KubeCon

CloudNativeCon

China 2018

Istio Certificate Management Through Vault

Lei Tang, Yonggang Liu, *Google LLC*.

Lei Tang

Software Engineer
Istio

Google Cloud

leitang@google.com

wechat: LTANG2015

Oliver (Yonggang) Liu

Software Engineer
Istio

Google Cloud

yonggangl@google.com

http://oliverliu.org

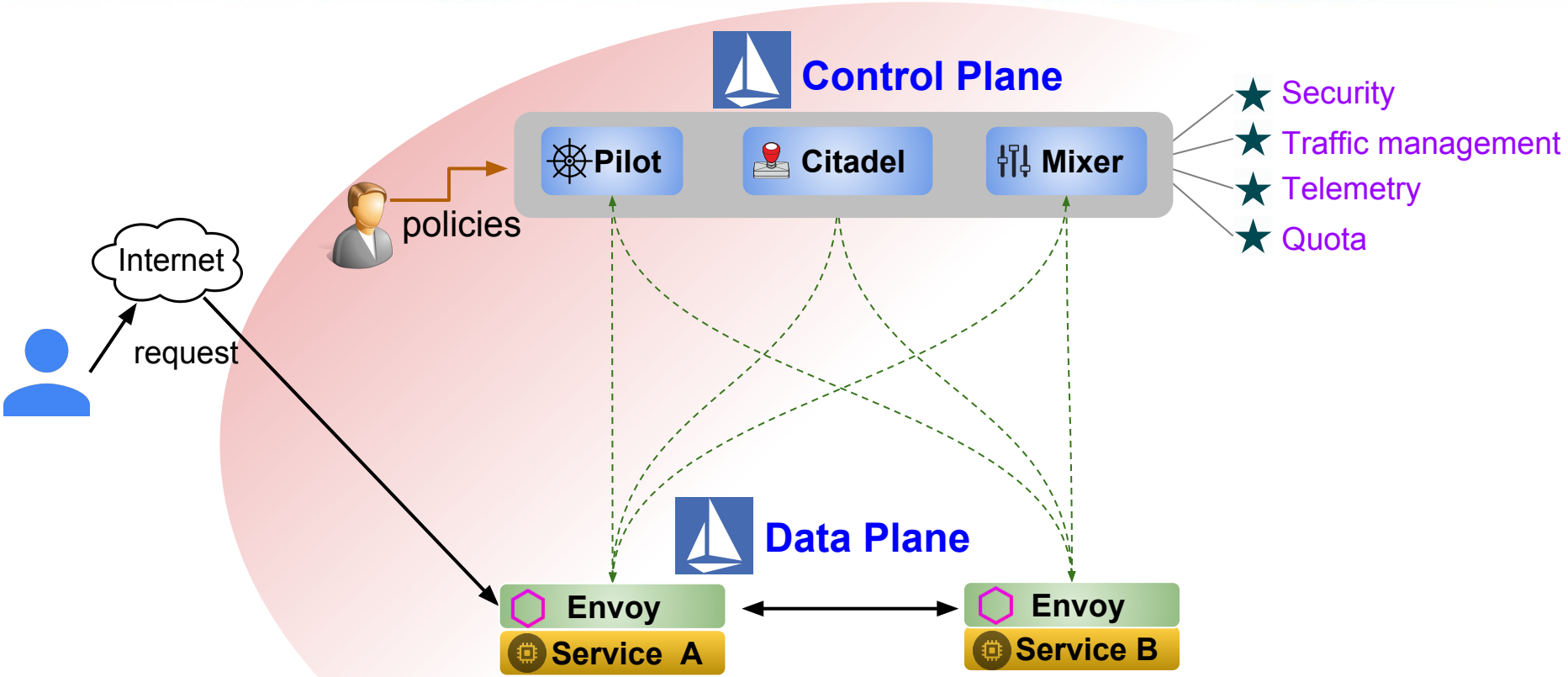
Istio manages your microservices

Relieve burden of service owners.

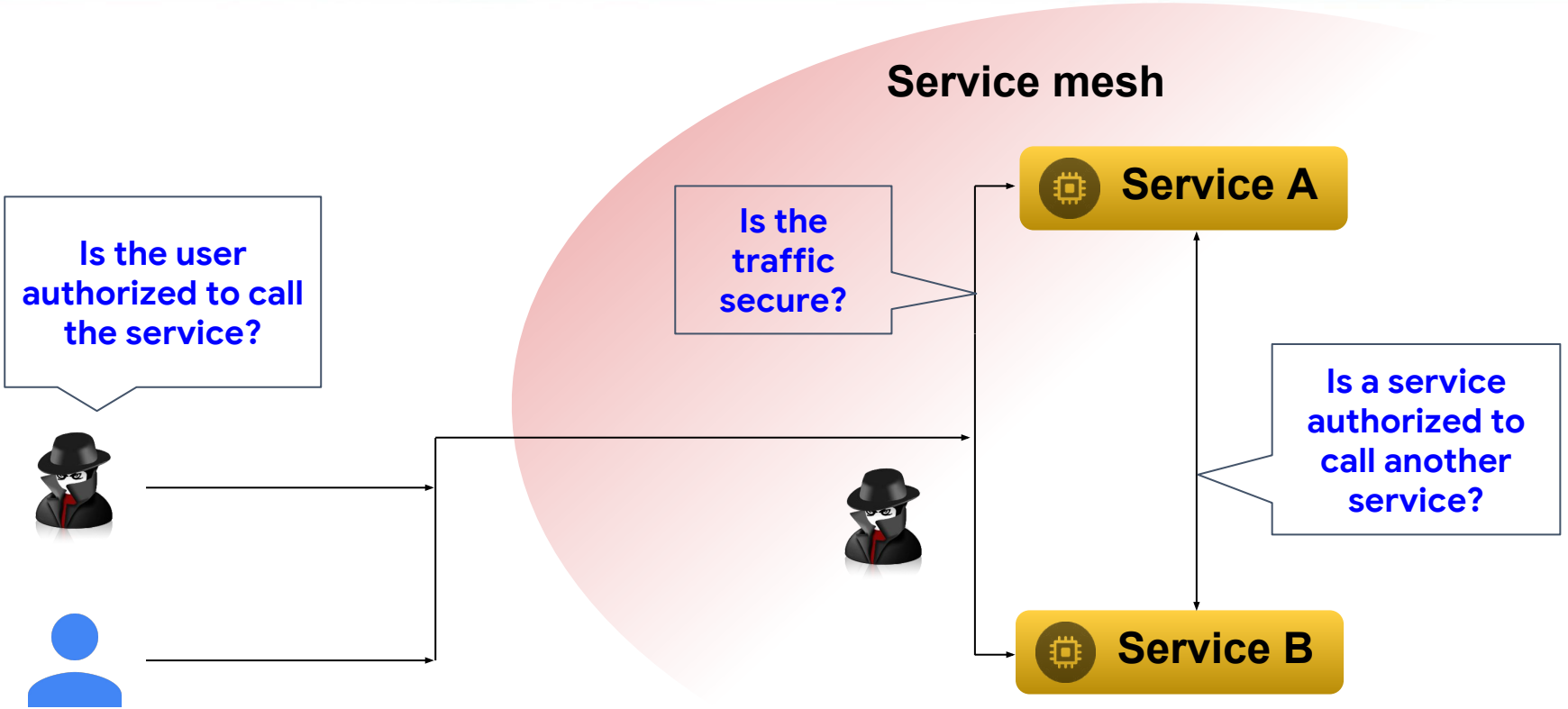
Bring order to chaos.

Photo credits

Istio 30,000-foot view

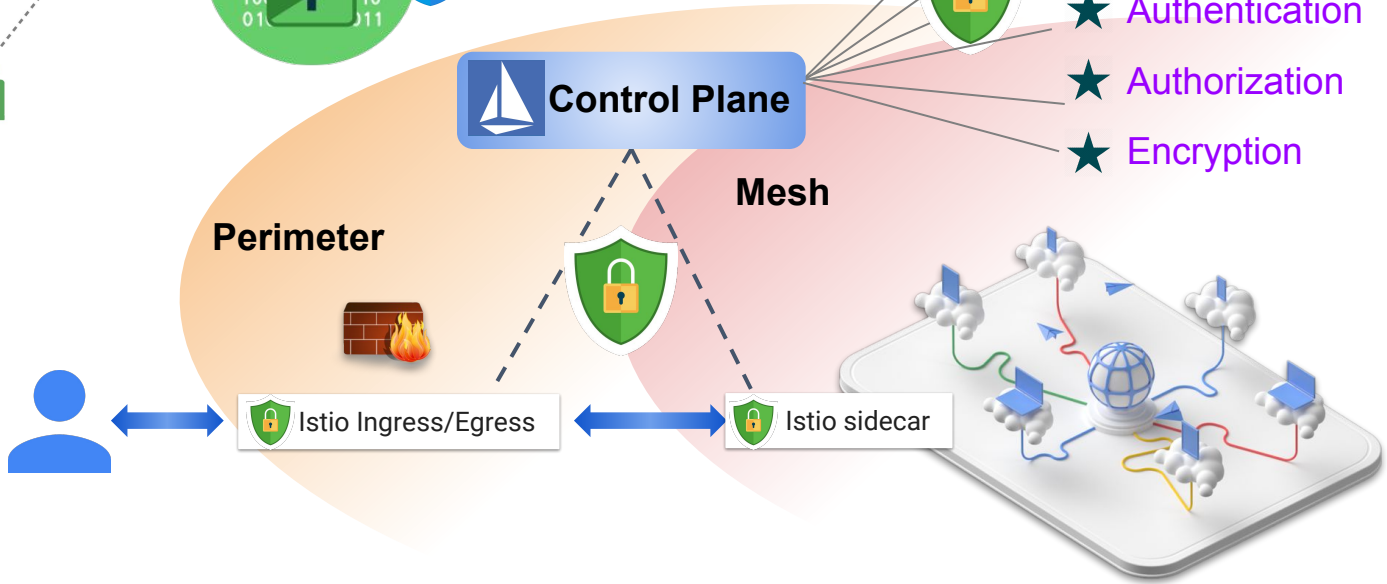


Security risks for service meshes

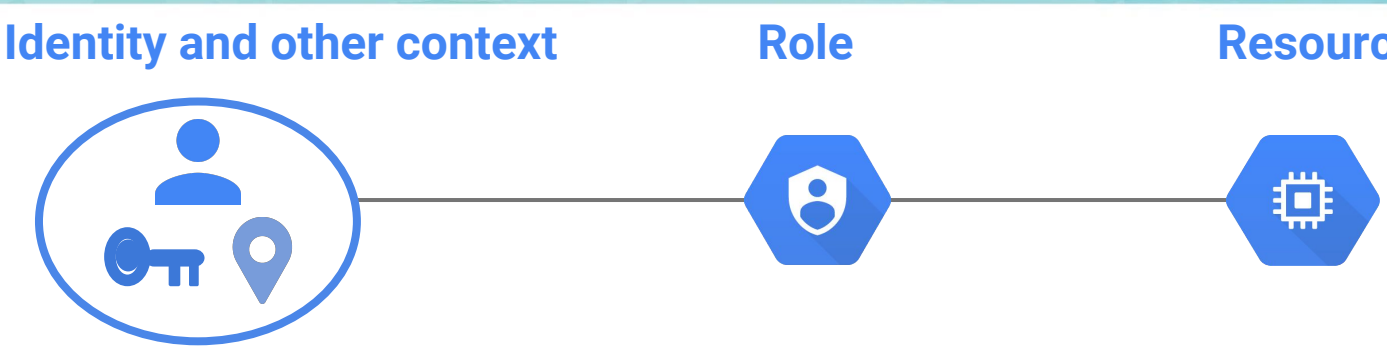


Solution: Istio security

- Zero-trust network
- Context-aware access control
- Secure by default
- Authentication
- Authorization
- Encryption



Istio context-aware access control



JWT (Json Web Token)

{ "typ": "JWT" }	**Header**
{ "iss": "issuer@example.com", "groups": [“dev”, “admin”], }	**Payload**
{RSA-SHA256(header+payload)}	**Signature**

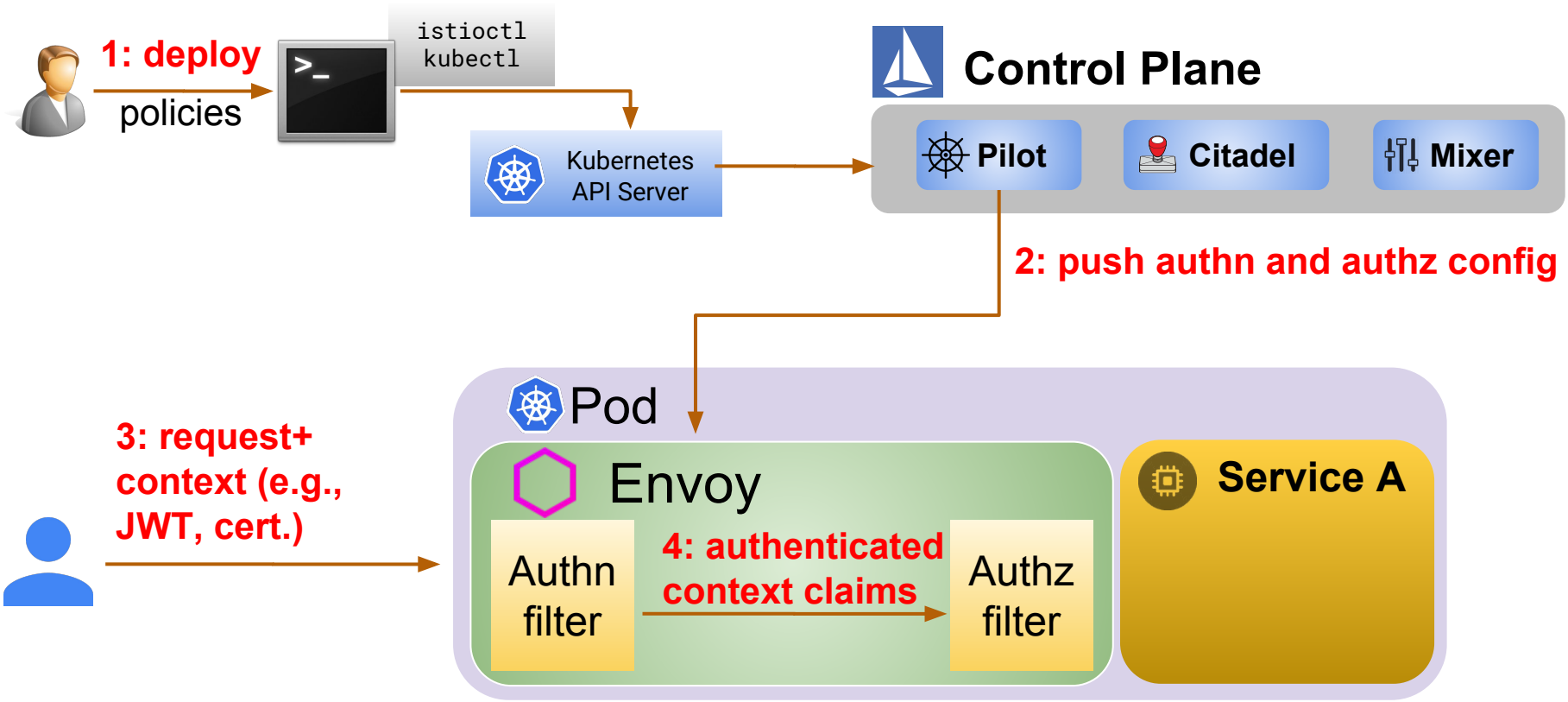
Certificate

Certificate:

Subject Alternative Name:

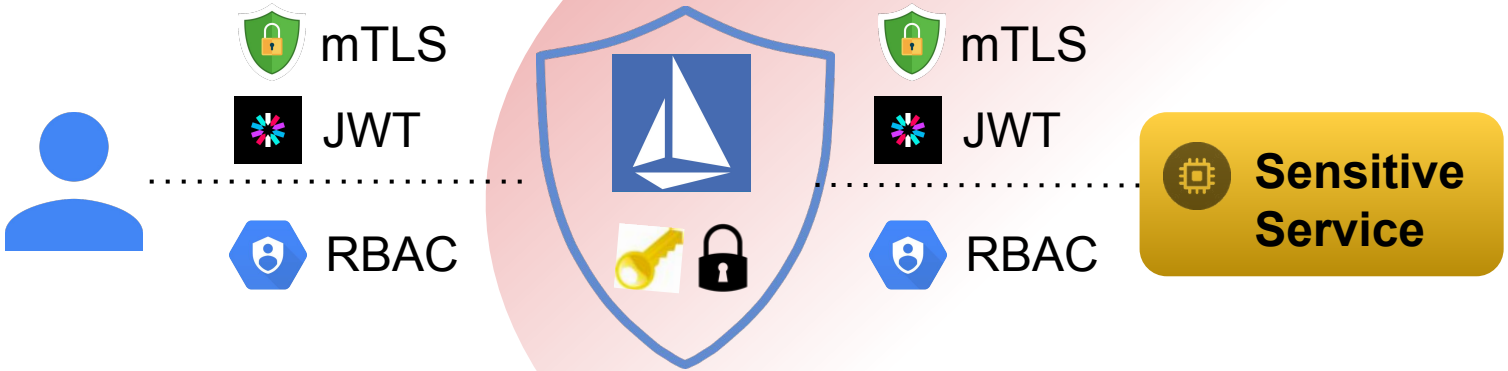
spiffe://cluster.local/ns/{name-space}/sa/{service-account-name}

Example flow of context-aware access



Demo: Istio context-aware access control

- A user must be in a specific group to access a sensitive service.
- The access must be protected by mTLS.
- May also control the calling path.



Demo: authorization policies

```
apiVersion: "rbac.istio.io/v1alpha1"
kind: ServiceRole
metadata:
  name: httpbin-viewer
spec:
  rules:
  - services:
    ["httpbin.rbac-groups-test-ns.svc.cluster.local"]
   methods: ["GET"]
  …
```

```
apiVersion: "rbac.istio.io/v1alpha1"
kind: ServiceRoleBinding
metadata:
  name: bind-httpbin-viewer
spec:
  subjects:
  - properties:
      request.auth.claims[groups]: "group1"
  roleRef:
    kind: ServiceRole
    name: "httpbin-viewer"
  ...
```

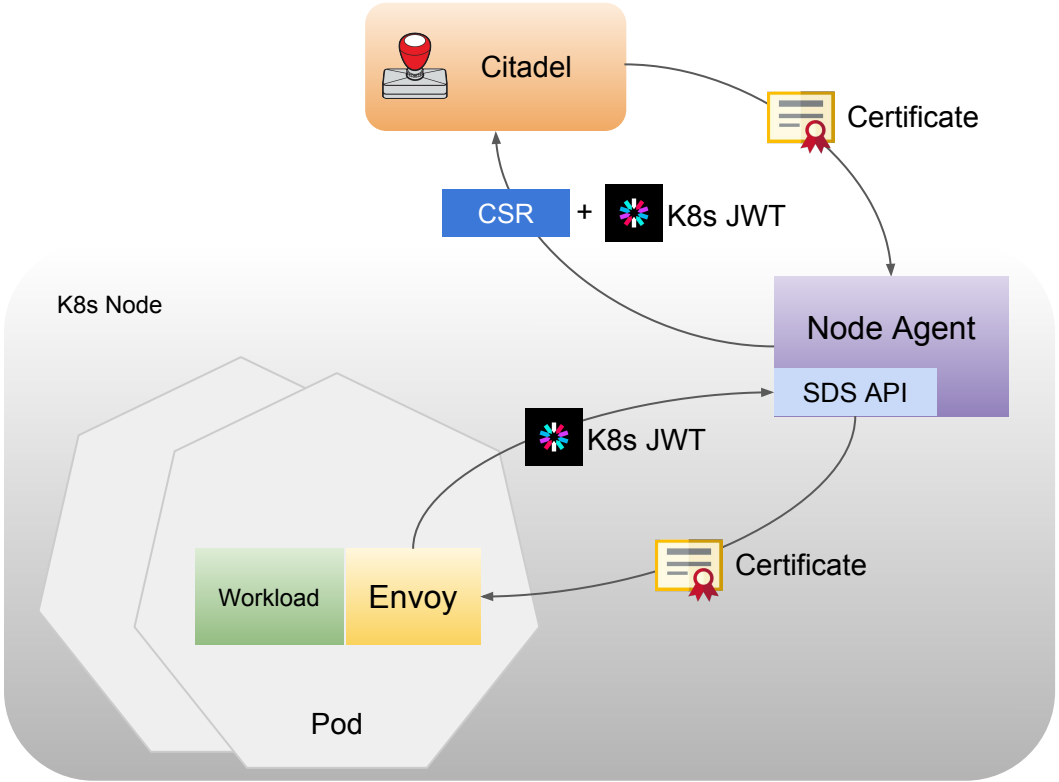
Demo: authentication policy

```
apiVersion: "authentication.istio.io/v1alpha1"
kind: "Policy"
metadata:
  name: "require-mtls-jwt"
spec:
  targets:
  - name: httpbin
  peers:
  - mtls: {}
  origins:
  - jwt:
      issuer: "testing@secure.istio.io"
```

Demo

Demo of Istio context-aware access control

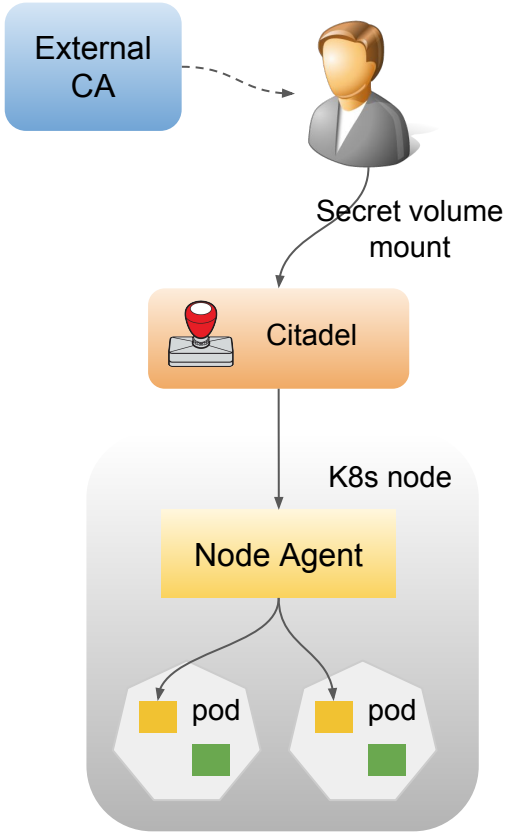
Certificate Provision Flow



Integration with external CAs

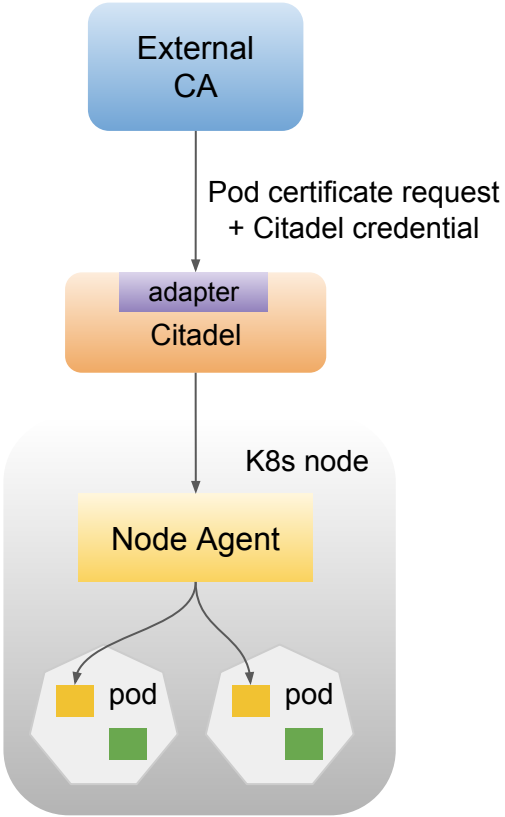
	Signing-key -injection	Citadel -integration	Nodeagent -integration
Automatic key and cert provision	No	Yes	Yes
Citadel involvement	Yes	Yes	No

Approach 1: Signing-key-injection



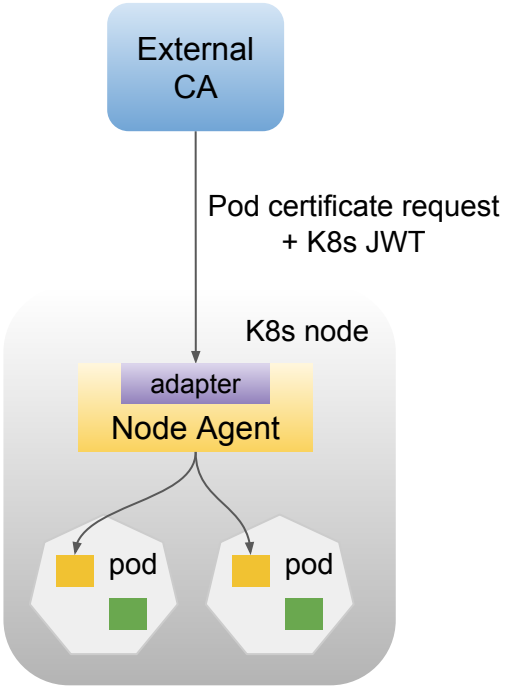
- Operator involved for signing key and cert rotation

Approach 2: Citadel-integration



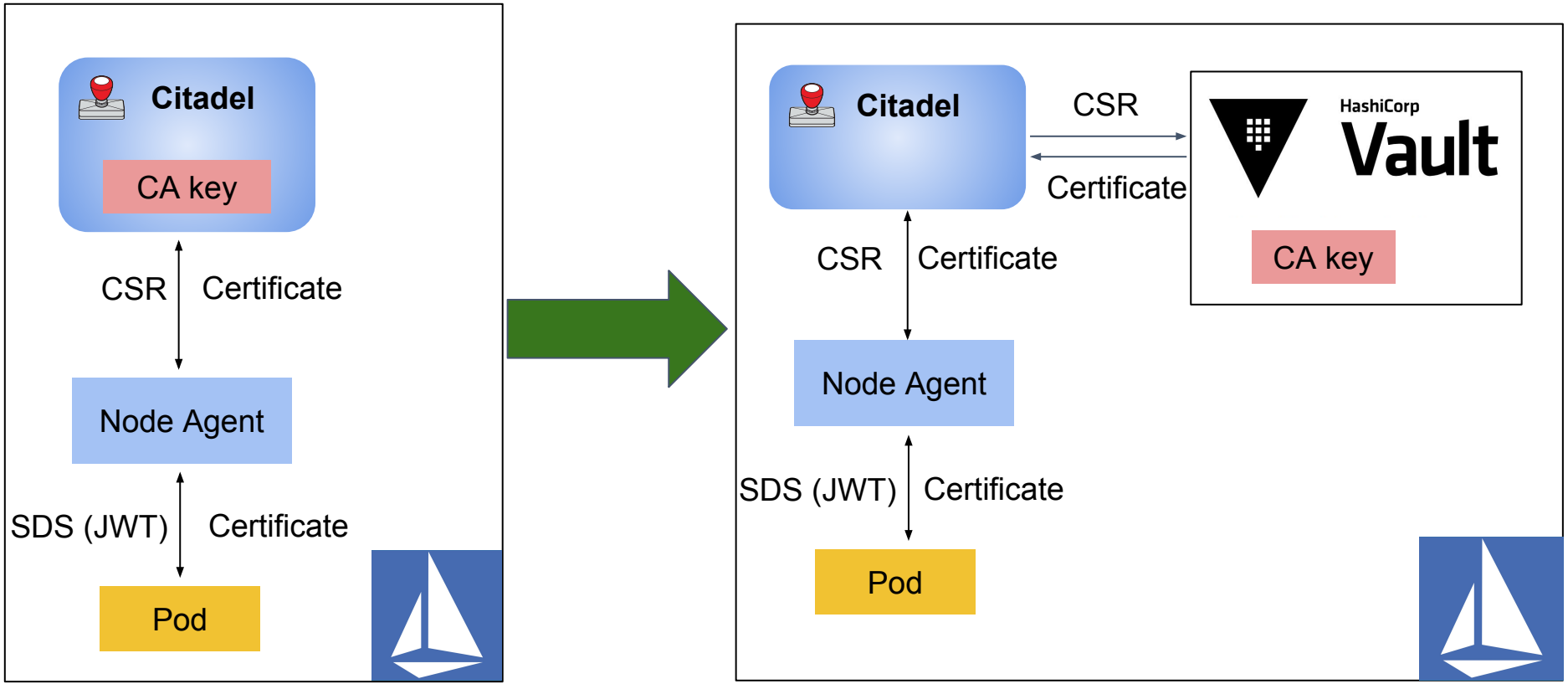
- Citadel authenticates and authorizes the CSRs
- Citadel is delegated to request certificates for workloads

Approach 3: Nodeagent-integration

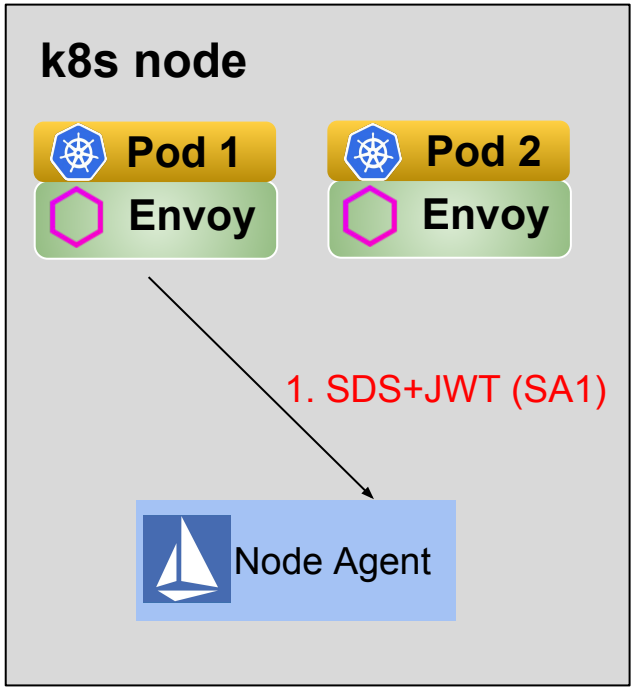


- The external CA handles the authentication and authorization of the workload CSRs
- The node agent forwards workload K8s JWT

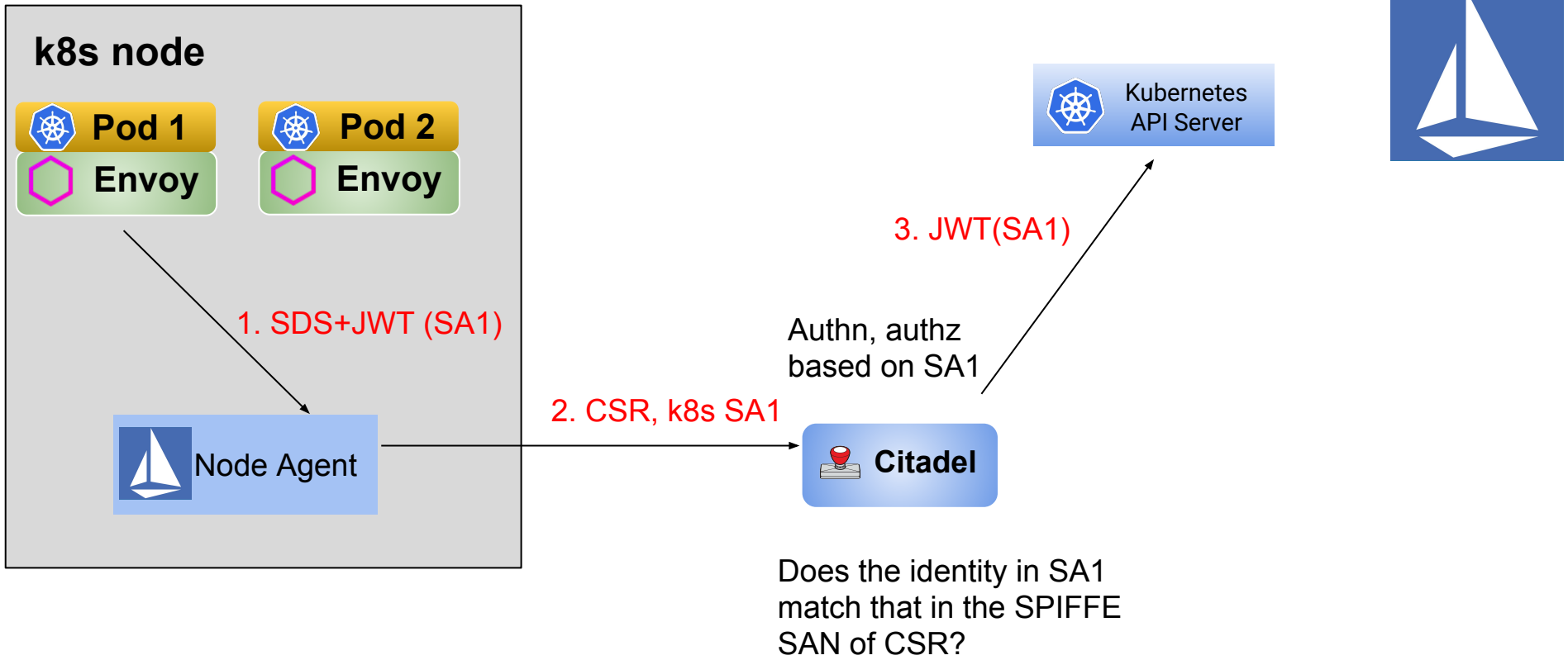
Prototype: Istio CA Vault integration



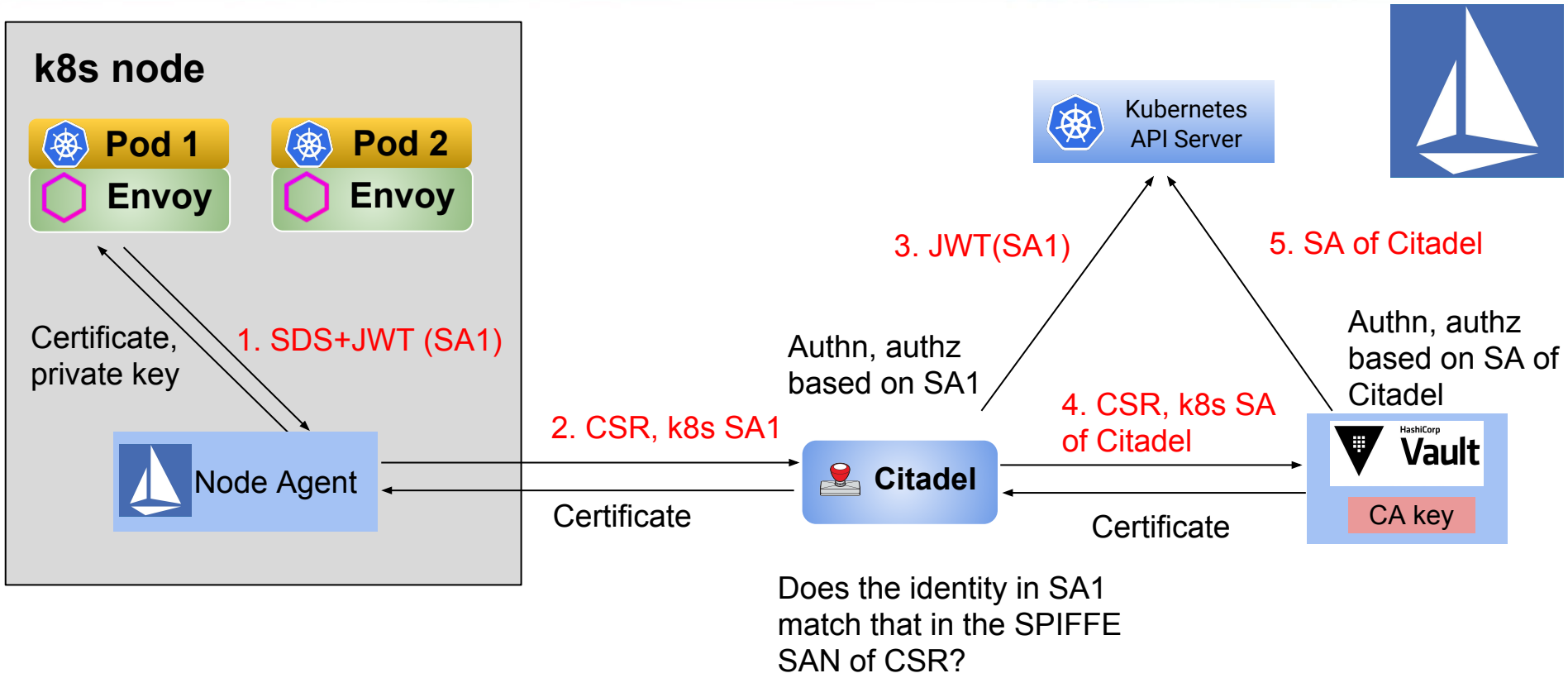
Istio CA Vault integration



Istio CA Vault integration



Istio CA Vault integration



Demo

Demo of Istio CA Vault integration

Istio survey

We would love to hear your feedbacks on Istio. Please fill the survey on the survey website; we have rewards waiting for you :)

KubeCon

CloudNativeCon

China 2018