Deep Dive SPIFFE/SPIRE

Scott Emmons and
Emiliano Berenbaum

SCYTALE

AGENDA

- Since last KubeCon
- Experimental Istio CA Module
- Deploying SPIRE on Kubernetes
- Demo

SCYTALE

SPIFFE talks at KubeCon 2019

Introduction to SPIFFE	Tuesday, May 21 11:55
Zero Trust Service Mesh with Calico, SPIRE and Envoy	Wednesday, May 22 11:05
Deep Dive: SPIFFE	Wednesday, May 22 14:50
Securing Multi-Cloud Cross-Cluster Communication with SPIFFE and SPIRE	Thursday, May 23 14:00
Uber x Security: Why and How we Built Our Workload Identity Platform	Thursday, May 23 16:45

Since Last KubeCon

SCYTALE

K8 work

SAT Attestor

SCYTALE

K8 work

SAT Attestor

PSAT Attestor

SCYTALE

K8 work

SAT Attestor

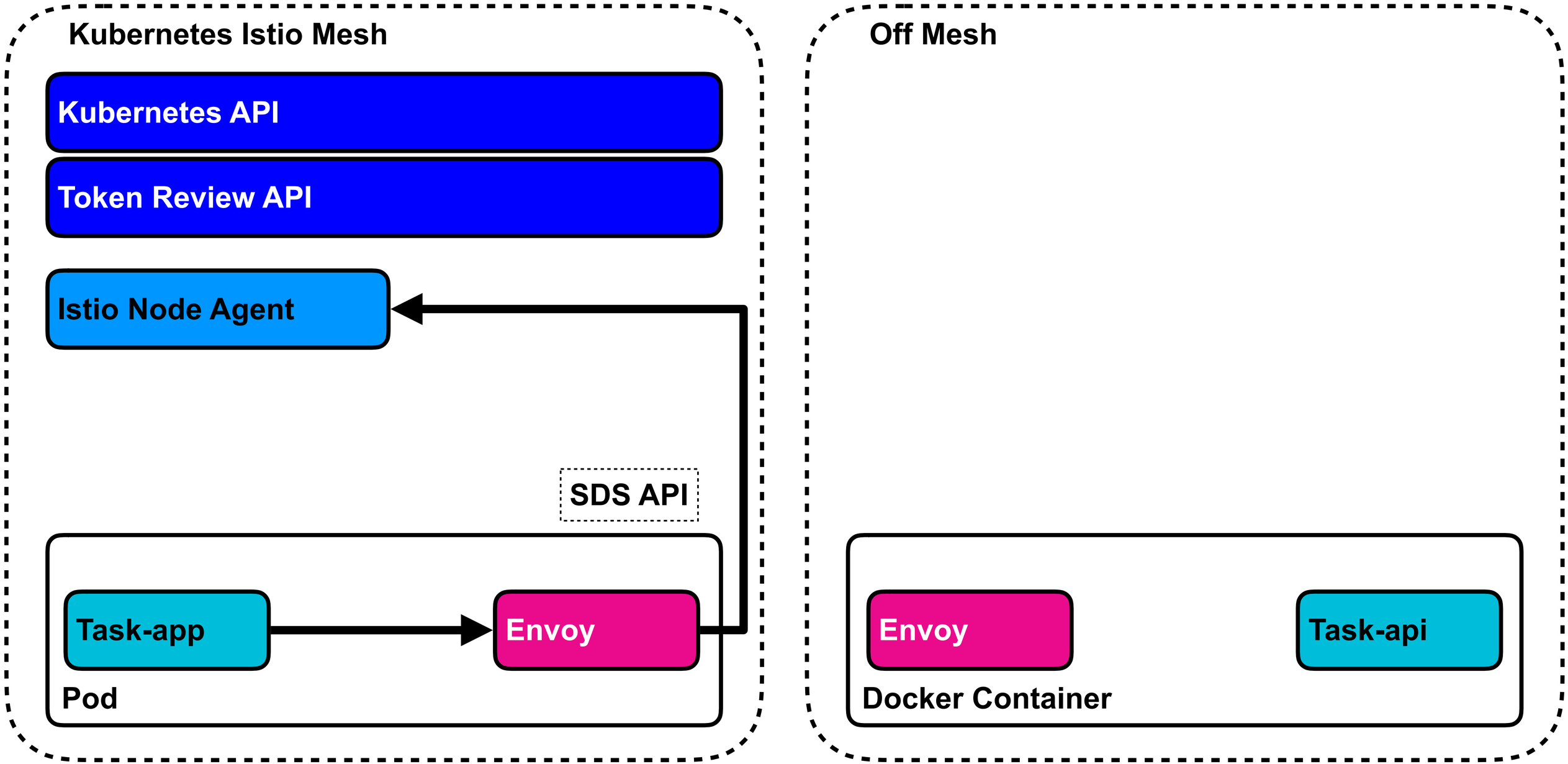
PSAT Attestor

K8s Bundle Notifier

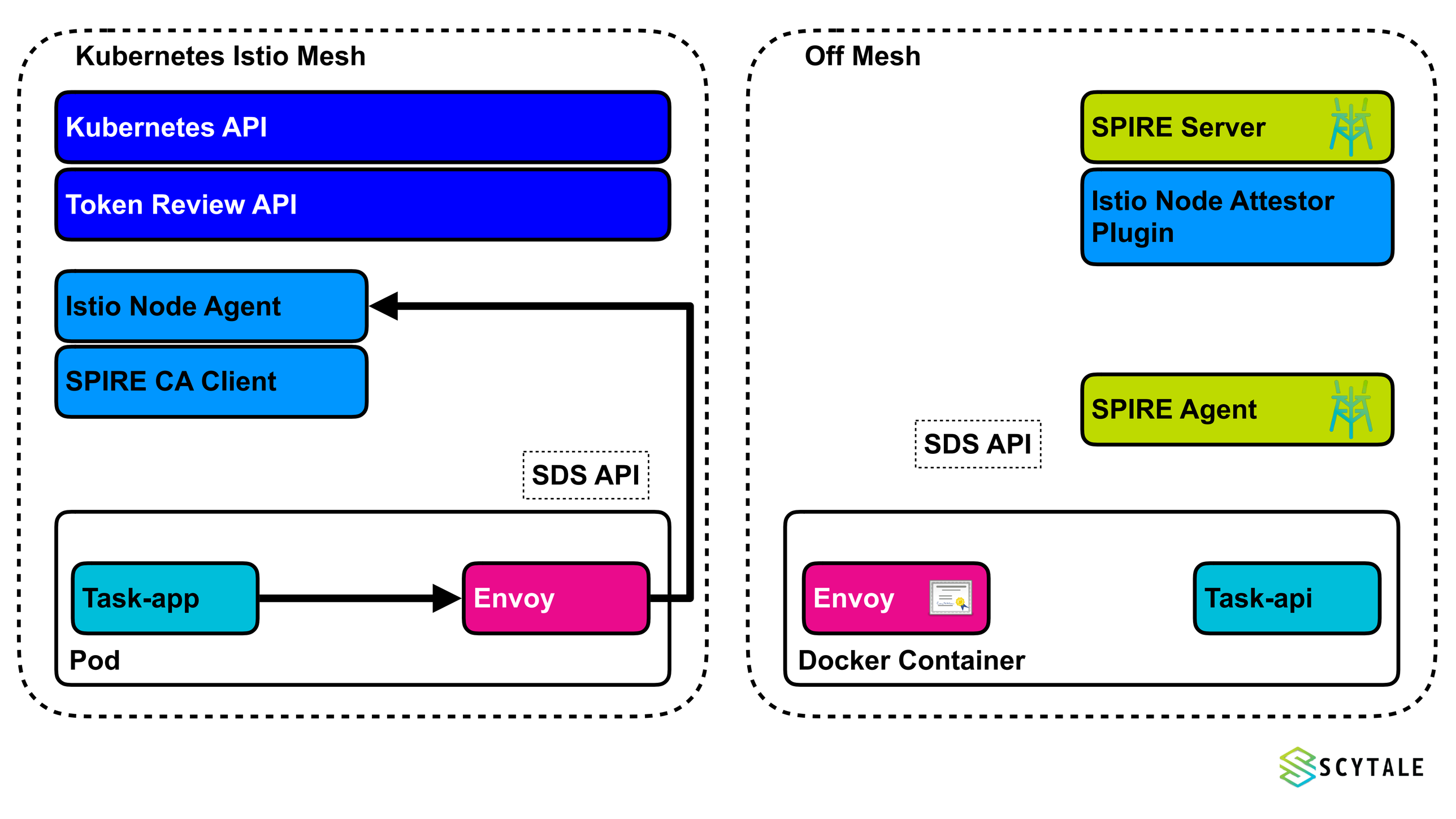
SCYTALE

Experimental Istio CA Module

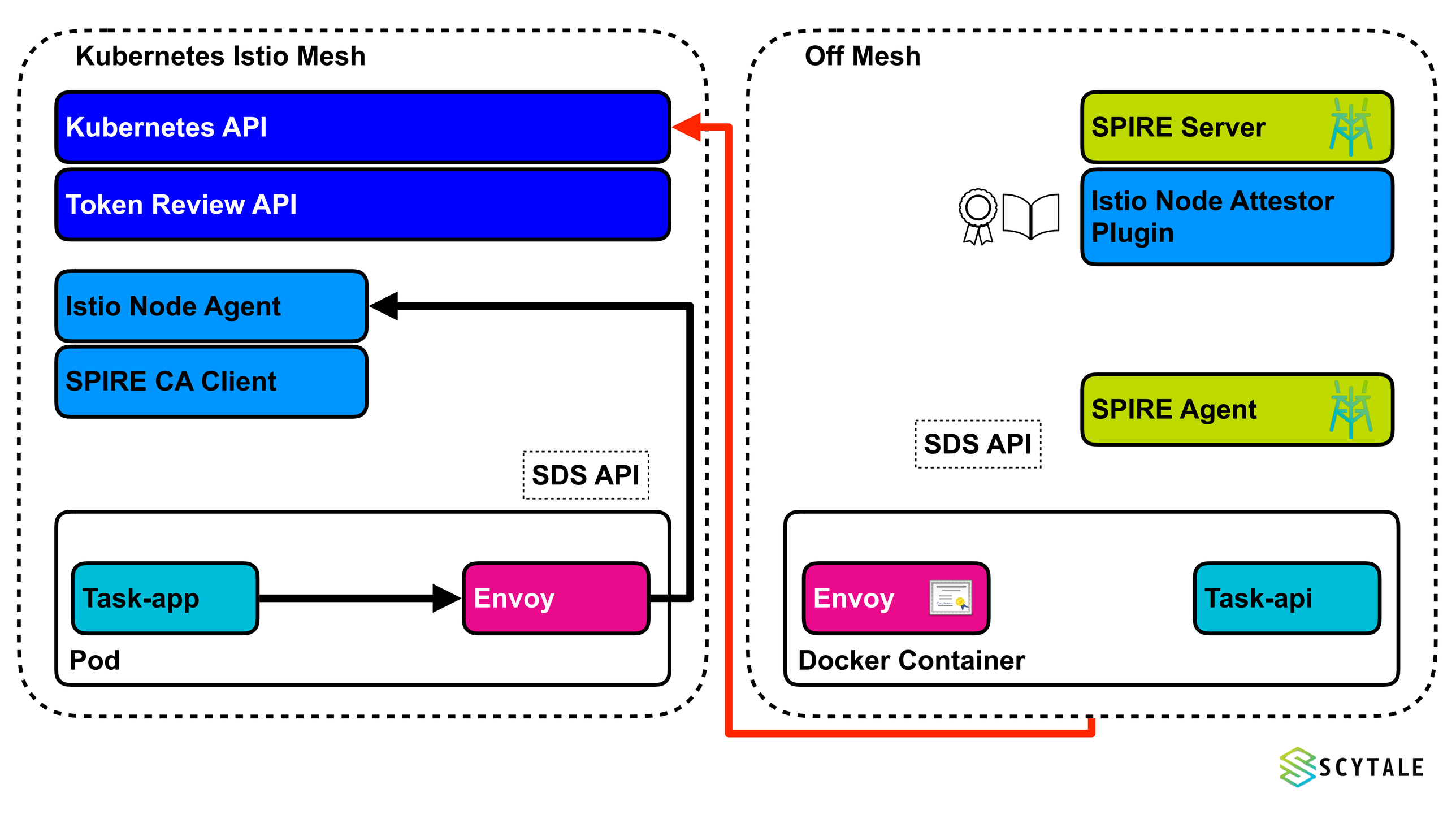
SCYTALE

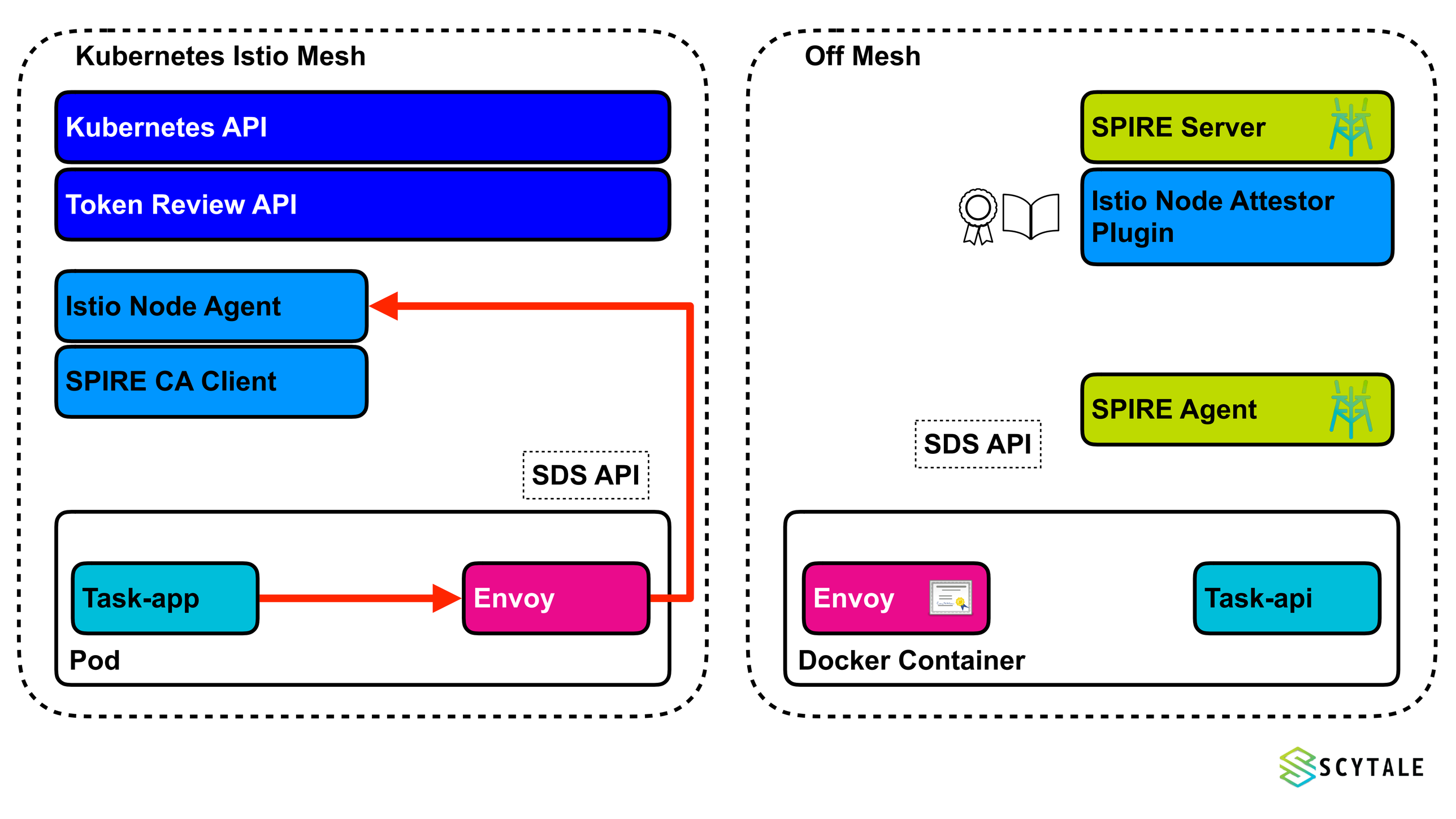

Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SDS API
Task-app
Envoy
Pod
Off Mesh
Envoy
Task-api
Docker Container

SCYTALE

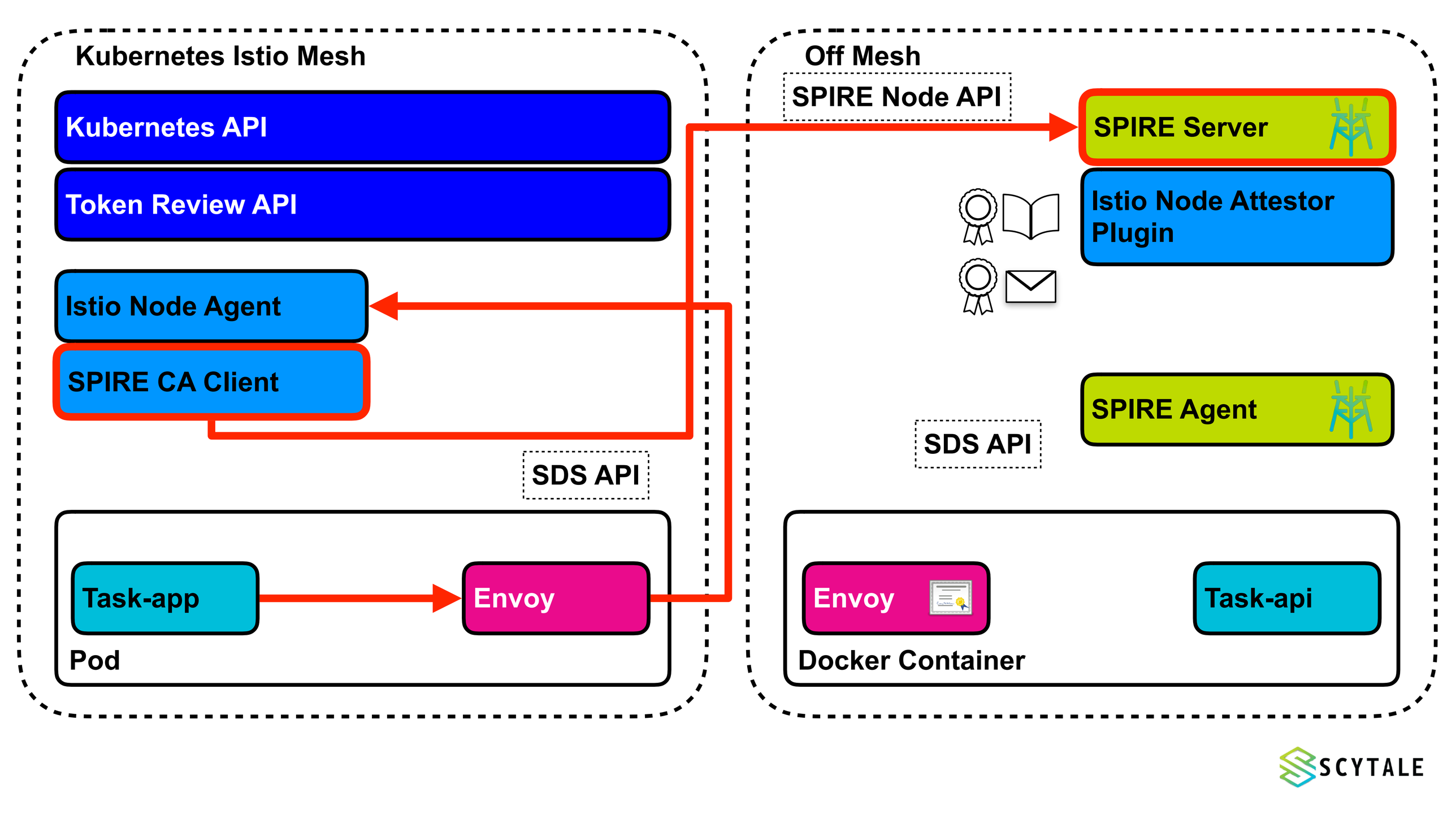

Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container

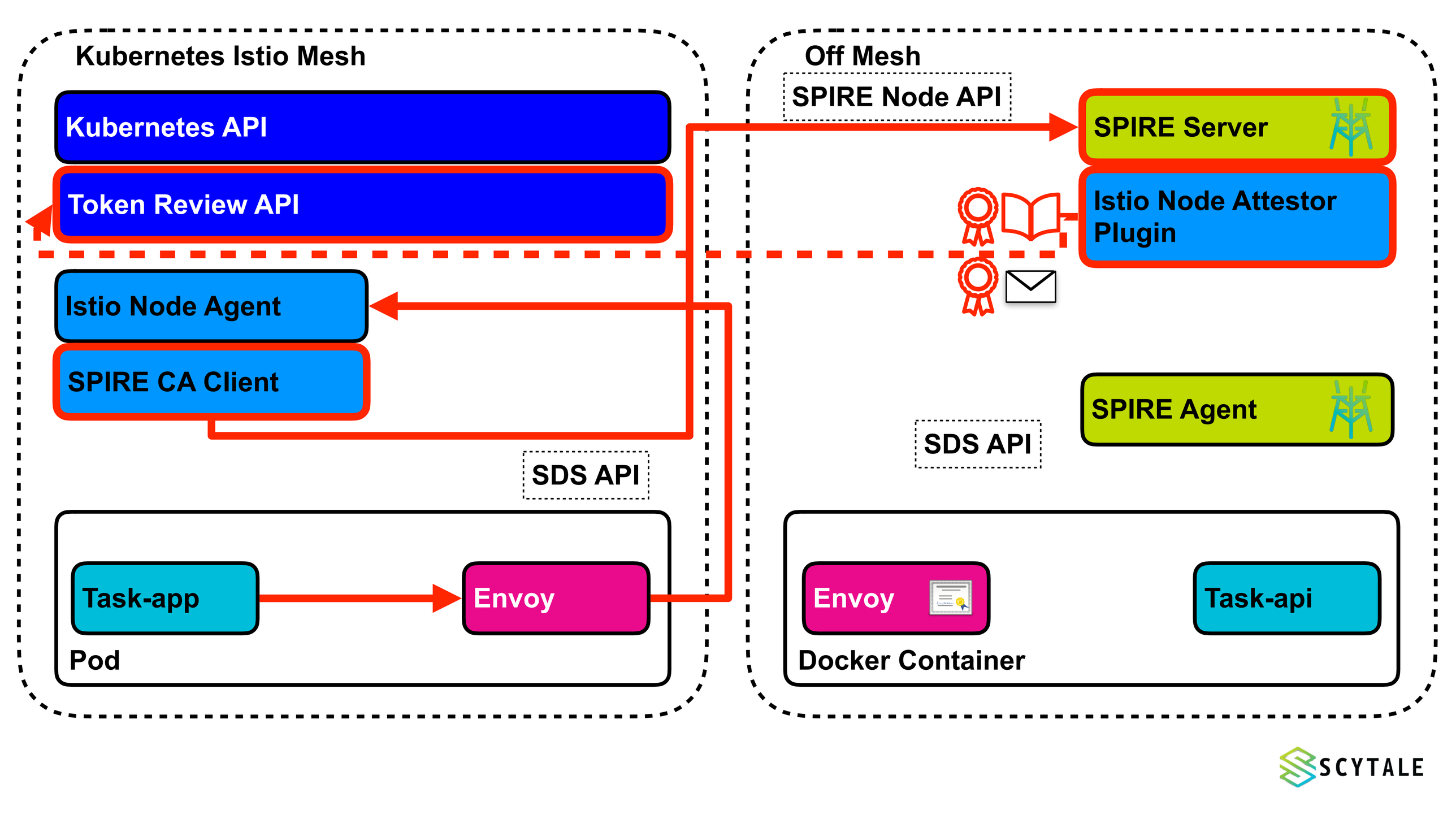
SCYTALE

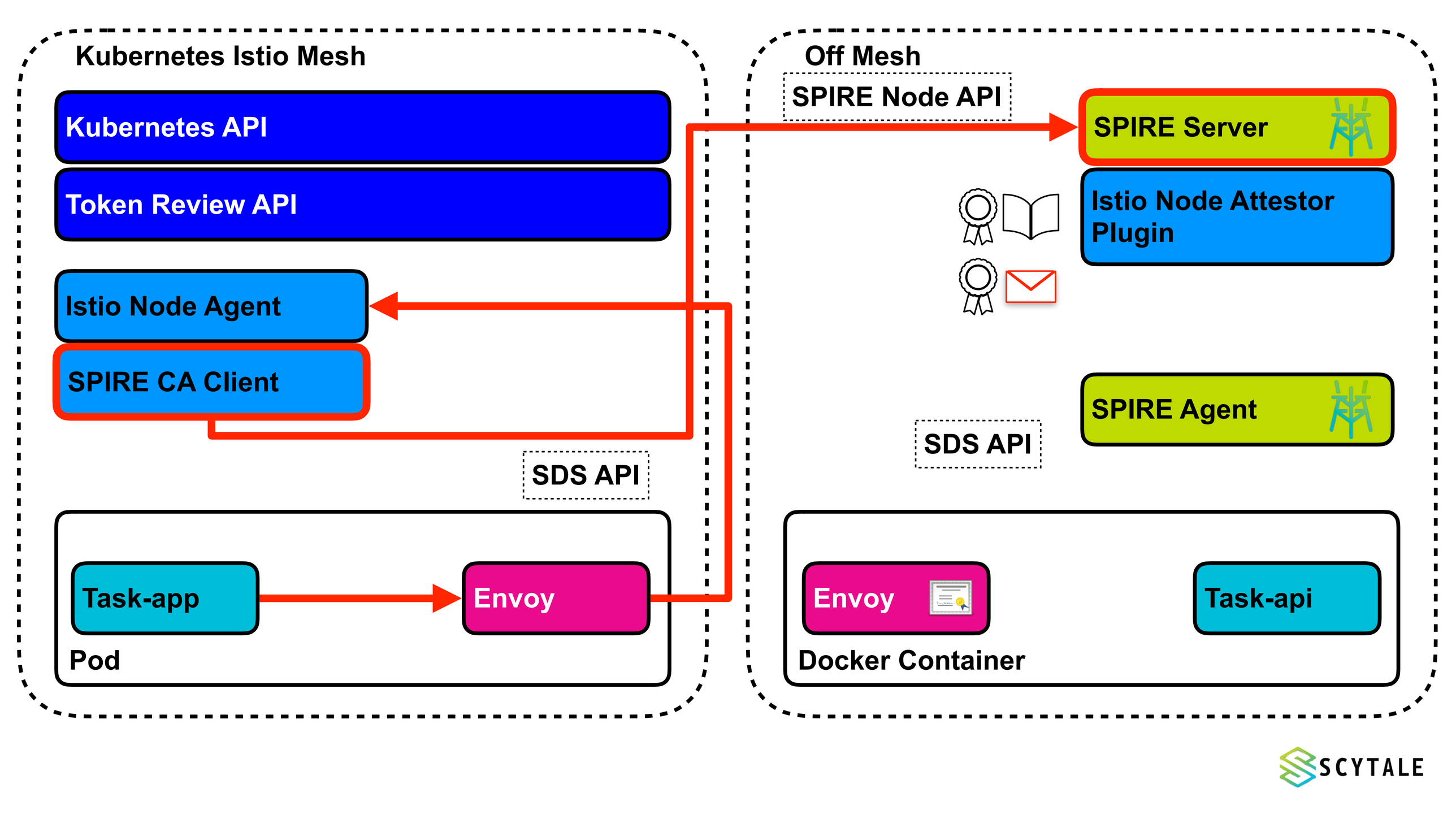

Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container
SCYTALE


Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container

SCYTALE


Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Node API
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container
SCYTALE


Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Node API
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container
SCYTALE


Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Node API
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container
SCYTALE

Kubernetes Istio Mesh

Kubernetes API

Token Review API

Istio Node Agent

SPIRE CA Client

SDS API

Task-app

Envoy

Pod

Off Mesh

SPIRE Server

Istio Node Attestor Plugin

SPIRE Agent

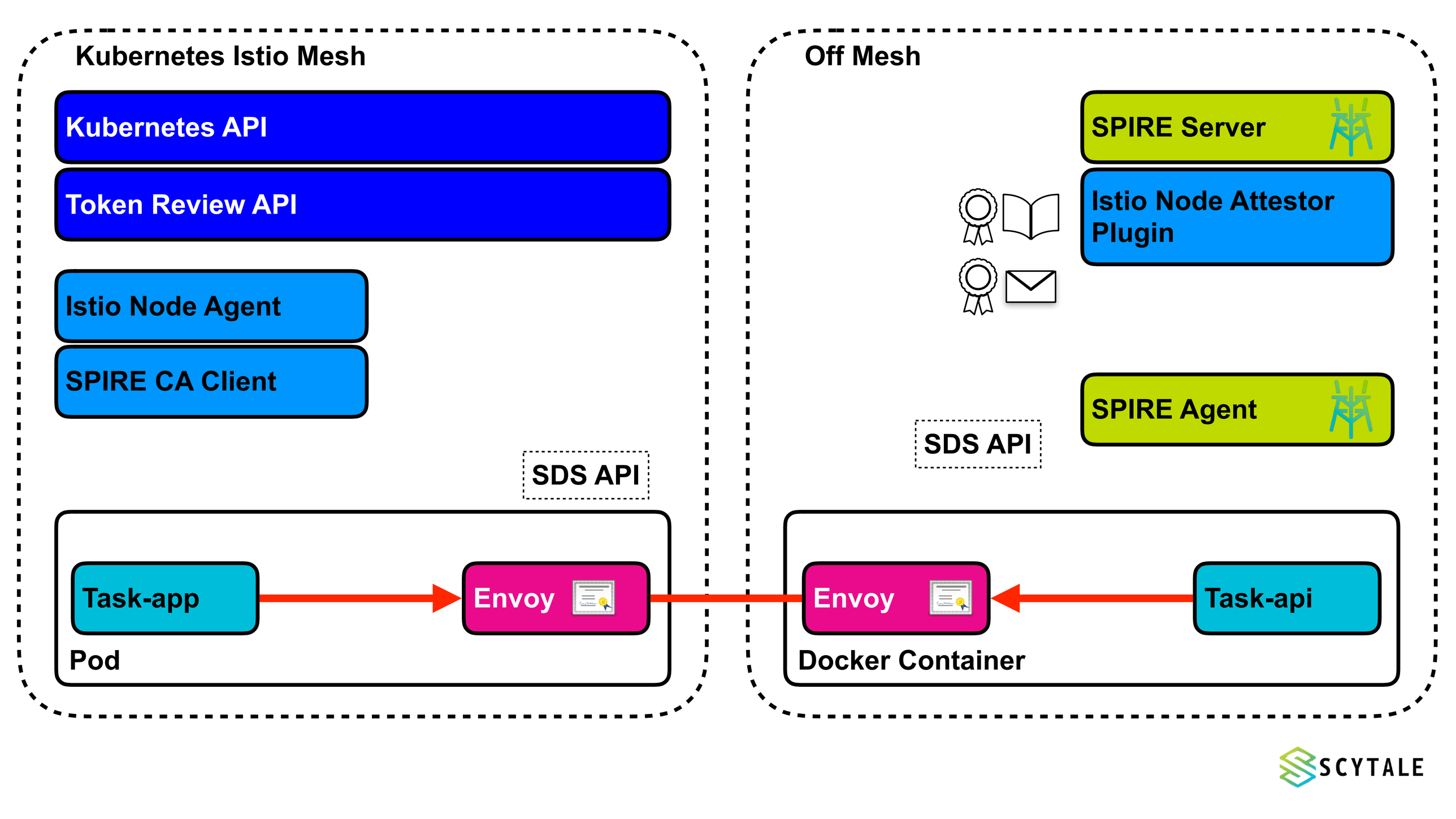
SDS API

Envoy

Task-api

Docker Container

SCYTALE


Kubernetes Istio Mesh
Kubernetes API
Token Review API
Istio Node Agent
SPIRE CA Client
SDS API
Task-app
Envoy
Pod
Off Mesh
SPIRE Server
Istio Node Attestor Plugin
SPIRE Agent
SDS API
Envoy
Task-api
Docker Container
SCYTALE

Kubernetes Istio Mesh

Kubernetes API

Token Review API

Istio Node Agent

SPIRE CA Client

SPIRE Server

Istio Node Attestor Plugin

Task-app

Envoy

Pod

Off Mesh

SPIRE Agent

Envoy

Task-api

Docker Container

SCYTALE

Deploying SPIRE on Kubernetes

SCYTALE

SPIRE Server

- Typically deployed as a StatefulSet
- Use a persistent volume for **data_dir** (VolumeClaimTemplate)
- Requires a shared database (Postgres or MySQL)
- Scaling out SPIRE servers is fairly easy
  - Load balancer or round-robin DNS
- The certificate store is eventually consistent, not synchronous
- Servers need to be deployed in a controlled, rolling manner

SPIRE Agent

- Deployed as a DaemonSet
- May require local storage for **data_dir** (hostPath)
  - Depends on attestor
- Expose agent workload API socket directory for workloads
  - Not just the socket file

SPIRE Agent

```
Agent:
      volumeMounts:
        - name: spire-agent-socket
          mountPath: /run/spire/sockets
          readOnly: false
…
   volumes:
    - name: spire-agent-socket
      hostPath:
        path: /run/spire/sockets
        type: DirectoryOrCreate
```

SCYTALE

SPIRE Agent

```
Workload:
      volumeMounts:
        - name: spire-agent-socket
          mountPath: /run/spire/sockets
          readOnly: true
…
   volumes:
    - name: spire-agent-socket
      hostPath:
        path: /run/spire/sockets
        type: Directory
```

SCYTALE

Node Attestation

- Kubernetes Attestors
  - SAT - Service Account Token
  - PSAT - Projected Service Account Token
- Cloud Provider Attestors
  - AWS IID, AZURE MSI, and GCP IID Attestors
  - Requires local **data_dir** - agent can only attest once per instance

Kubernetes Attestors - SAT, PSAT

- Verification Methods
  - Token Certificate / Public Key
  - Token Review API
- SAT and PSAT attestors support either

SPIRE Server - k8s bundle notifier

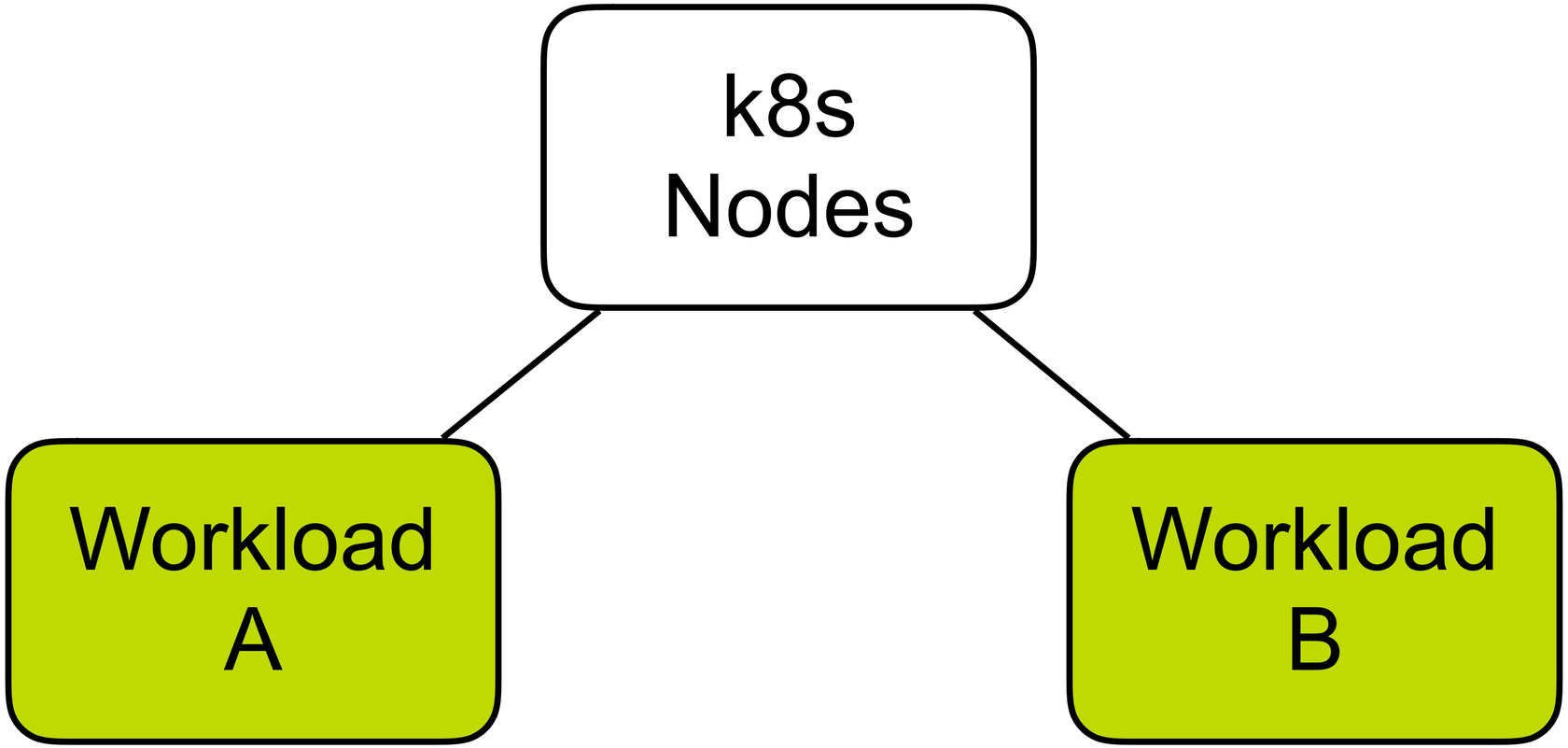
- New bundle notifier plugin can replace both bootstrap certificate and upstream CA
- Certificate bundle is stored in a ConfigMap
- Certificates are created and rotated by the SPIRE server via k8s API
- The ConfigMap is mounted ReadOnly in SPIRE agents
- SPIRE server **data_dir** needs to be persistent

Registration Entries

- Put some thought into how workload nodes will be grouped
- Create hierarchies and groupings that are natural
- Avoid creating manual entries that use specific node UUIDs for example:

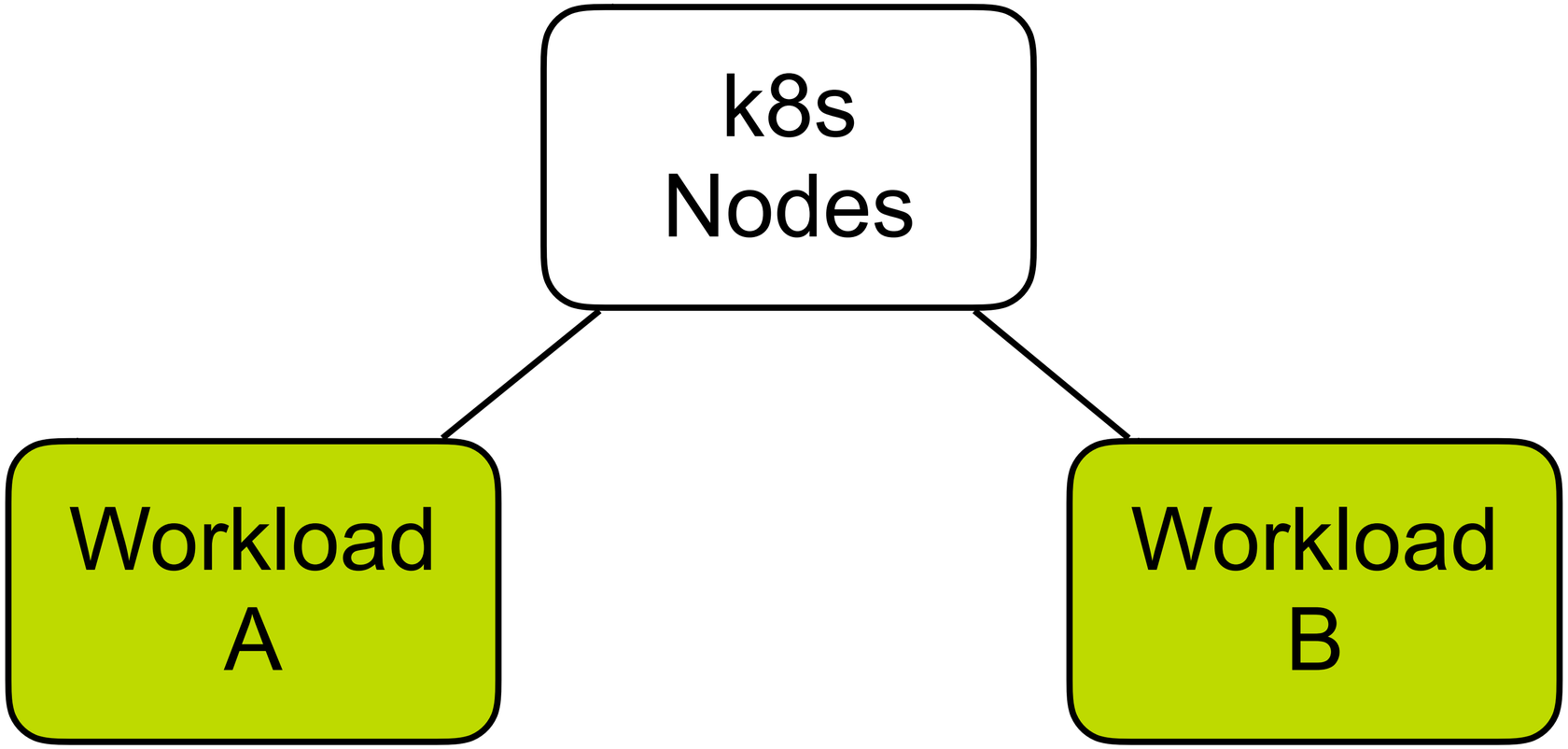
spiffe://mycluster/spire/agent/k8-sat/mycluster/2527c4f7-e154-a169-318a2f61478

Registration Entries



Registration Entries

spiffe://mycluster.io/nodes

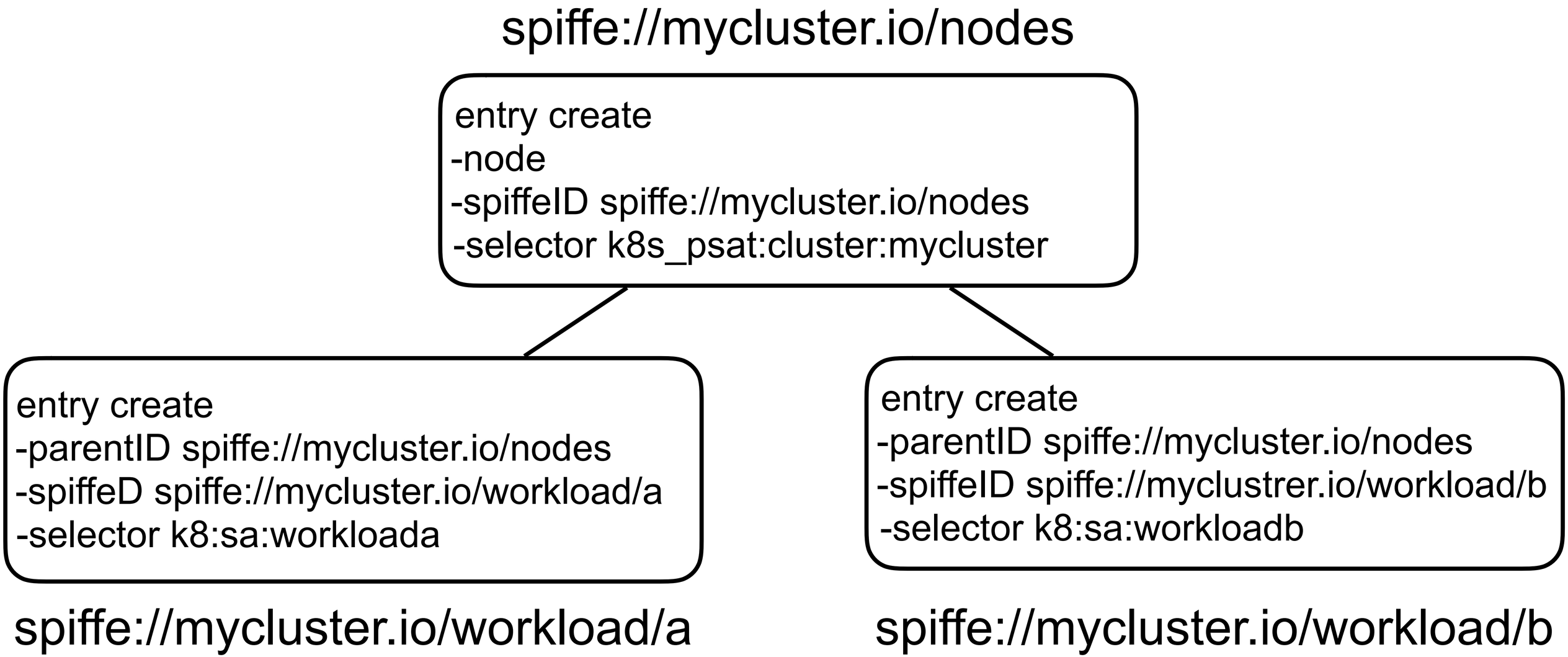


spiffe://mycluster.io/workload/a

spiffe://mycluster.io/workload/b

SCYTALE

Registration Entries



SCYTALE

Demo time!

SCYTALE

Try it out

spiffe/spiffe

spiffe/spire

slack.spiffe.io

SCYTALE

Questions?

SCYTALE