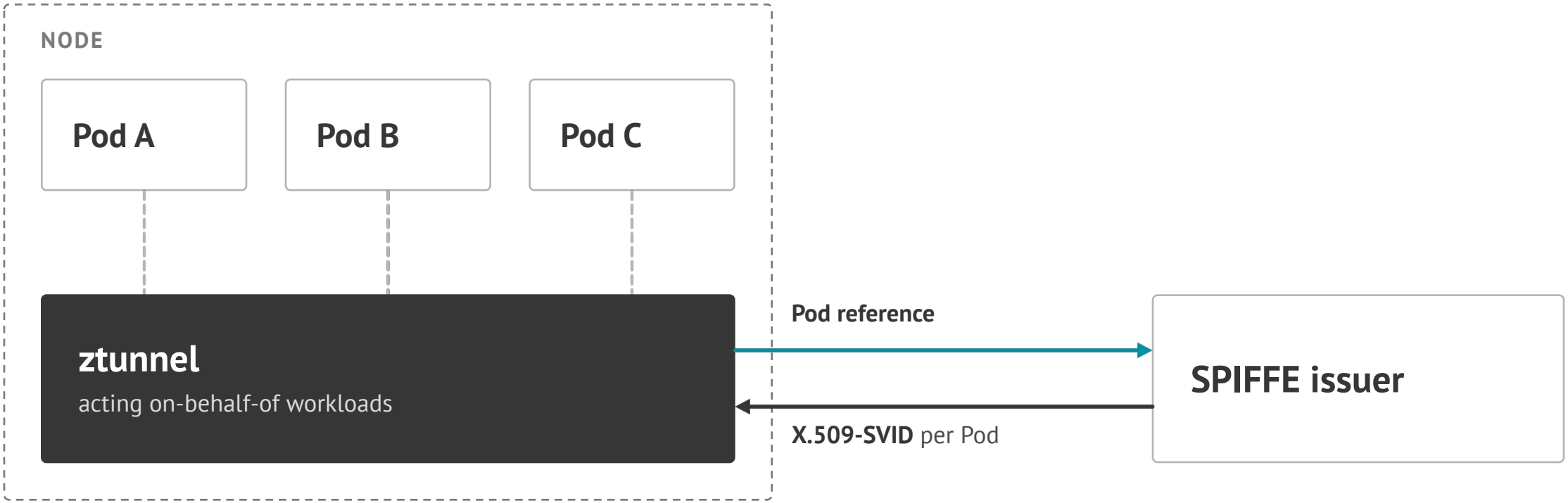
Talks started

Istio Sidecar Mode



Works today: Standard SPIFFE Workload API

Istio Ambient Mode



In progress: SPIFFE Broker API is being added to Istio



External Secrets Operator

SecretStore

`external-secrets`

Provider connection and auth

ExternalSecret

`external-secrets`

Fetch from secret managers

PushSecret

`external-secrets`

Push to secret managers

Others

Theoretical: no implementation yet

Vision: every operator is a broker

For operator builders

A standard, easy way to add authn/z support

For platform teams

Standardized identity across operators and clusters

For resource owners

Fine-grained policies and provenance

For security teams

Strong identity controls and auditing

THANK YOU

Build a broker with us

Join **#sig-spec** on SPIFFE Slack · meeting weekly

Questions?

spiffe