KubeCon

North America 2017

Istio: Sailing to a Secure Services Mesh

Spike Curtis, *Tigera* & Dan Berg, *IBM*

Problem Statement

IT’s shift to a modern distributed architecture has left enterprises unable to monitor, manage or secure their services in a consistent way.

Why?

- **Network:** How do you handle lapses?
- **Auth[n|z] is critical:**
  - Each service does its own authentication and authorization
  - Increased attack vector
- **Observability:** To understand the behavior of the system requires deep monitoring of every service
- **Fault tolerance:** Many teams reimplementing retries, flow control, circuit breaking
- **Ops needs a cross-platform toolchain:**
  - Canary releases, Blue-Green Deployments
  - Tracing and Hot spot analysis across services
  - Making changes without slowing dev workflows
  - Managing and rolling out configuration changes

Introducing Istio

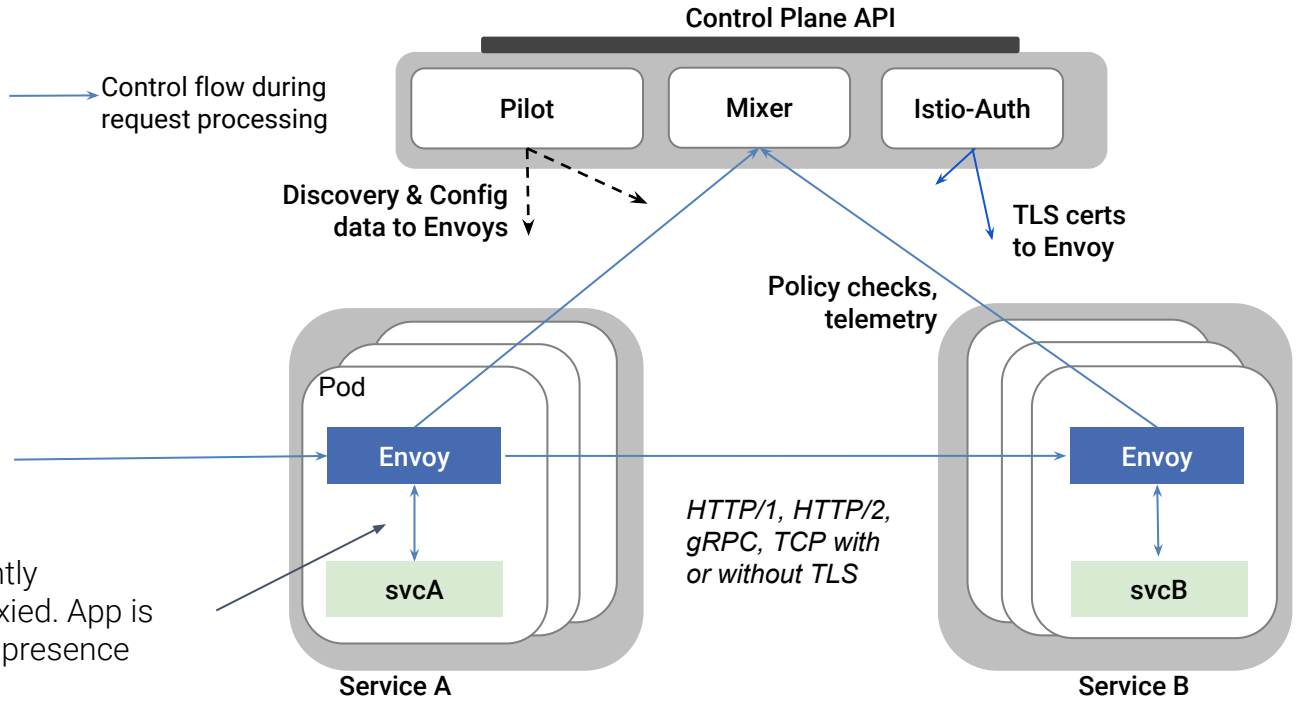
An open platform to connect, manage, monitor and secure services

- **Connect**: Resiliency, discovery, load balancing
- **Manage**: Traffic control, policy enforcement
- **Monitor**: Metrics, Logging, Tracing
- **Secure**: End-to-end Authentication and Authorization

Why Istio?

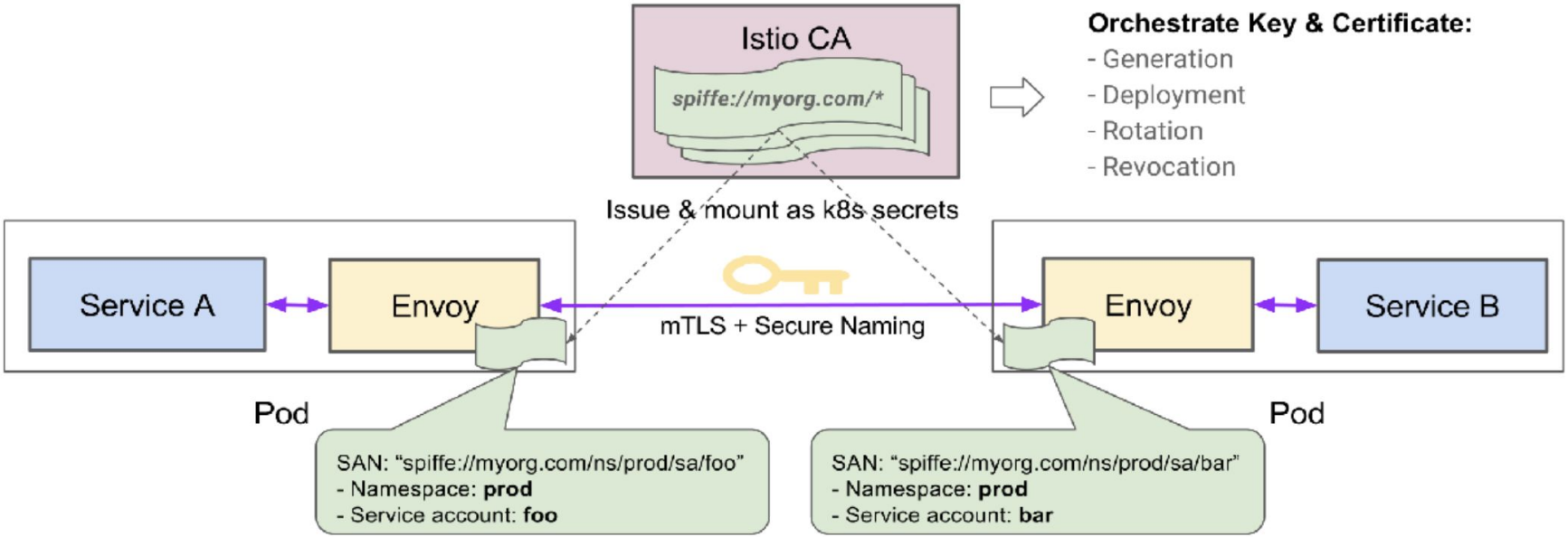
- **Resiliency & efficiency in services:**
  - Retries, flow control
- **Policy driven ops**
  - Traffic routing and shaping
  - Rate limits to prevent overload of services
  - Improvements to security, monitoring, scaling without code changes
- **Fleet wide visibility**
  - Monitor: metrics, logging, tracing
  - Cost Visibility
- **Secure by default**
  - End-to-end authentication and authorization

Architecture of Istio

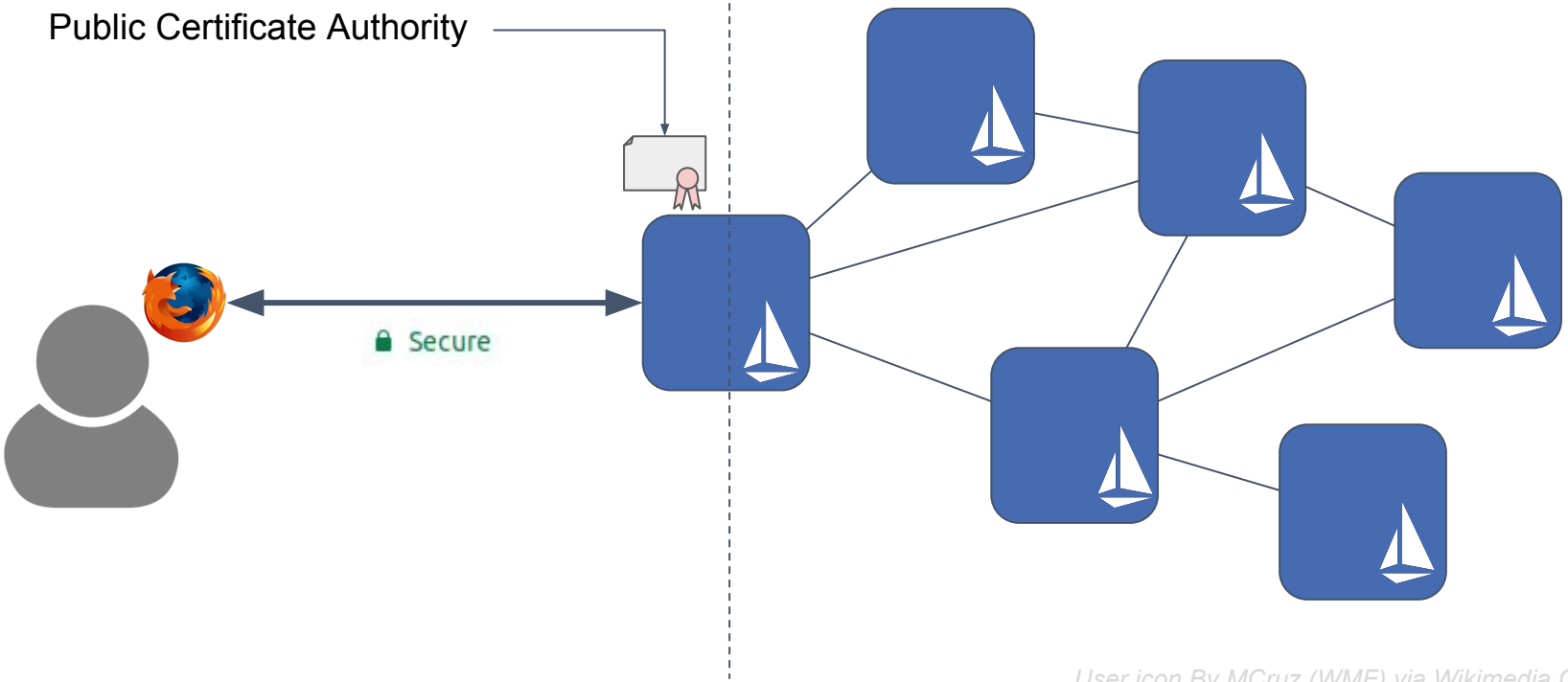


Traffic is transparently intercepted and proxied. App is unaware of Envoy's presence

Mutual TLS with Istio-Auth

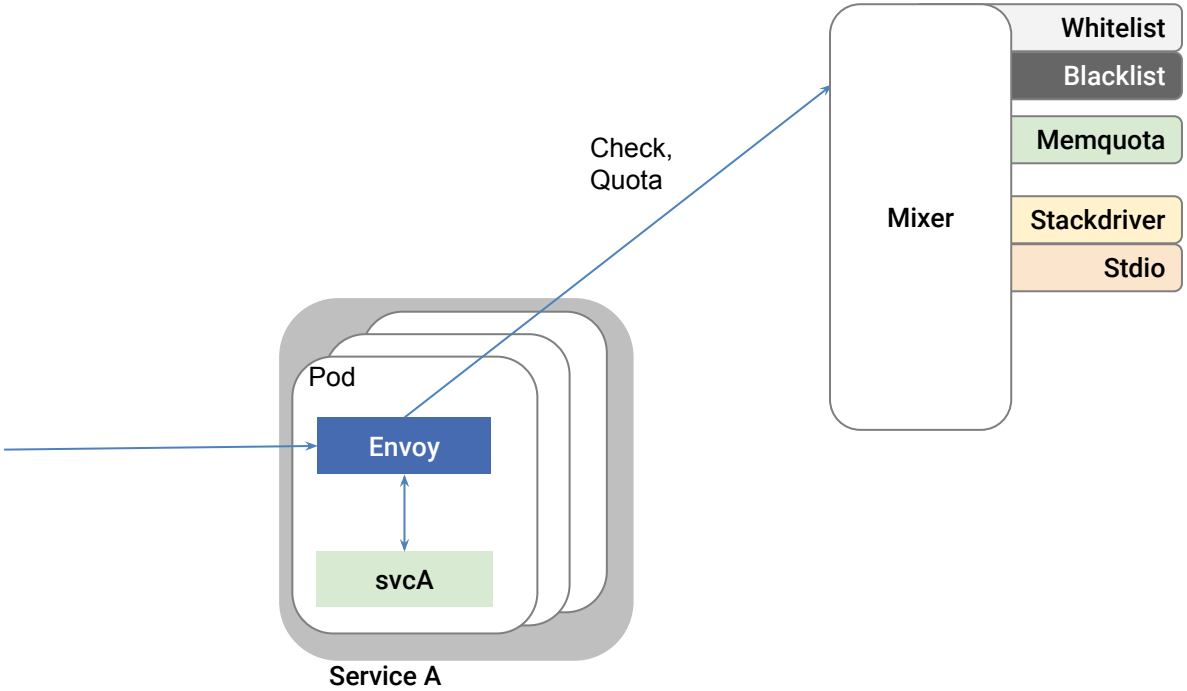


Istio Ingress TLS

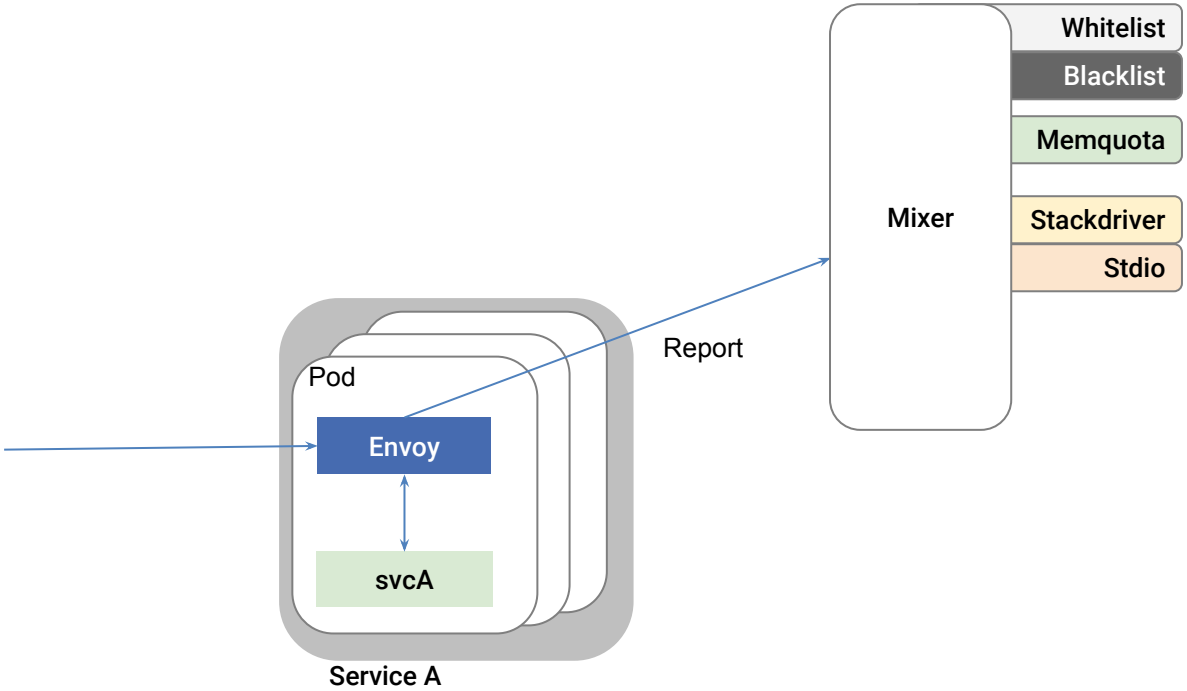


User icon By MCruz (WMF) via Wikimedia Commons

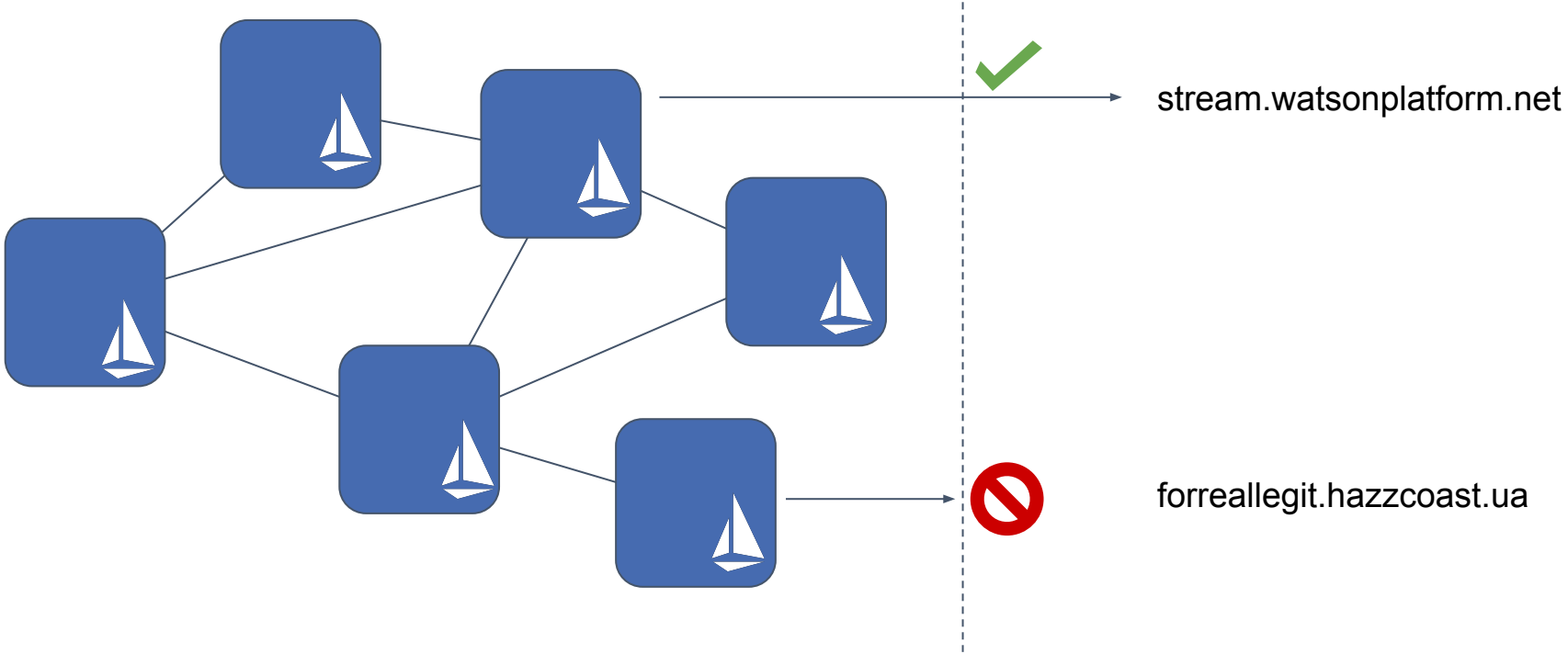
Mixer Authorization Adapters



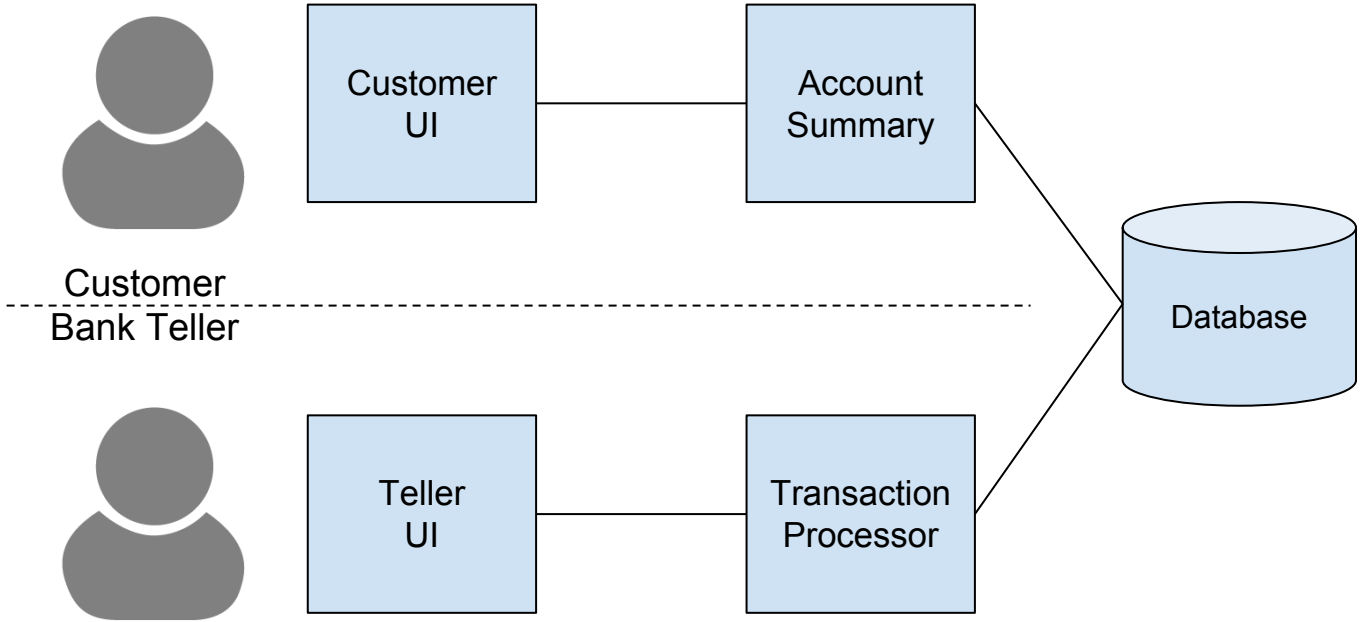
Mixer Logging Adapters



Istio Egress Policy



Demo



Istio Security Built on K8s Concepts

- Istio Config = K8s Custom Resources
  - Secure Istio Config the same way you secure K8s Config.
- Workload Identity = ServiceAccount
- Authorization
  - Istio RBAC designed to look like Kubernetes RBAC
  - Calico policy extends from K8s Network Policy

Roadmap (*planned*)

Q4 2017

- Mutually Authenticated TLS (mTLS)
  - Per-service enable/disable
  - No downtime rollout
- SNI for Ingress
- Authorization Policy Choices
  - Role-Based Access Control (RBAC)
  - Open Policy Agent
  - Calico Unified Policy
- “Istio on Istio” security for Pilot, Mixer, CA

Roadmap (*proposed*)

Q1 2018

- Mutually Authenticated TLS
  - Interop with non-mesh services
  - Authentication across cluster boundaries
- End user authentication with JSON Web Tokens (JWTs)
- Integrate with cloud Identity & Access Management
- External Certificate Authorities (e.g. Vault)

Thanks!

Contact us:

istio-users@googlegroups.com

istio-dev@googlegroups.com

@IstioMesh

More information: istio.io