

Envoy SDS: Fortifying Istio Security

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

Istio Value Proposition

Securing service traffic



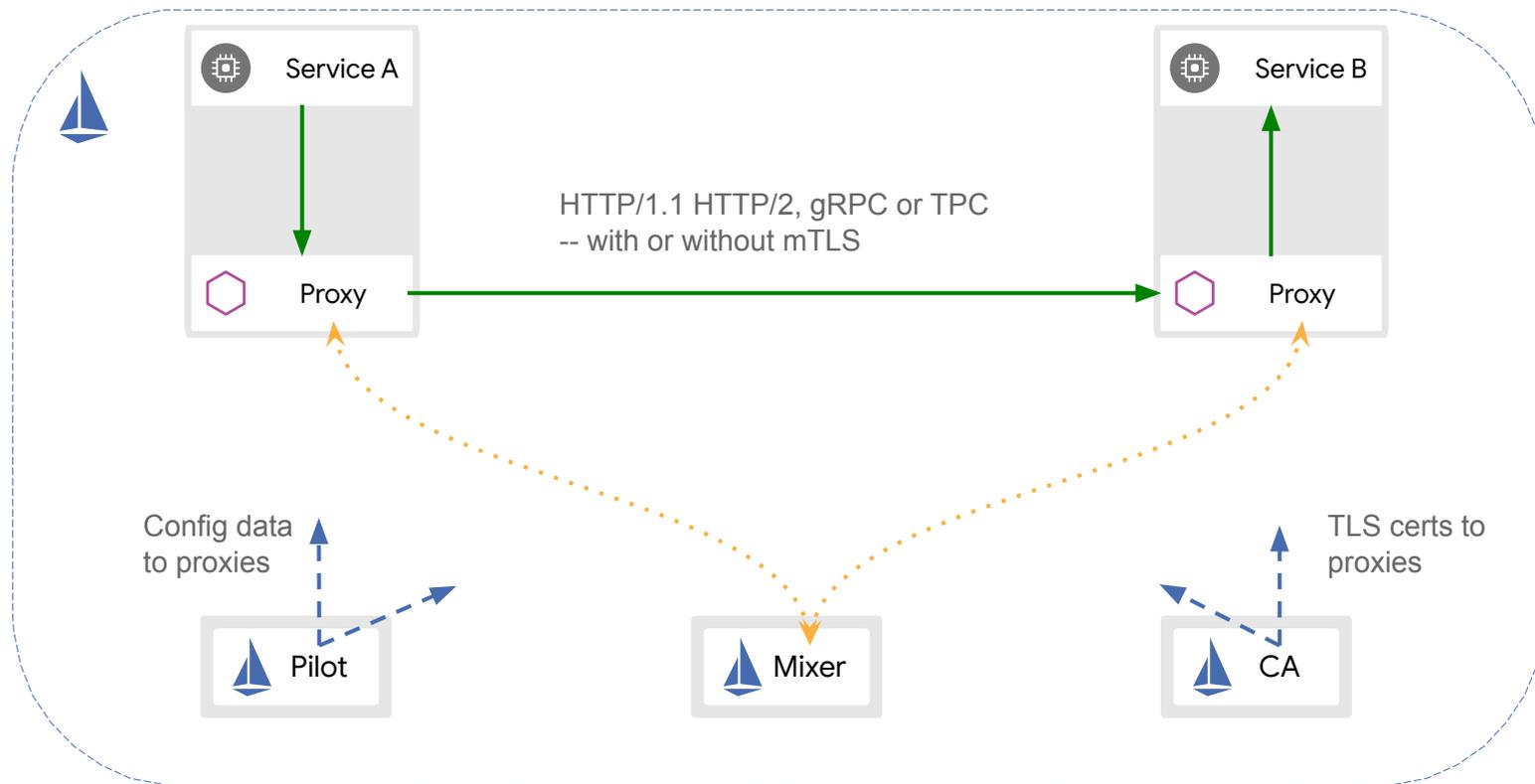
Uniform observability



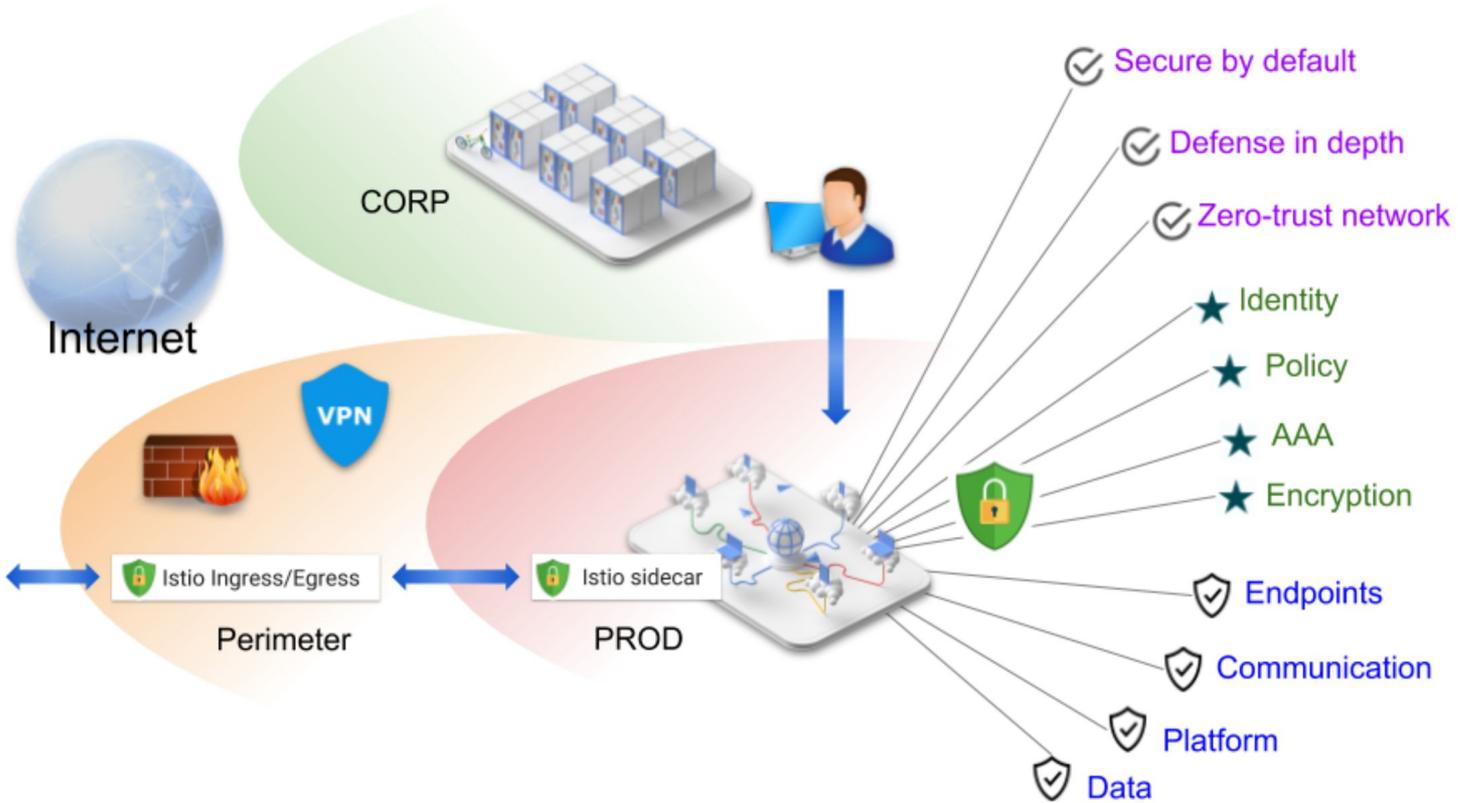
Operational agility



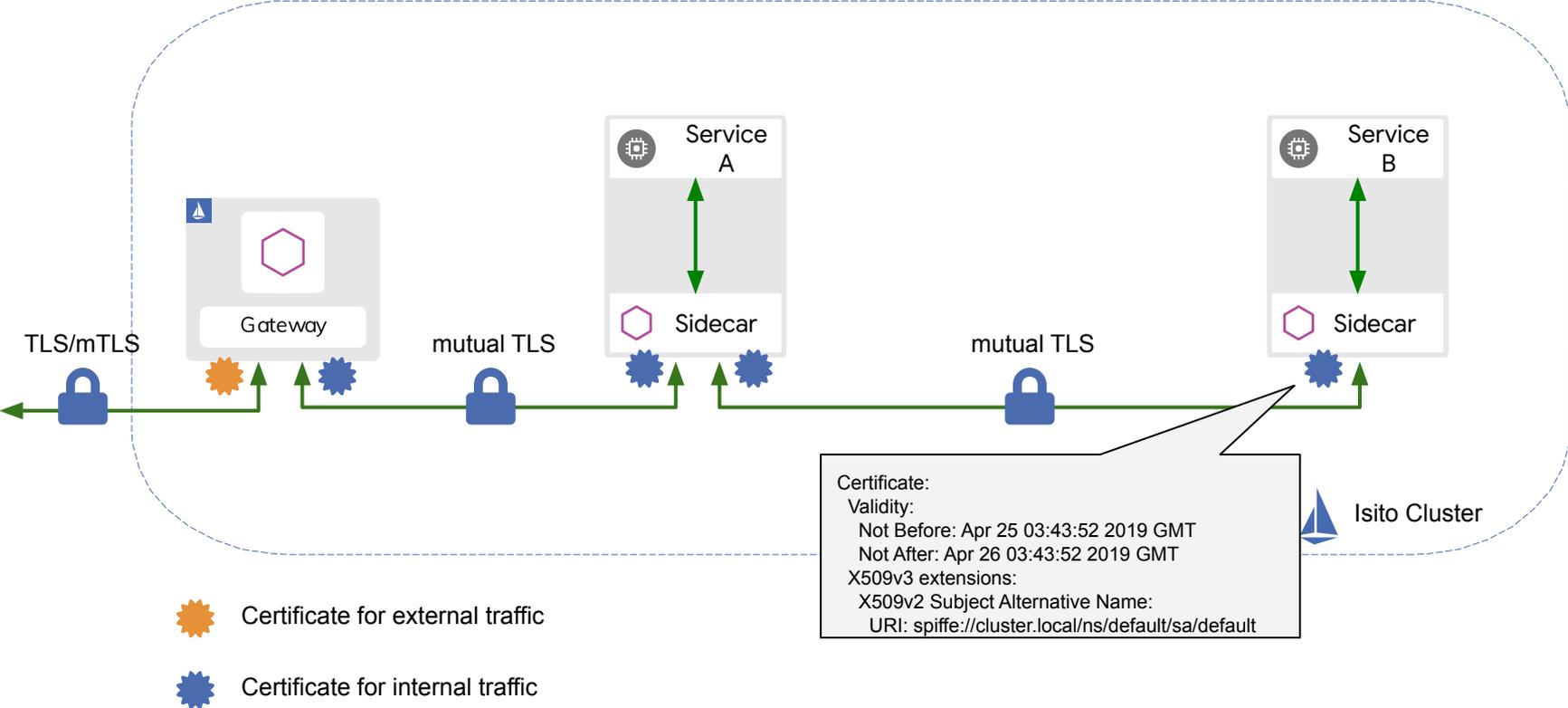
Istio arch overview



Istio security overview



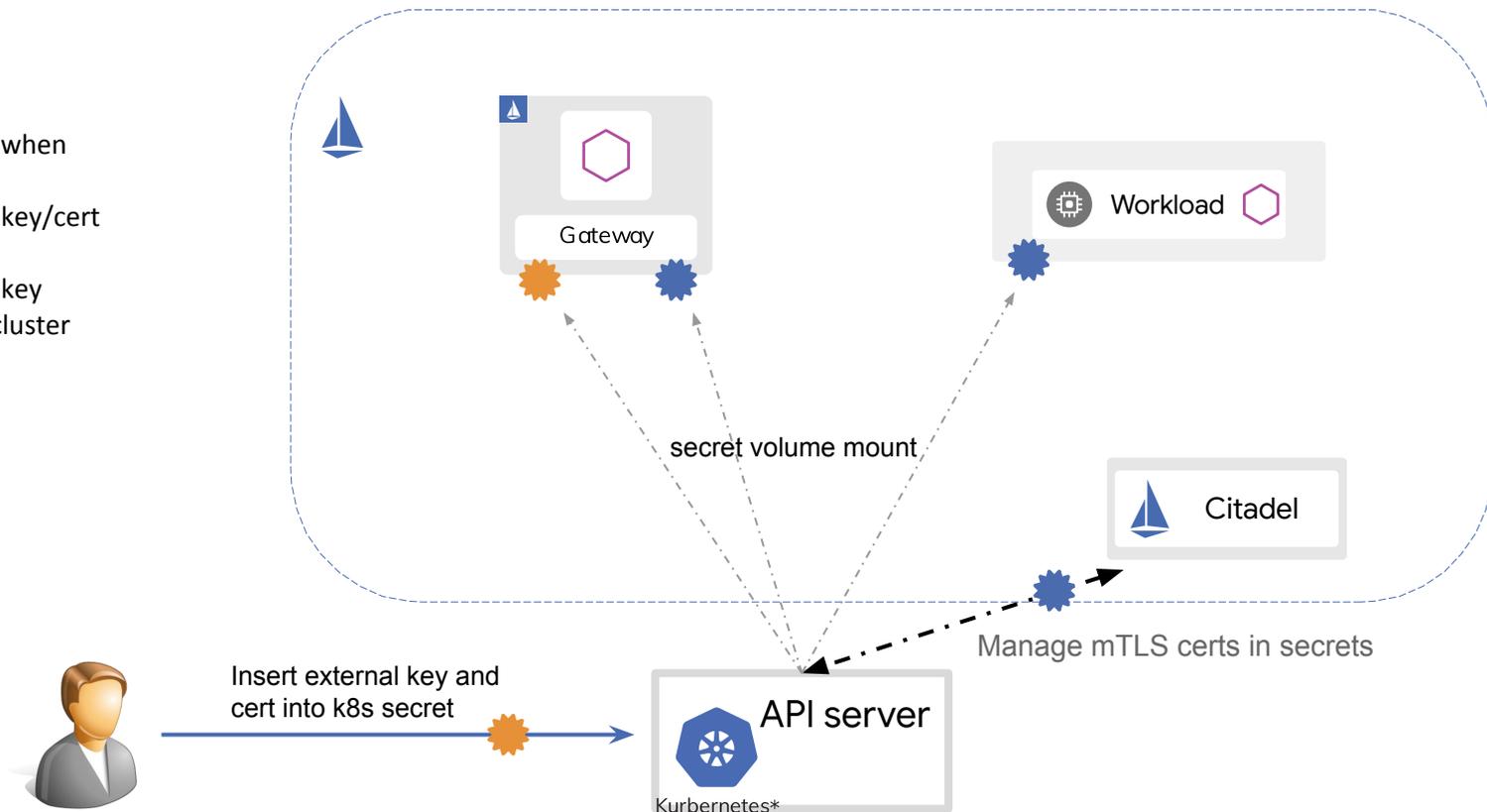
Istio authentication flows



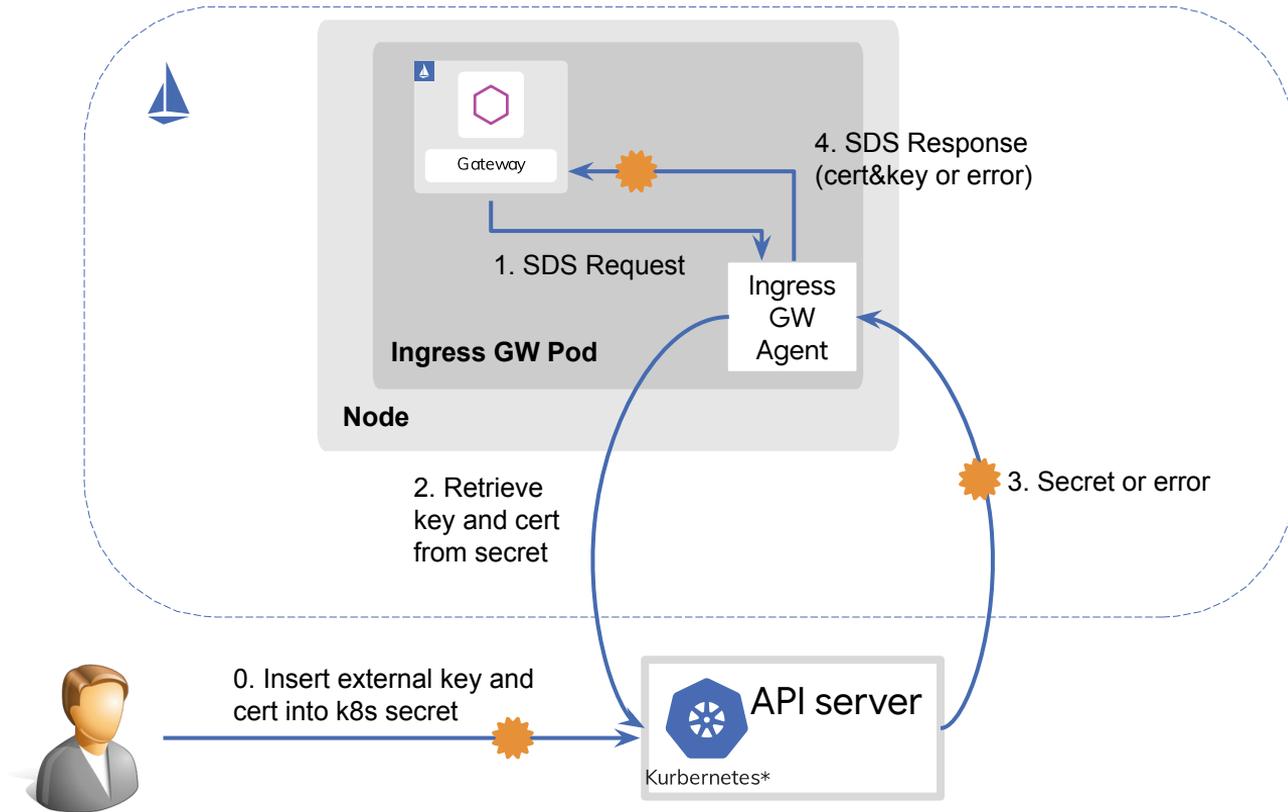
Legacy cert management with secret volume mount

Problems

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



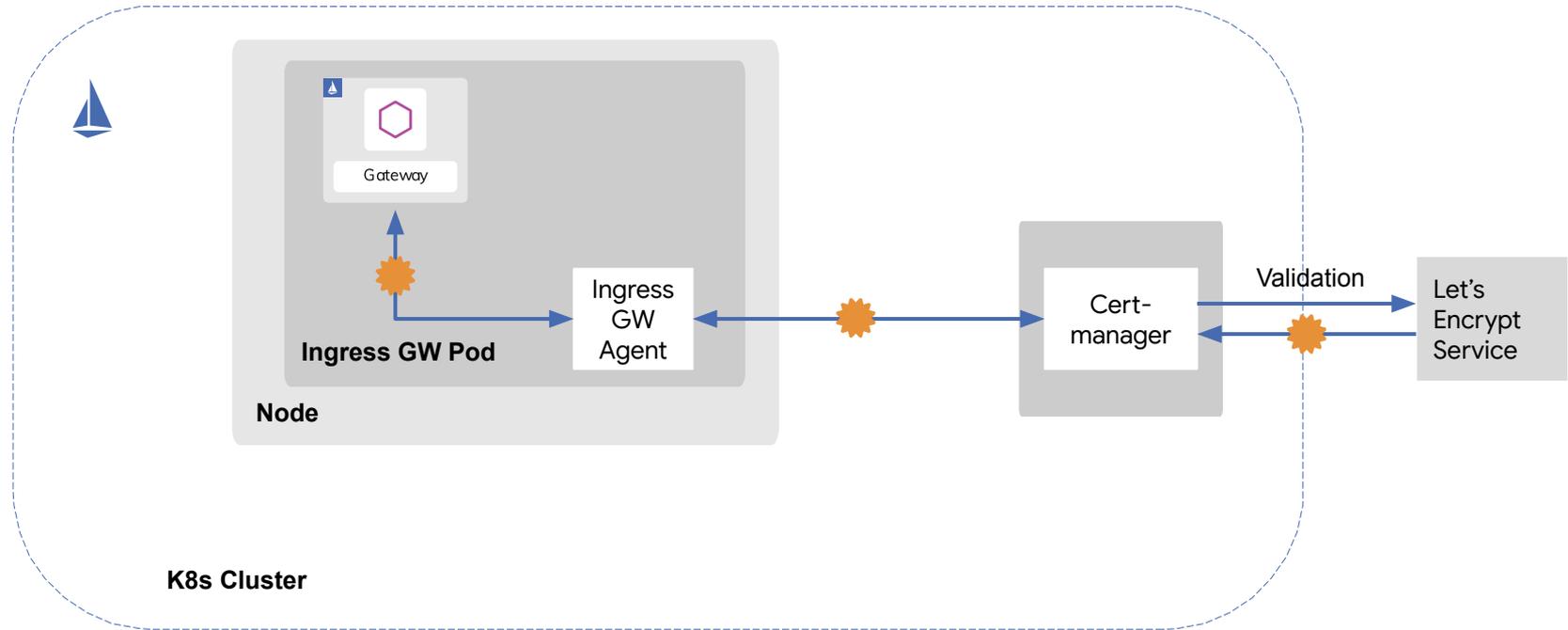
SDS external certificate management



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

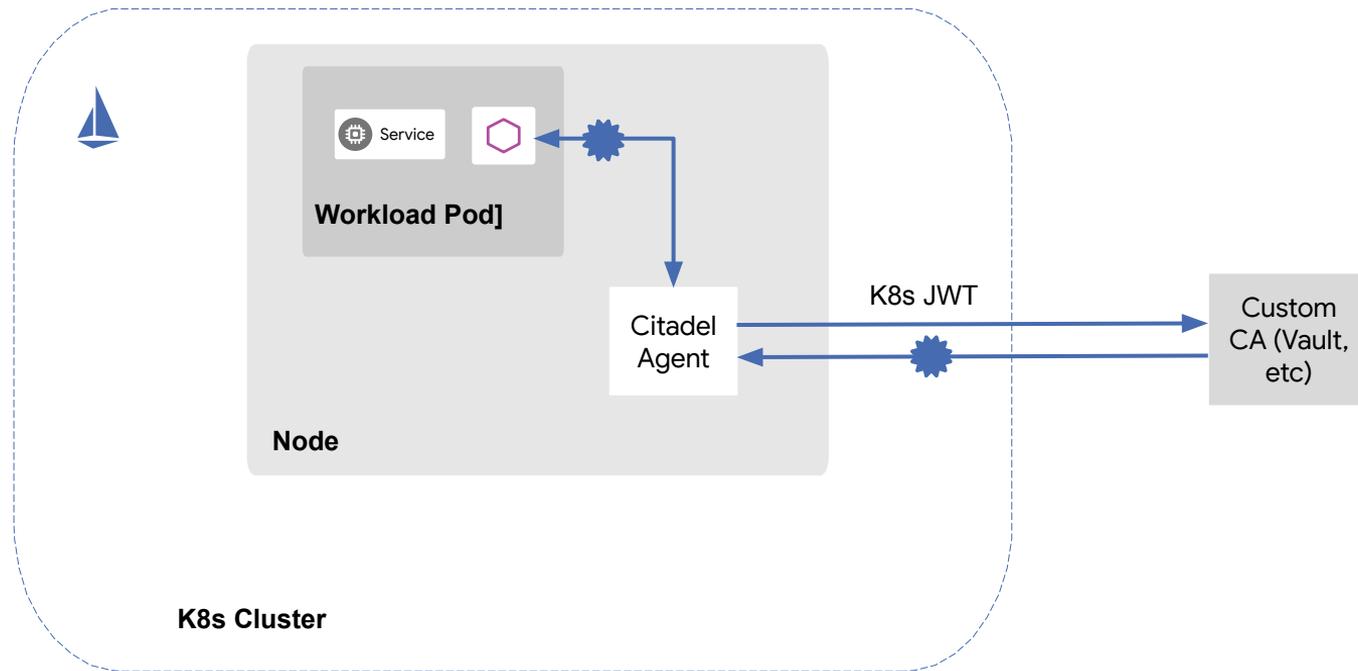
Integrate with cert-manager (Let's Encrypt)



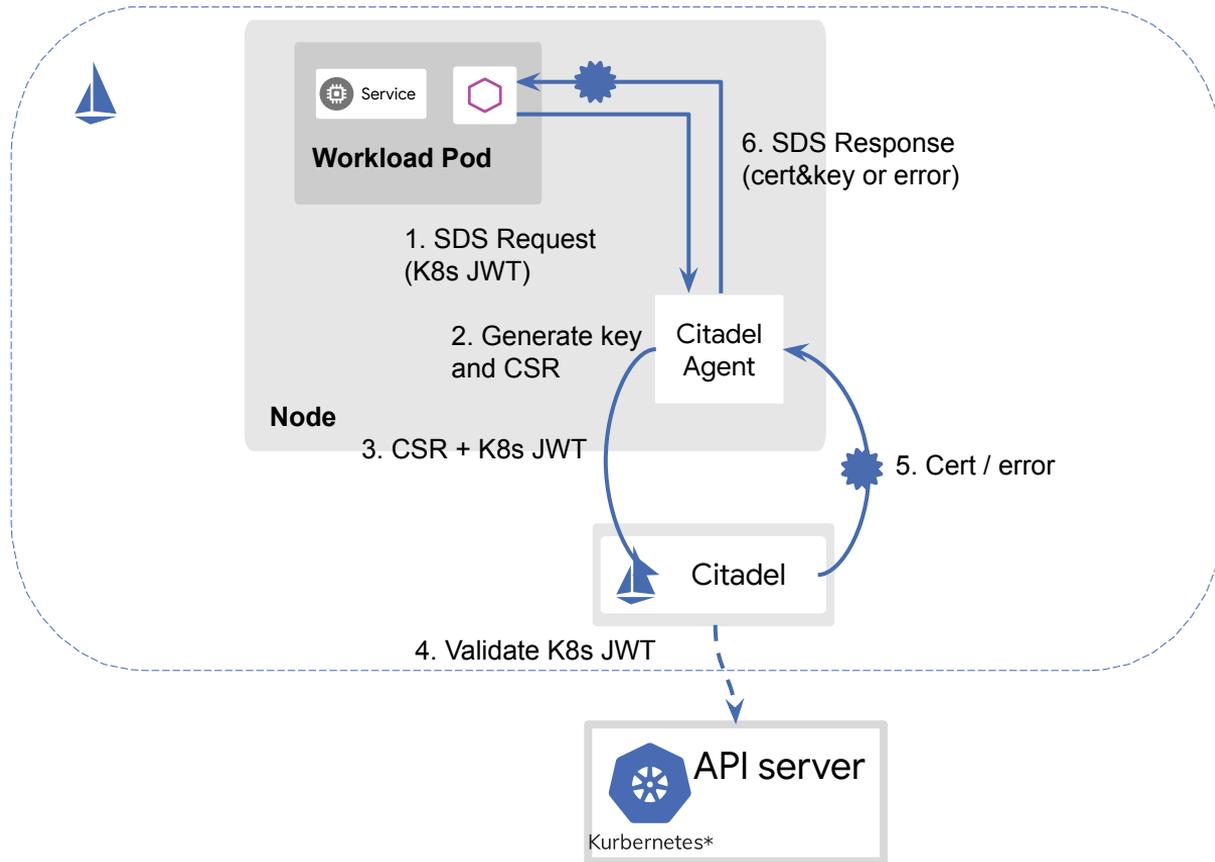
Demo

Q&A

Integrate with custom CA



SDS workload certificate management





KubeCon



CloudNativeCon

Europe 2019



KubeCon



CloudNativeCon

Europe 2019

Istio Value Proposition



KubeCon



CloudNativeCon

Europe 2019



KubeCon



CloudNativeCon

Europe 2019