



KubeCon



CloudNativeCon

China 2018

# Istio Certificate Management Through Vault

Lei Tang, Yonggang Liu, *Google LLC.*





**Lei Tang**

Software Engineer  
Istio



[leitang@google.com](mailto:leitang@google.com)

wechat: LTANG2015



**Oliver (Yonggang) Liu**

Software Engineer  
Istio



[yonggangl@google.com](mailto:yonggangl@google.com)

<http://oliverliu.org>

# Istio manages your microservices



KubeCon



CloudNativeCon

China 2018



**Relieve burden of service owners.  
Bring order to chaos.**



# Istio 30,000-foot view

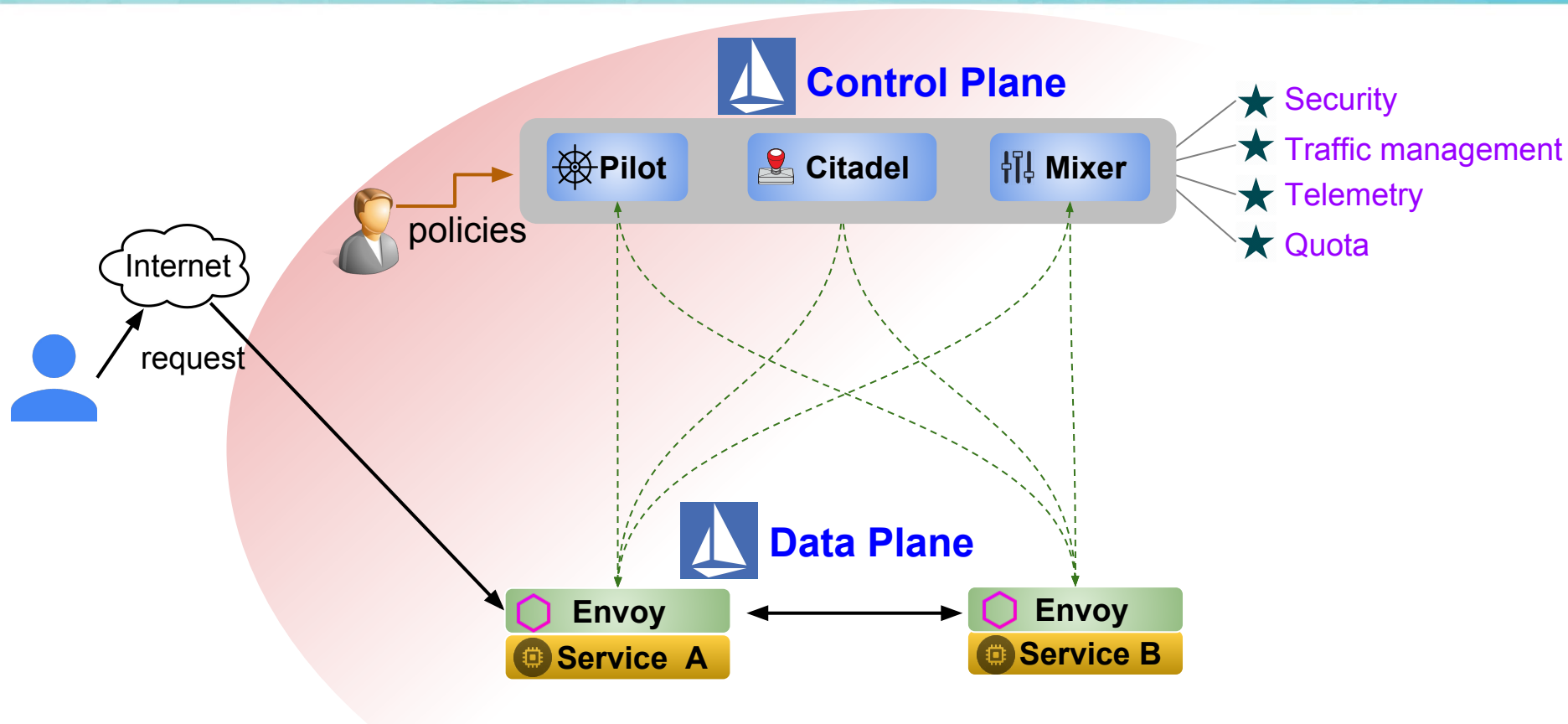


KubeCon



CloudNativeCon

China 2018



# Security risks for service meshes

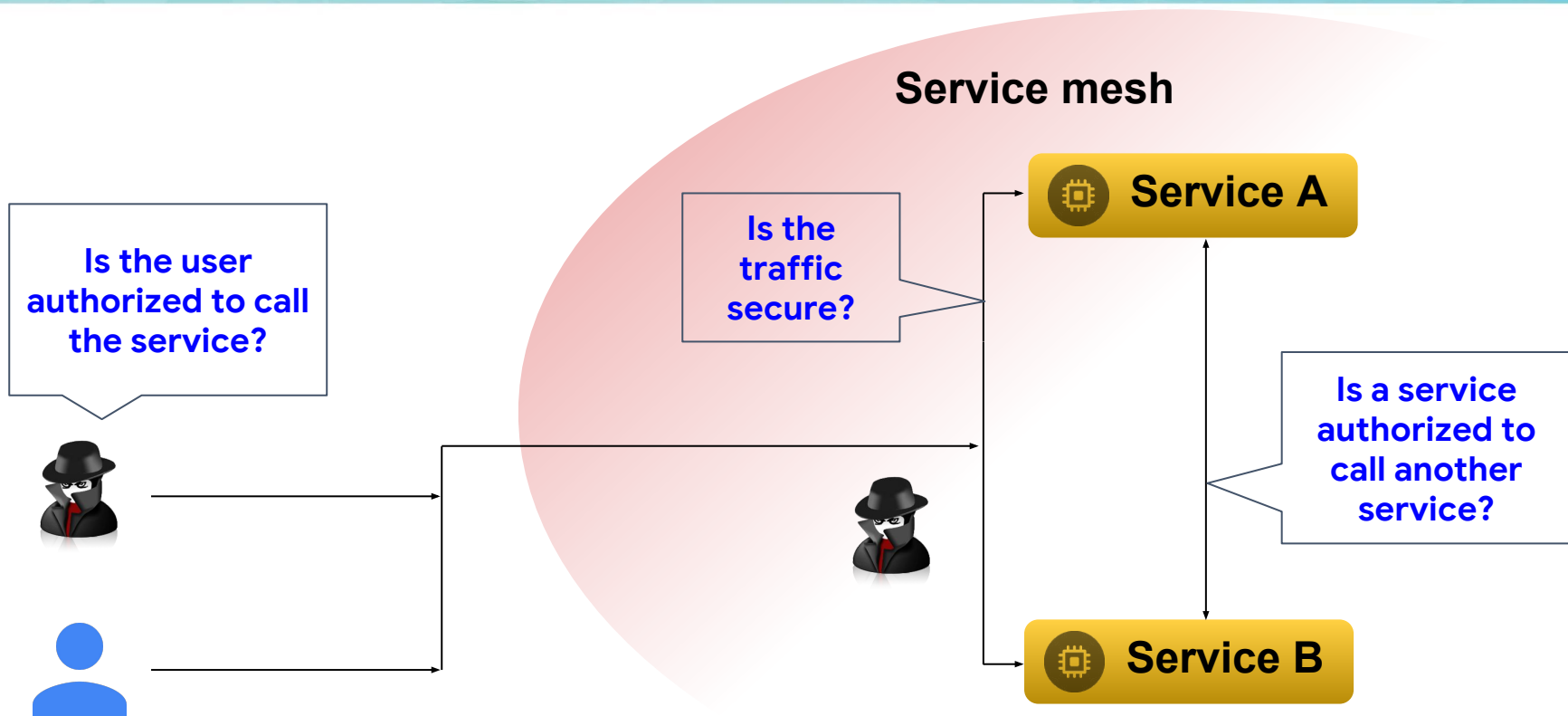


KubeCon



CloudNativeCon

China 2018



# Solution: Istio security



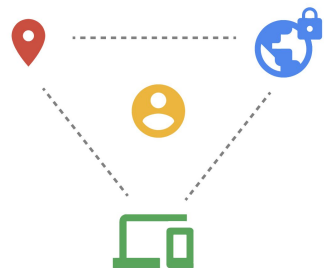
KubeCon



CloudNativeCon

China 2018

BeyondCorp



ALTS



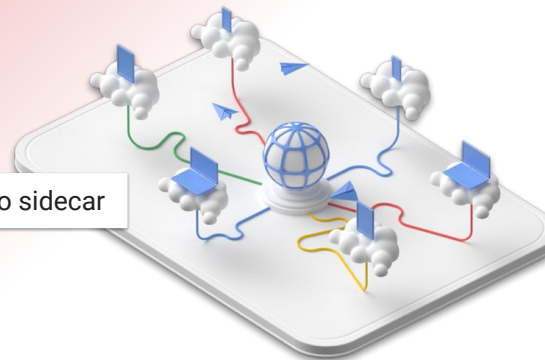
Mesh

Perimeter



Istio Ingress/Egress

Istio sidecar



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

# Istio context-aware access control



KubeCon



CloudNativeCon

China 2018

Identity and other context



Role



Resource



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

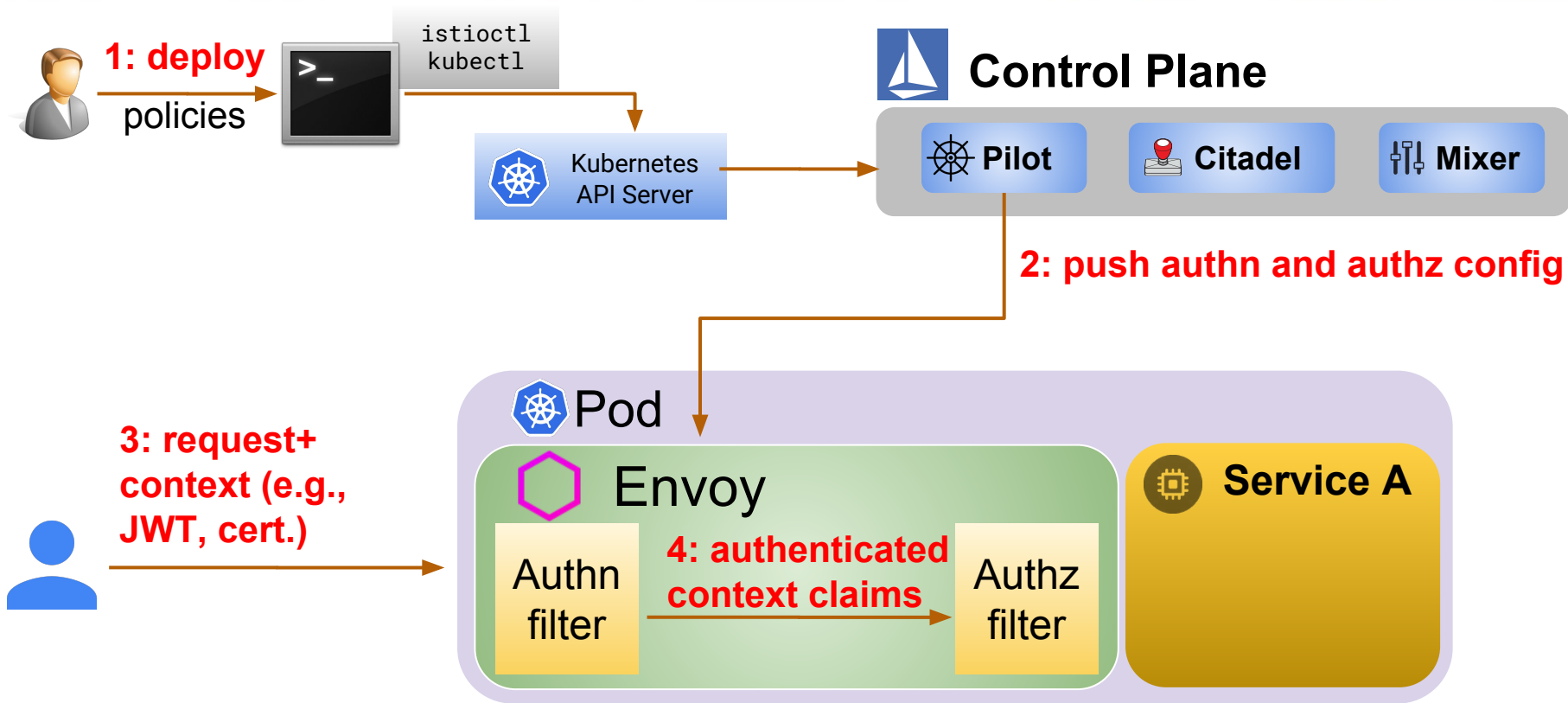


KubeCon



CloudNativeCon

China 2018





# Demo: Istio context-aware access control



KubeCon



CloudNativeCon

China 2018

- 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



KubeCon



CloudNativeCon

China 2018



```
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



KubeCon



CloudNativeCon

China 2018

```
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



KubeCon



CloudNativeCon

China 2018

## Demo of Istio context-aware access control

# Certificate Provision Flow

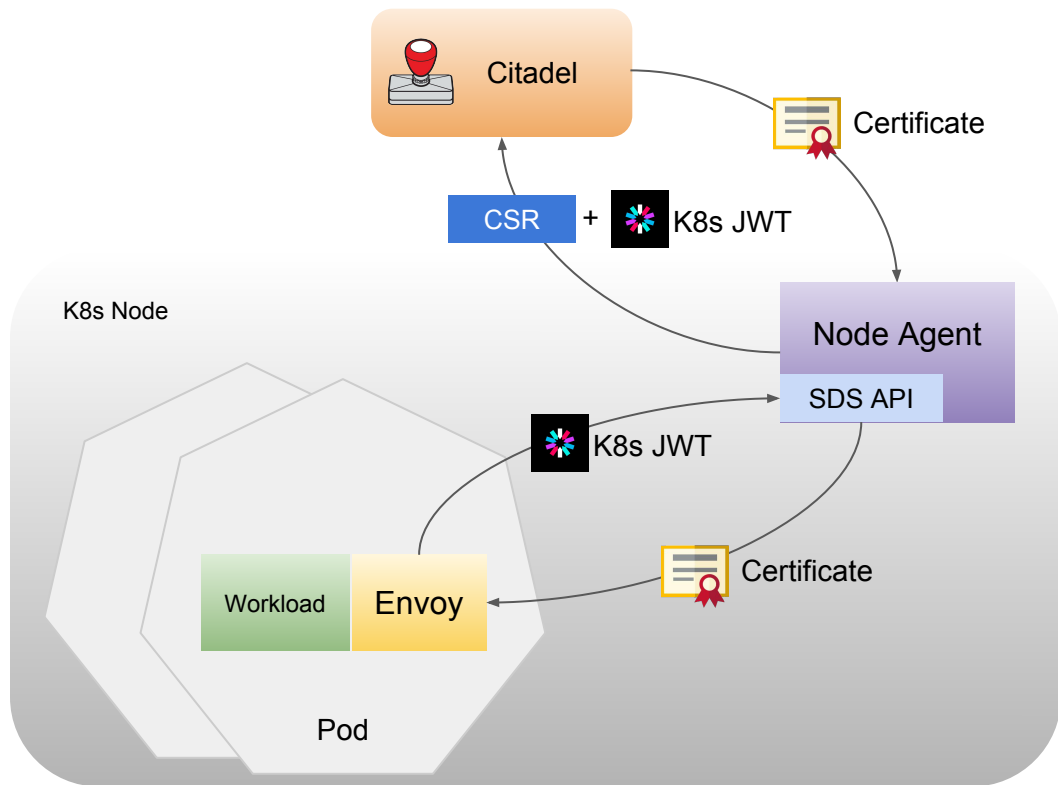


KubeCon



CloudNativeCon

China 2018





# Integration with external CAs



KubeCon



CloudNativeCon

China 2018

	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

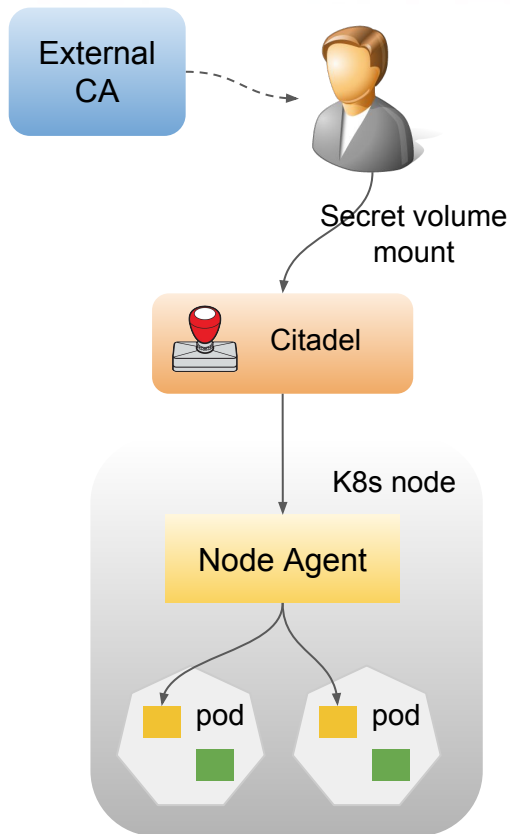


KubeCon



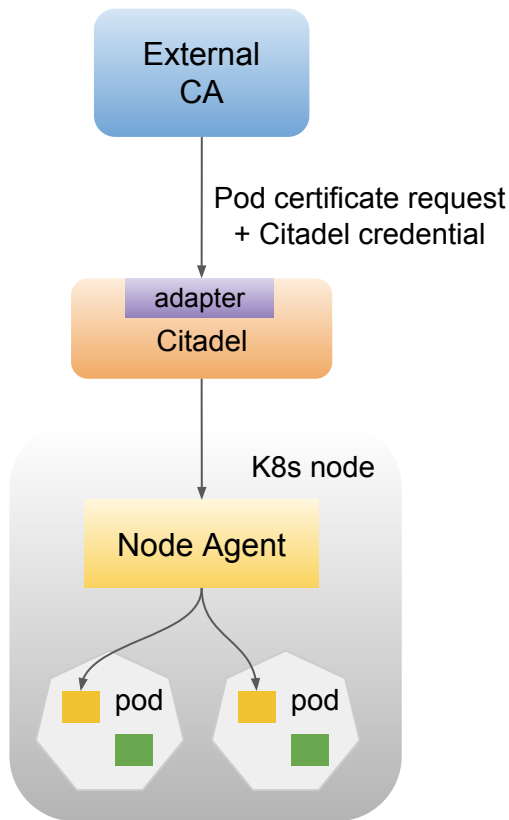
CloudNativeCon

China 2018



- 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

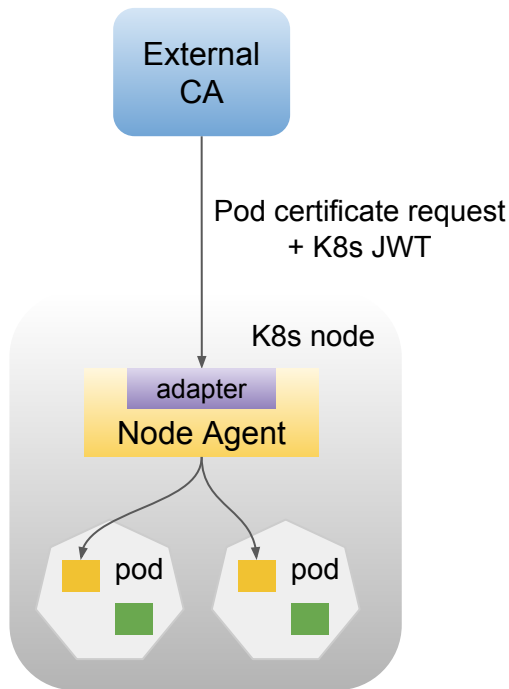


KubeCon



CloudNativeCon

China 2018



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

# Prototype: Istio CA Vault integration

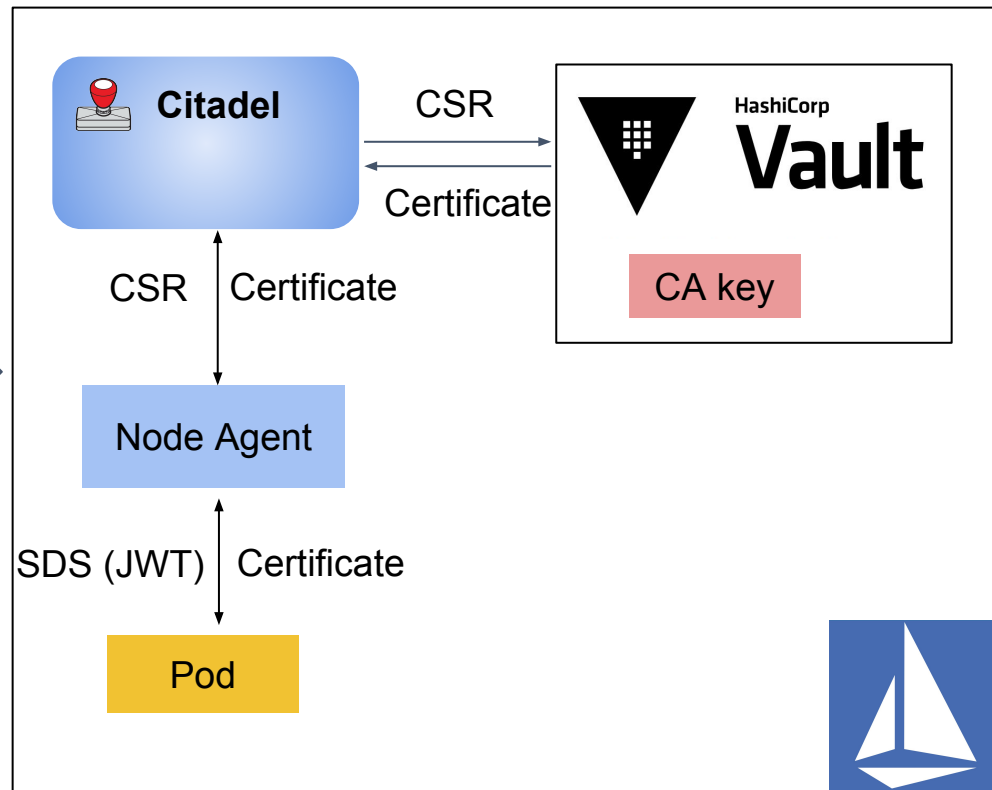
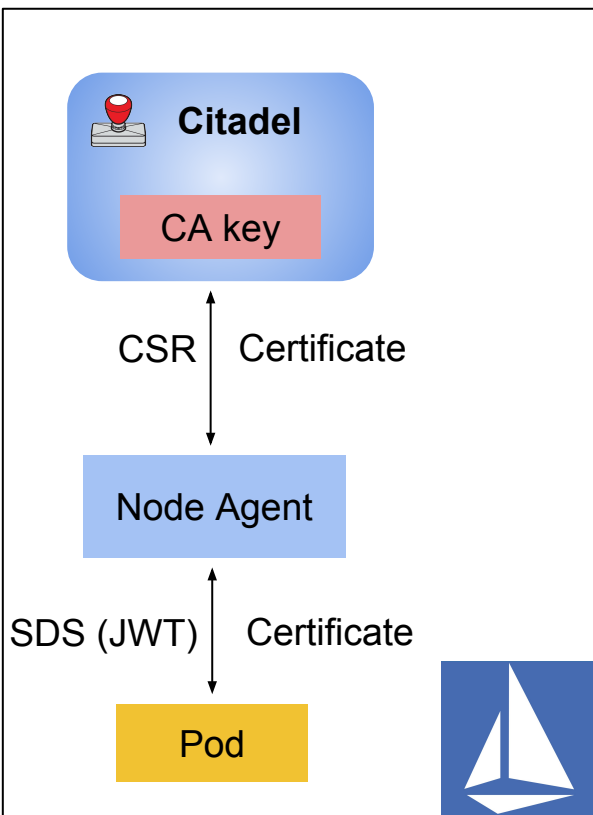


KubeCon



CloudNativeCon

China 2018





# Istio CA Vault integration



KubeCon



CloudNativeCon

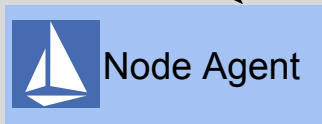
China 2018



**k8s node**



1. SDS+JWT (SA1)



# Istio CA Vault integration



KubeCon



CloudNativeCon

China 2018



## k8s node



Pod 1



Envoy



Pod 2



Envoy

1. SDS+JWT (SA1)



Node Agent

2. CSR, k8s SA1



Citadel

3. JWT(SA1)

Authn, authz  
based on SA1



Kubernetes  
API Server

Does the identity in SA1  
match that in the SPIFFE  
SAN of CSR?

# Istio CA Vault integration



KubeCon



CloudNativeCon

China 2018

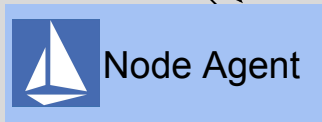


## k8s node



Certificate,  
private key

1. SDS+JWT (SA1)



2. CSR, k8s SA1

Certificate

Authn, authz  
based on SA1

3. JWT(SA1)

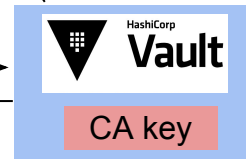


4. CSR, k8s SA  
of Citadel

Certificate

5. SA of Citadel

Authn, authz  
based on SA of  
Citadel



Does the identity in SA1  
match that in the SPIFFE  
SAN of CSR?

# Demo



KubeCon



CloudNativeCon

China 2018

## Demo of Istio CA Vault integration

# Istio survey



KubeCon



CloudNativeCon

China 2018



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

