Envoy SDS: Fortifying Istio Security

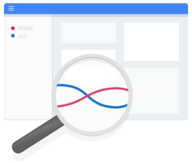
Quanjie Lin (Google) *quanlin@google.com*
Oliver Liu (Google) *yonggangl@google.com*

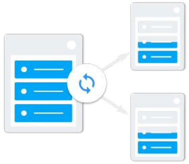
Istio Value Proposition

Securing service traffic

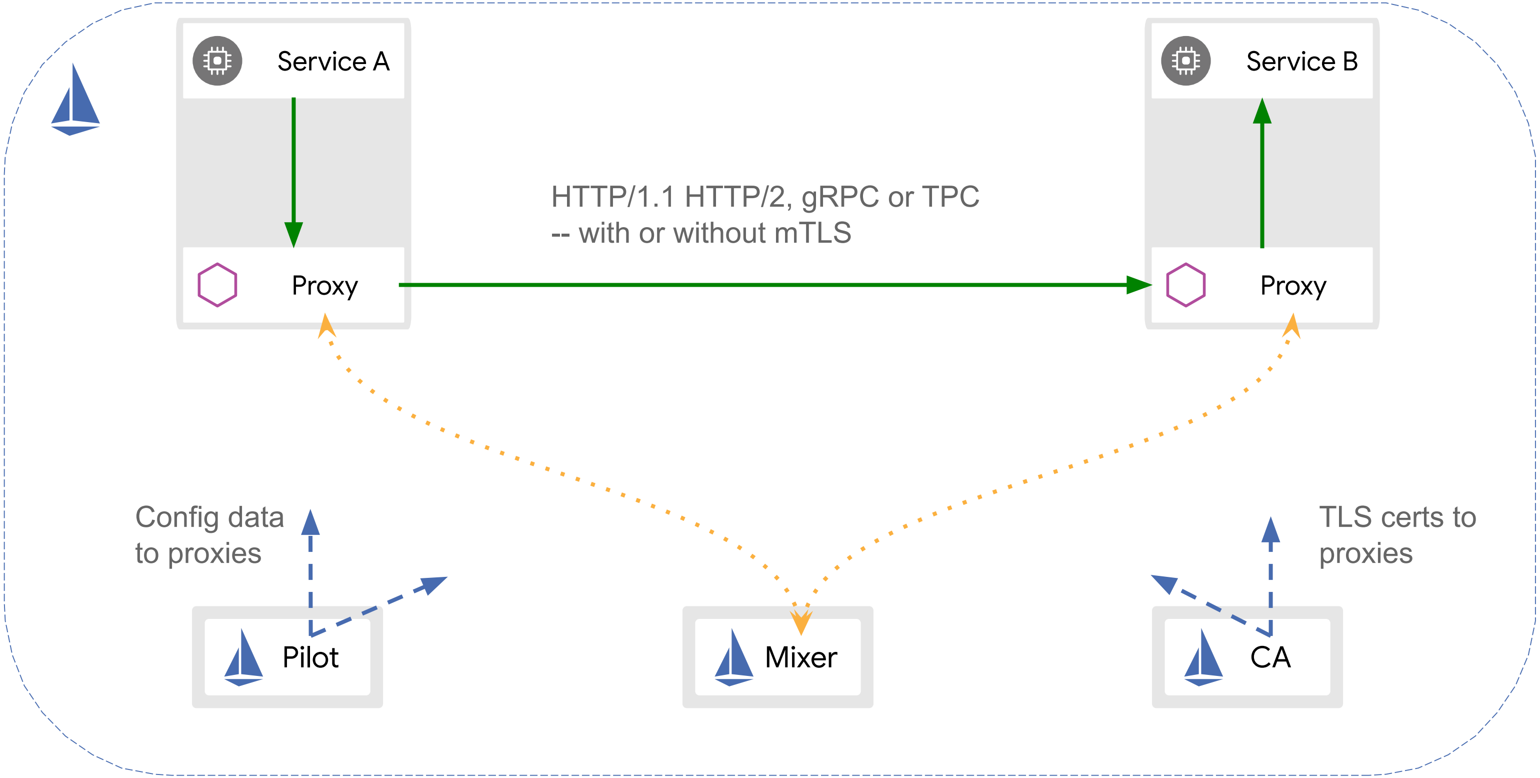
Uniform observability

Operational agility





Istio arch overview



Service A

Service B

Proxy

Proxy

HTTP/1.1 HTTP/2, gRPC or TPC
-- with or without mTLS

Config data
to proxies

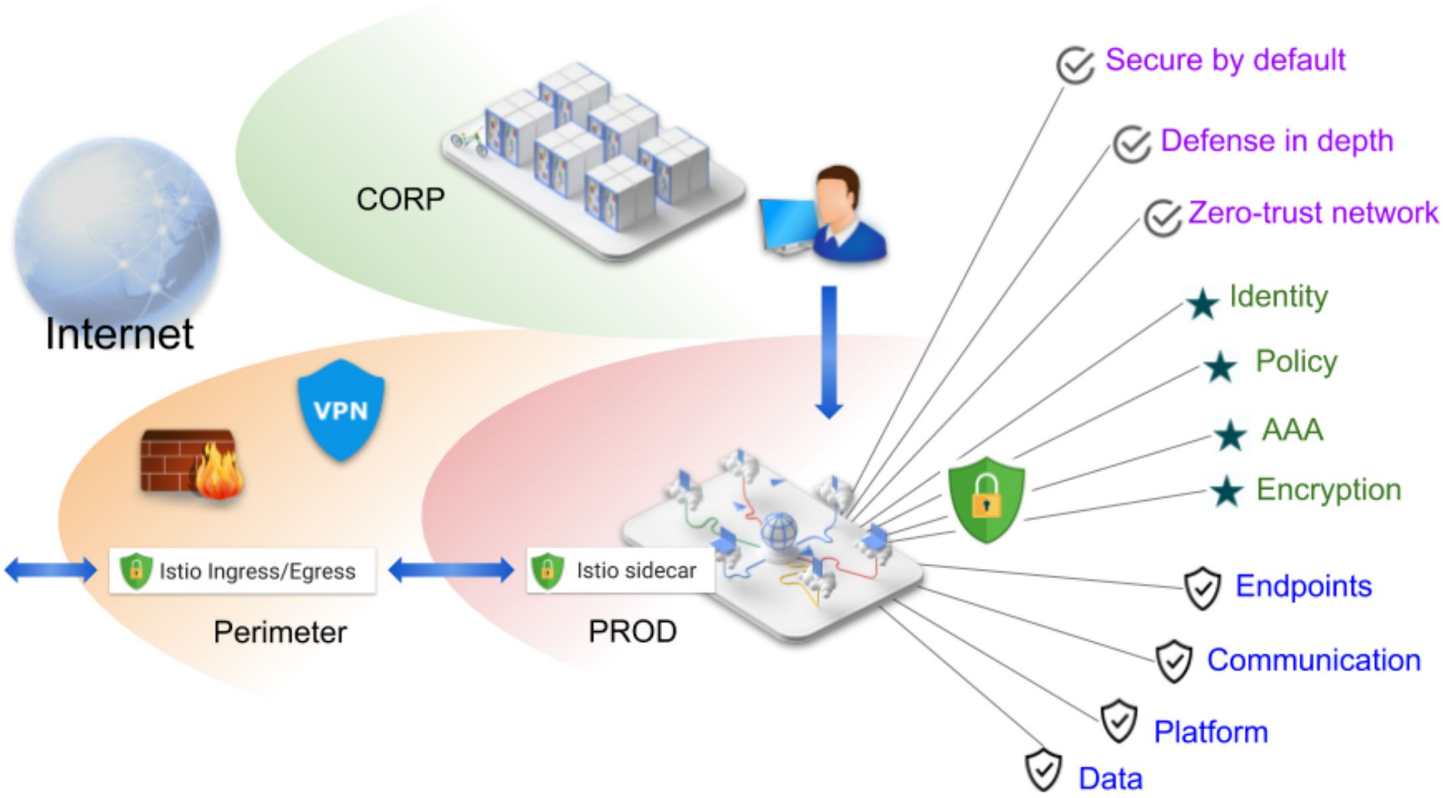
TLS certs to
proxies

Pilot

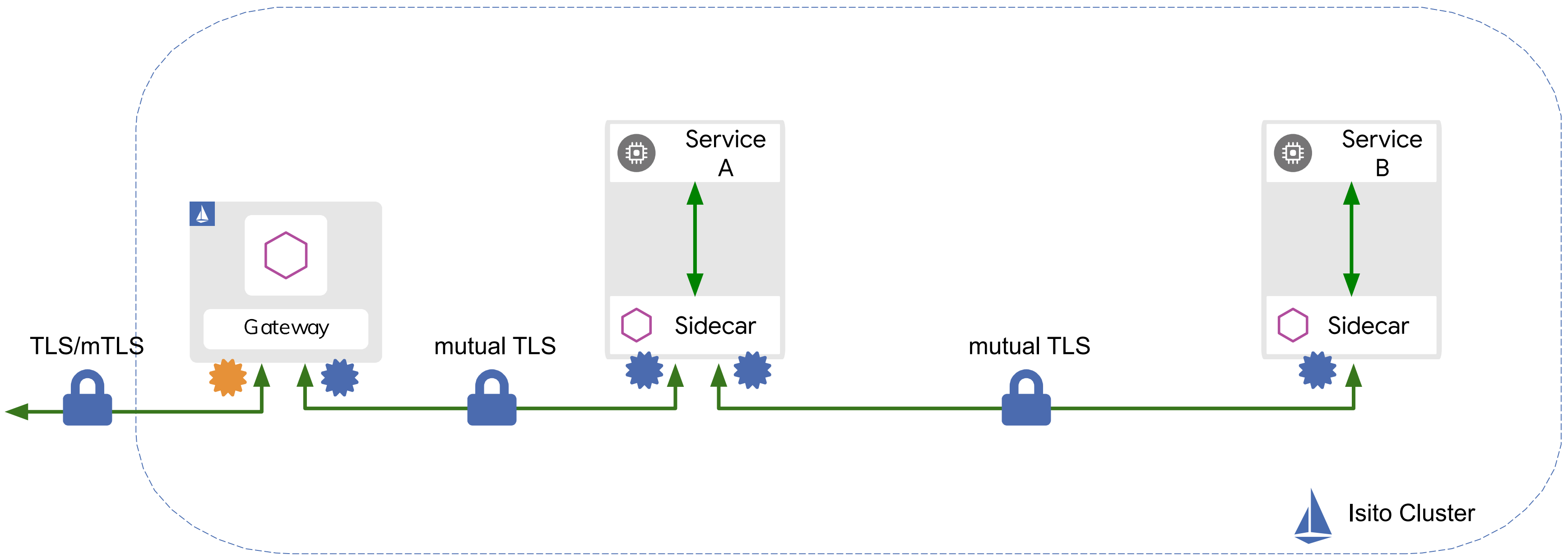
Mixer

CA

Istio security overview



Istio authentication flows



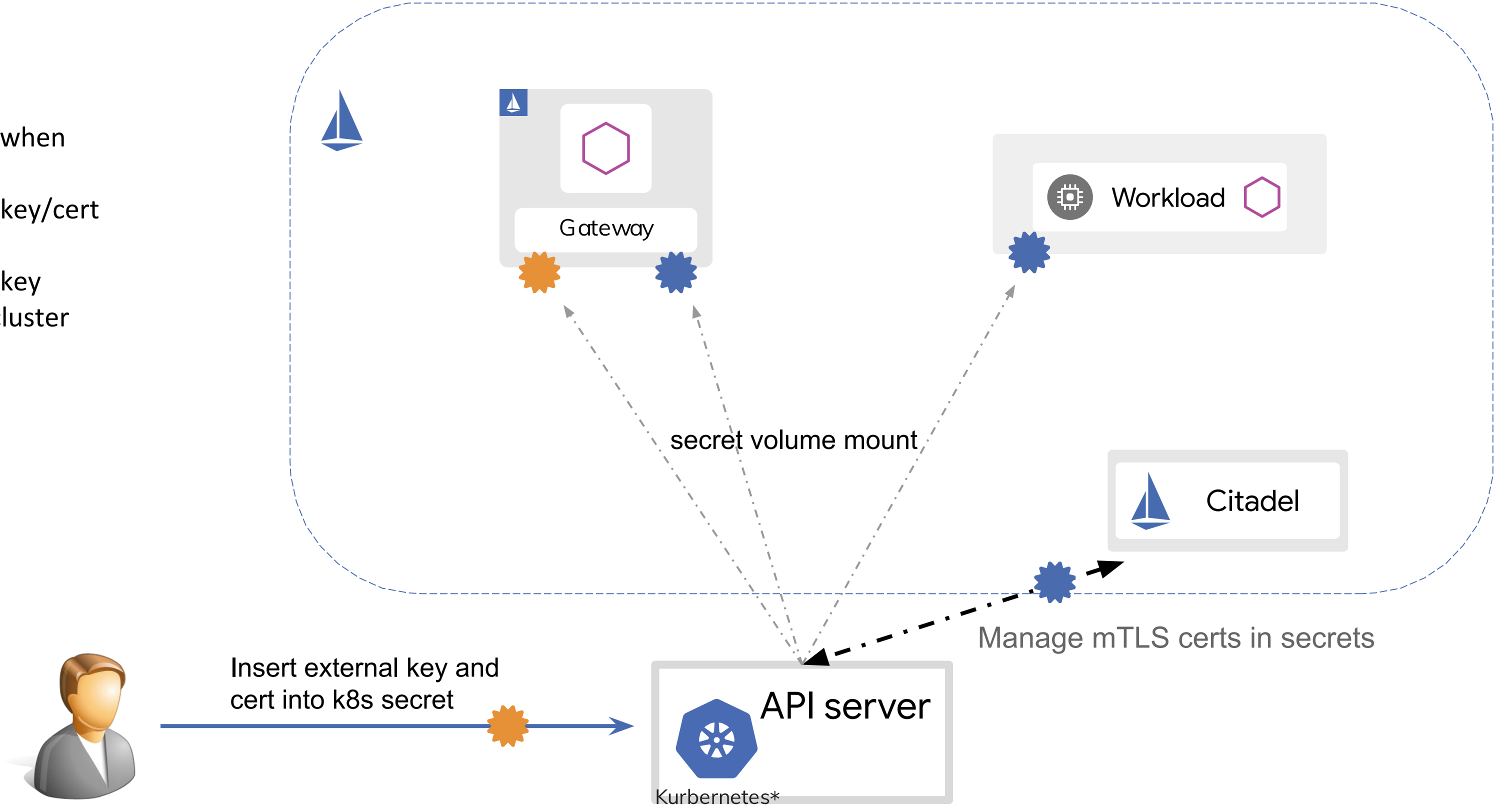
✸ Certificate for external traffic

✸ Certificate for internal traffic

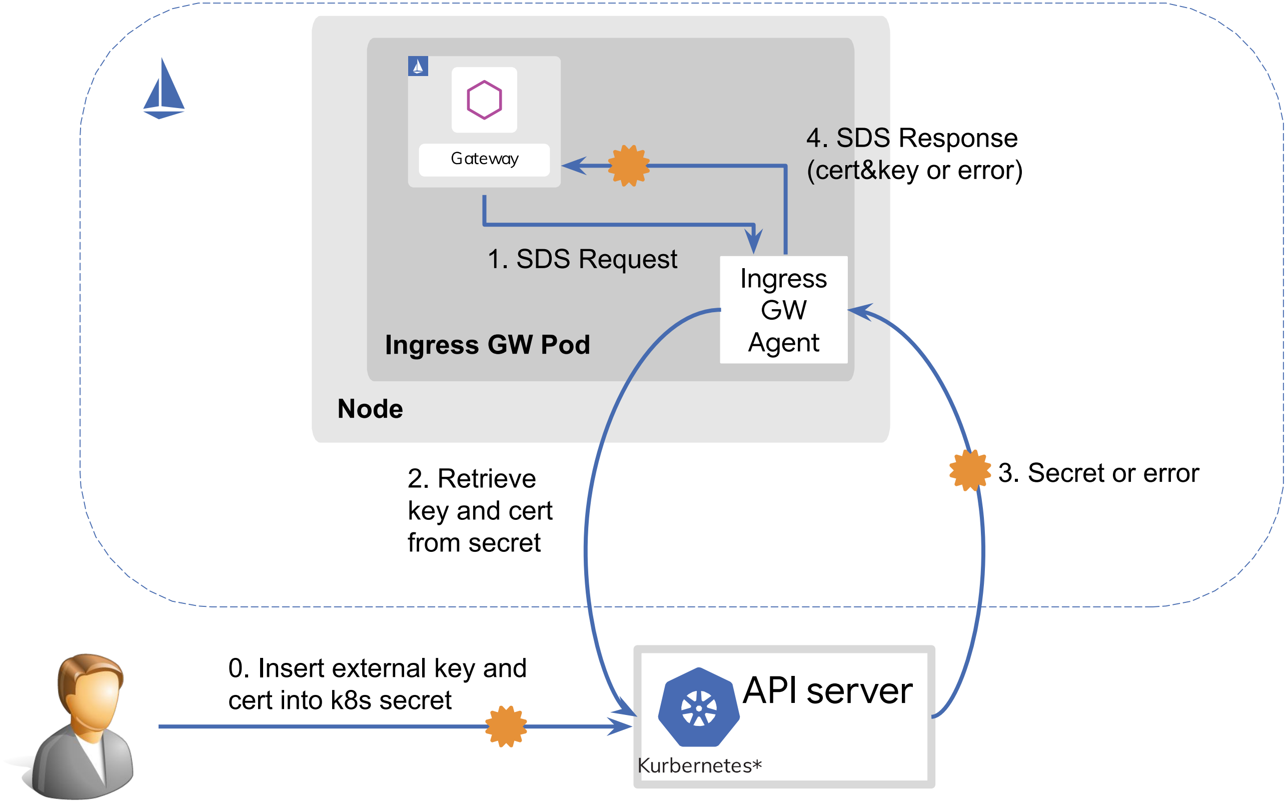
Legacy cert management with secret volume mount

Problems

- ❑ Envoy hot restart when certs are rotated
- ❑ Security concern: key/cert stored as files
- ❑ Security concern: key transferred over cluster network


Gateway
Workload
secret volume mount
Citadel
Manage mTLS certs in secrets
Insert external key and cert into k8s secret
API server
Kurbernetes*

SDS external certificate management



4. SDS Response (cert&key or error)

1. SDS Request

2. Retrieve key and cert from secret

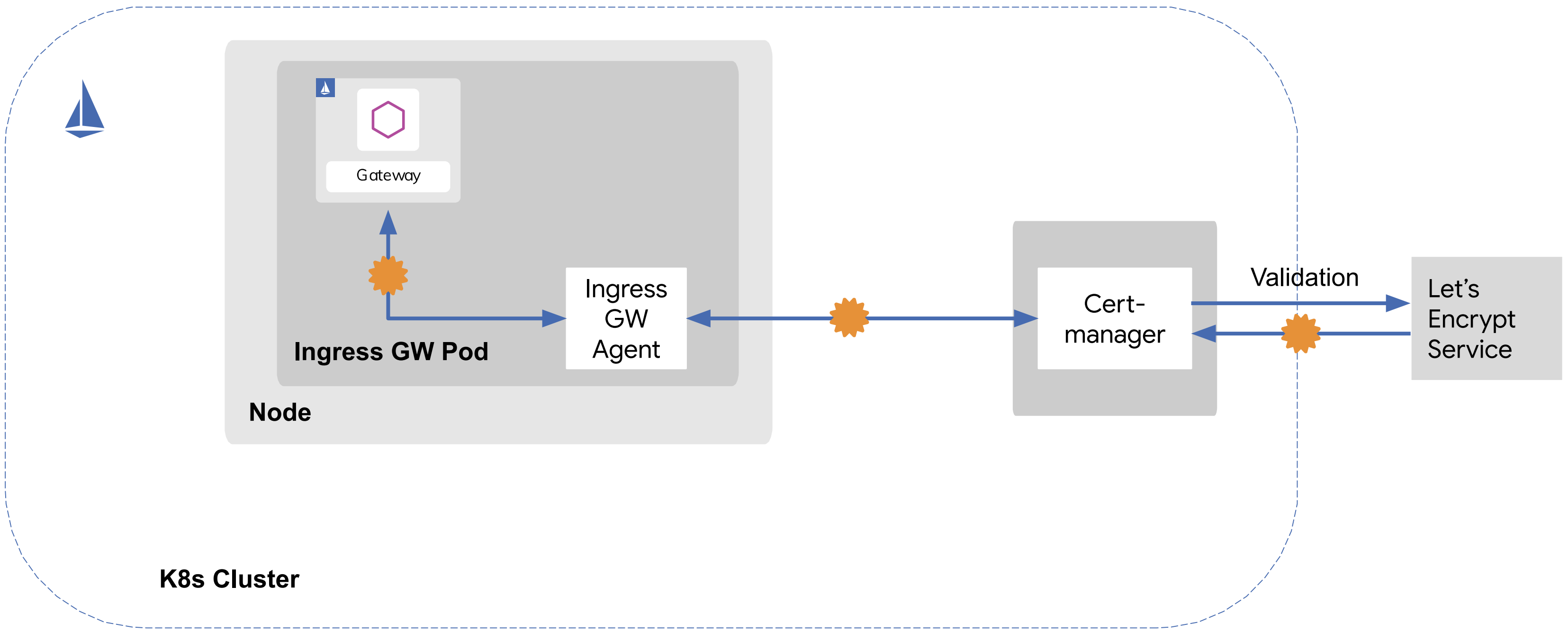
3. Secret or error

0. Insert external key and cert into k8s secret

Advantages brought by SDS

- Enhancing security
  - Private key never leaves node
  - Private key is not stored in local file system
- No interruption to traffic
  - Cert rotation will not require Envoy to restart
- Decoupling certificate management flow from underlying infra
  - Citadel can be deployed outside of cluster
  - Citadel Agent can integrate with custom CAs

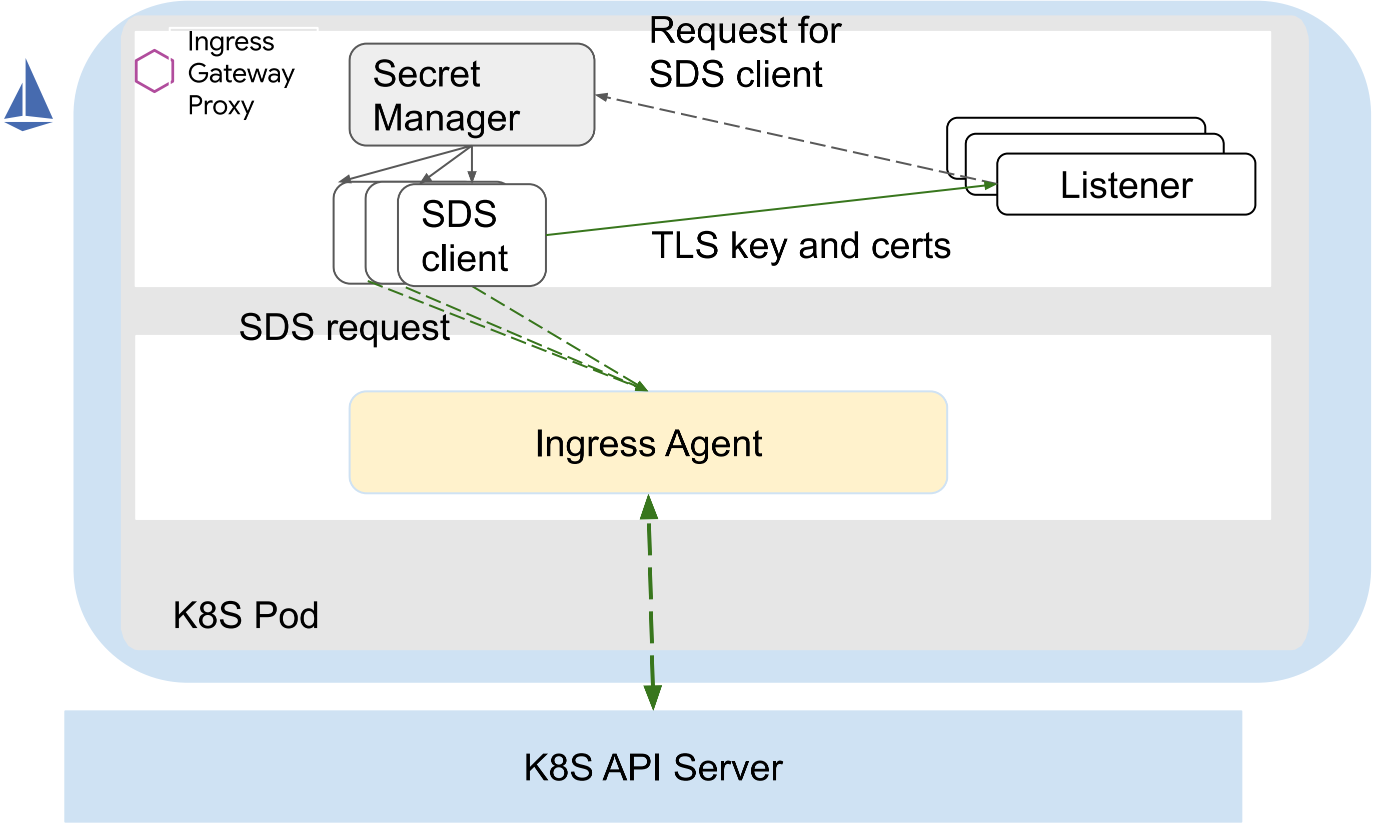
Integrate with cert-manager (Let’s Encrypt)



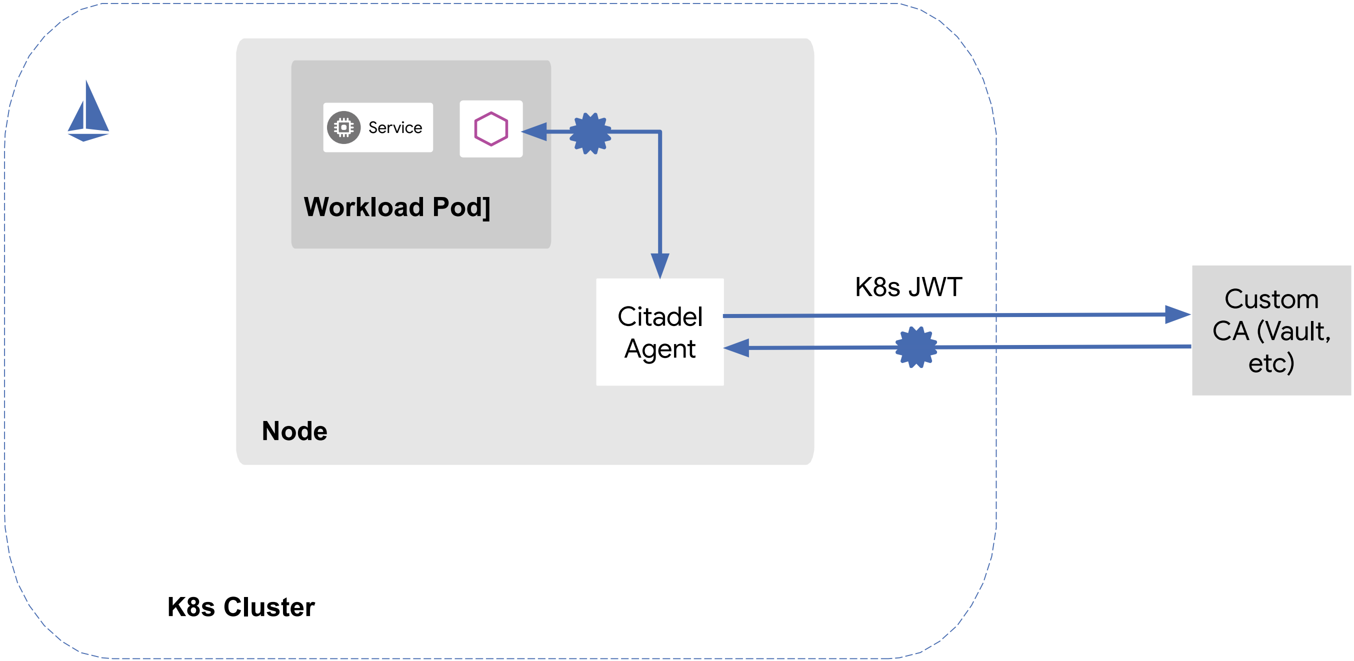
Demo

Q&A

Use case - SDS on ingress-gateway



Integrate with custom CA



Service

Workload Pod]

Citadel Agent

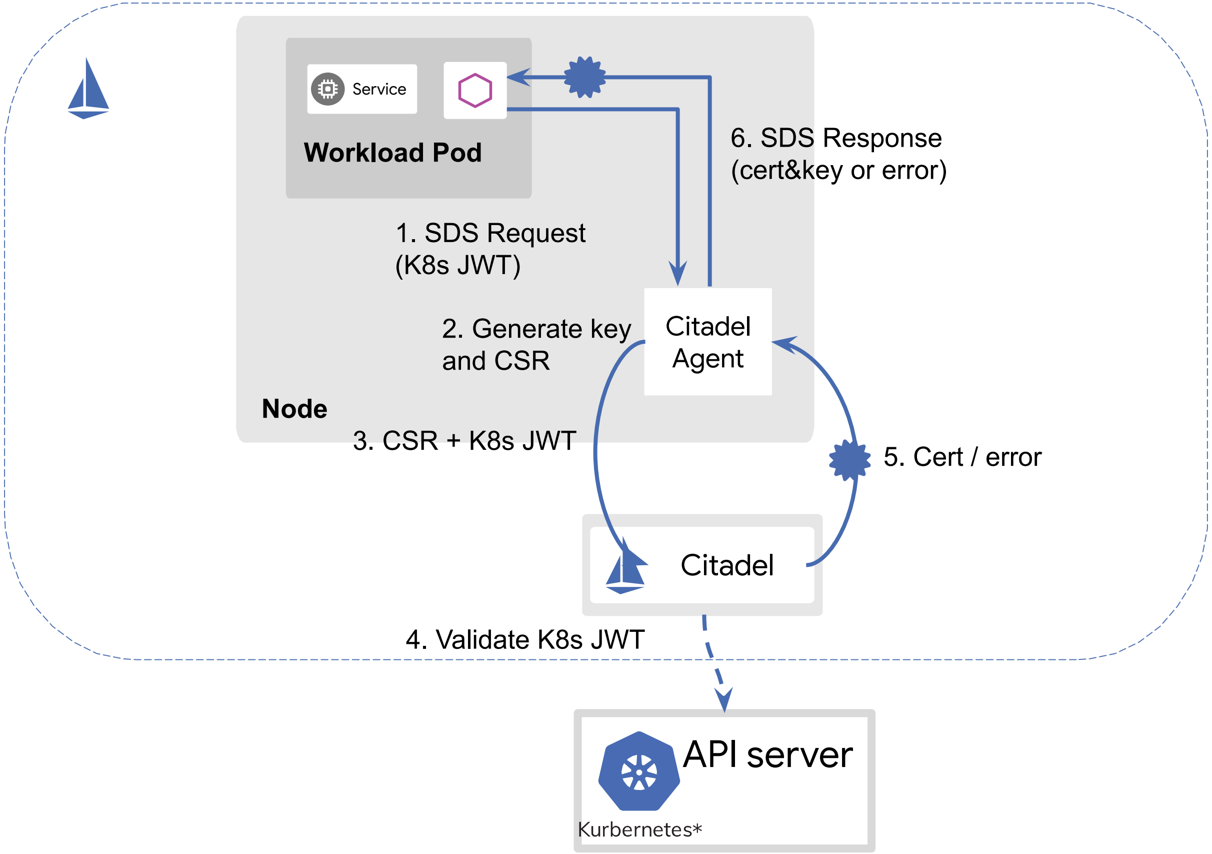
K8s JWT

Custom CA (Vault, etc)

Node

K8s Cluster

SDS workload certificate management



KubeCon | CloudNativeCon

Europe 2019

KubeCon | CloudNativeCon

Europe 2019

Istio Value Proposition