KubeCon | CloudNativeCon

North America 2019

KubeCon | CloudNativeCon

North America 2019

Securing Communication Between Meshes and Beyond with SPIFFE Federation

Evan Gilman, Oliver Liu

Agenda

Role of Identity in a Service Mesh

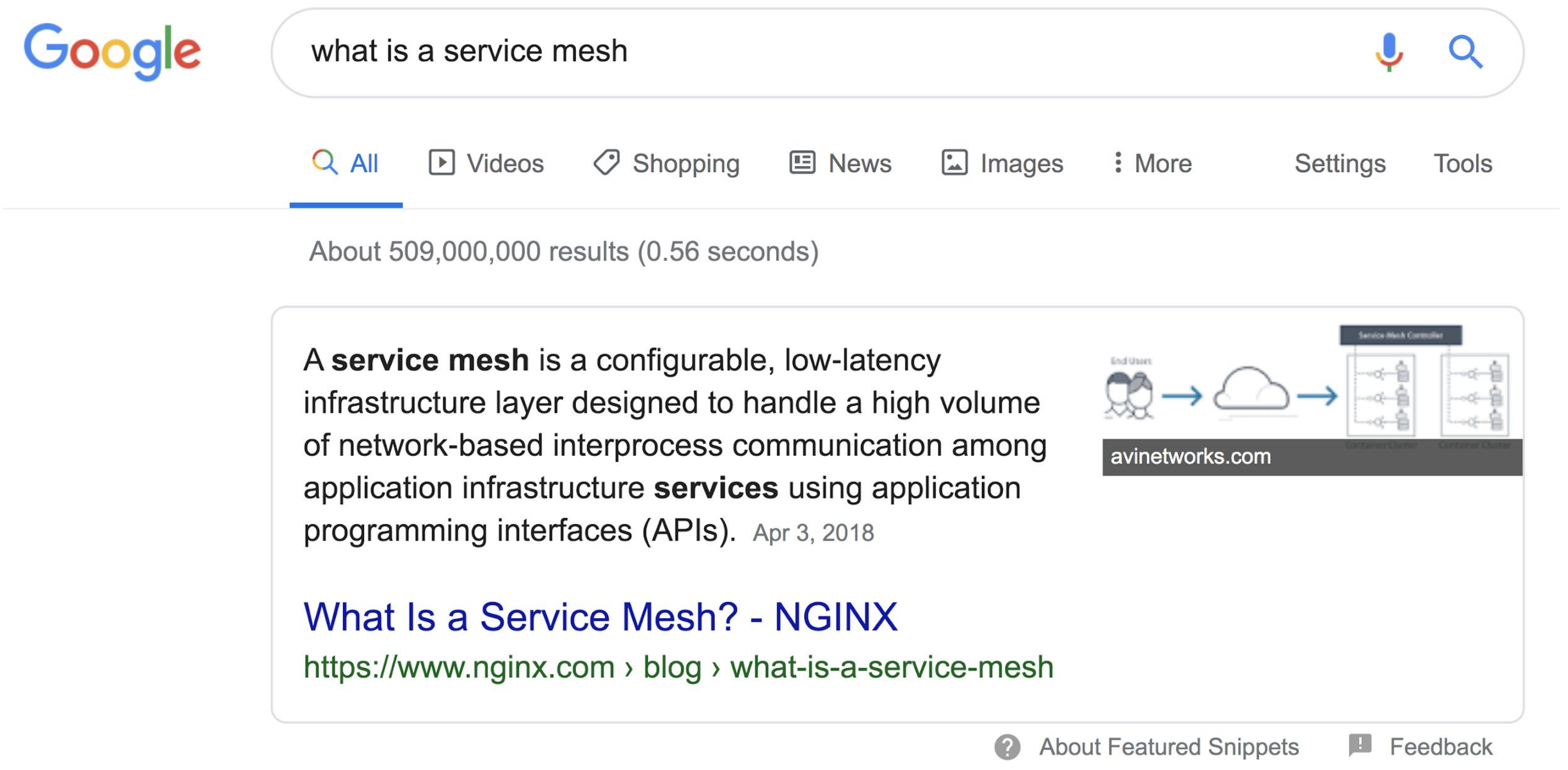
Hybrid and Multi-Mesh Challenges

SPIFFE Federation

Demo!

What is a Service Mesh?

What is a Service Mesh?



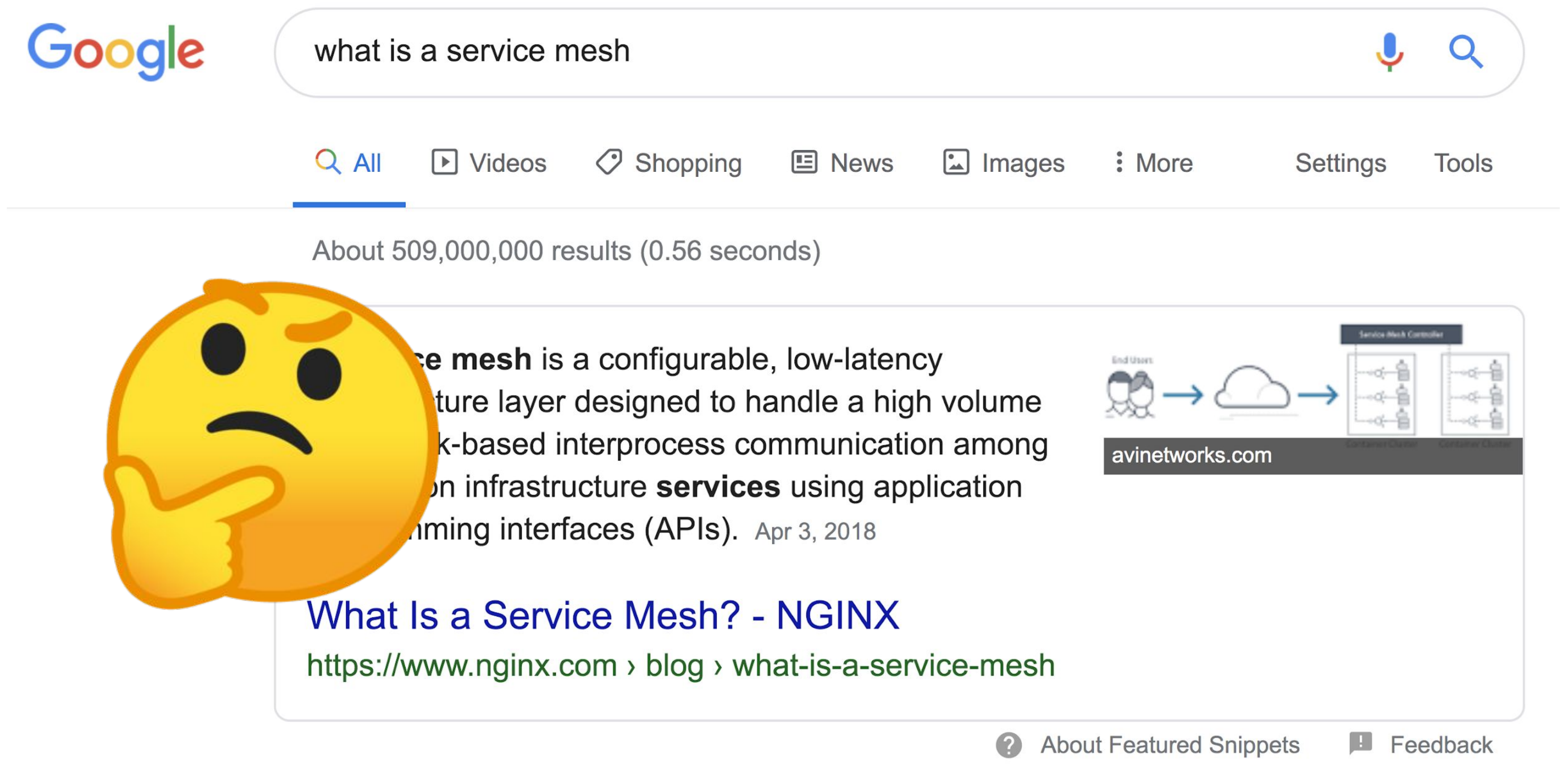
About 509,000,000 results (0.56 seconds)

A **service mesh** is a configurable, low-latency infrastructure layer designed to handle a high volume of network-based interprocess communication among application infrastructure **services** using application programming interfaces (APIs). Apr 3, 2018

What Is a Service Mesh? - NGINX

https://www.nginx.com › blog › what-is-a-service-mesh

What is a Service Mesh?



what is a service mesh

About 509,000,000 results (0.56 seconds)

ce mesh is a configurable, low-latency
ture layer designed to handle a high volume
k-based interprocess communication among
on infrastructure **services** using application
mming interfaces (APIs). Apr 3, 2018

avinetworks.com

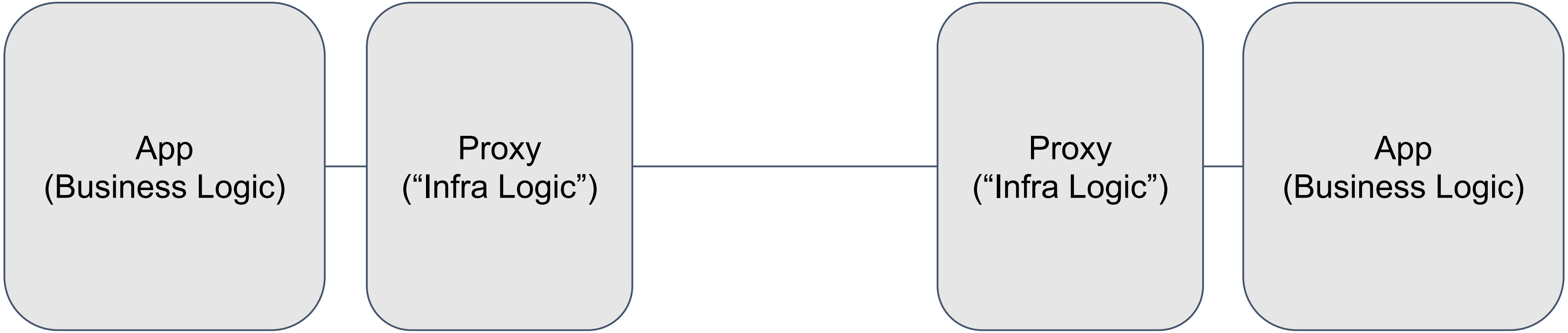
What Is a Service Mesh? - NGINX

https://www.nginx.com › blog › what-is-a-service-mesh

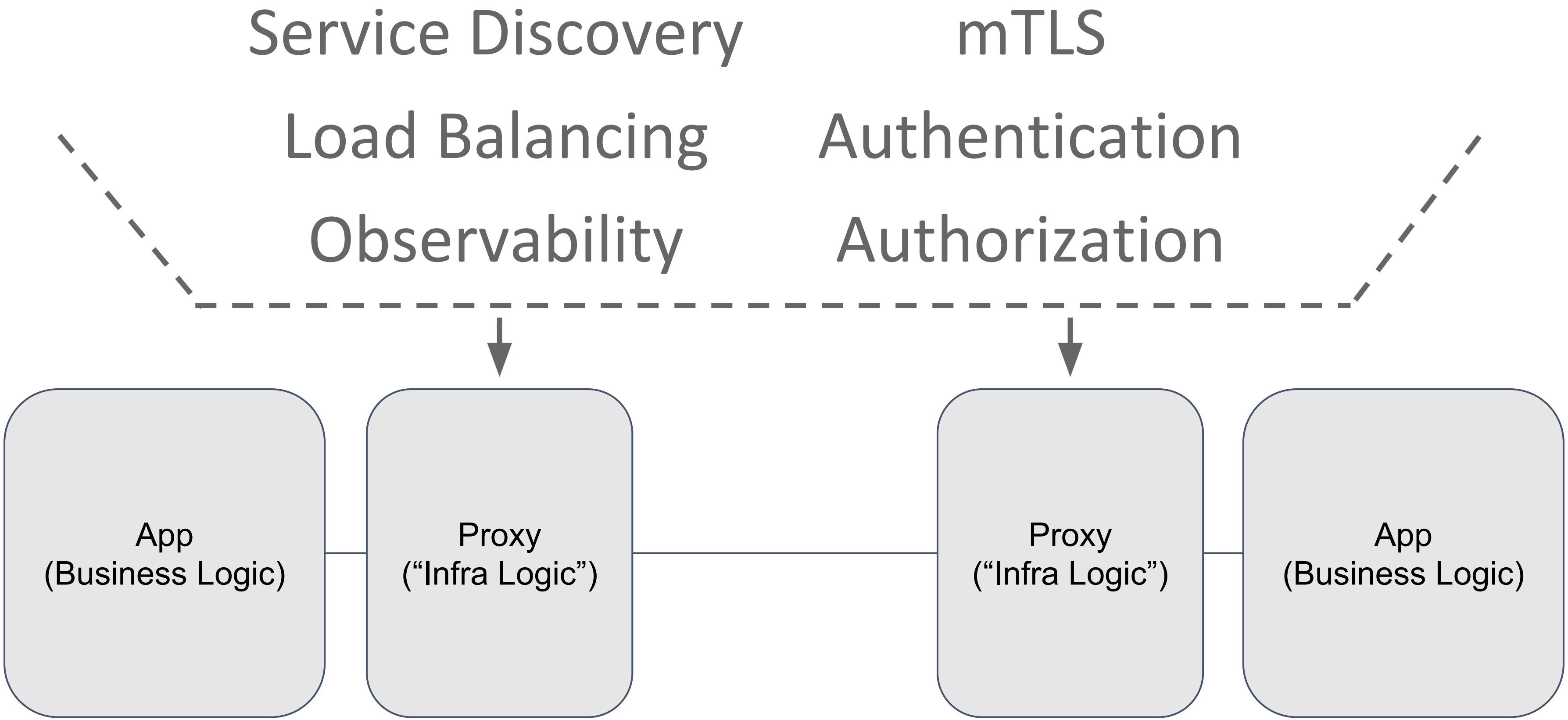
What is a Service Mesh?

An architectural pattern that provides common network services as a feature of the infrastructure

What is a Service Mesh?



What is a Service Mesh?



Service Discovery

Load Balancing

Observability

mTLS

Authentication

Authorization

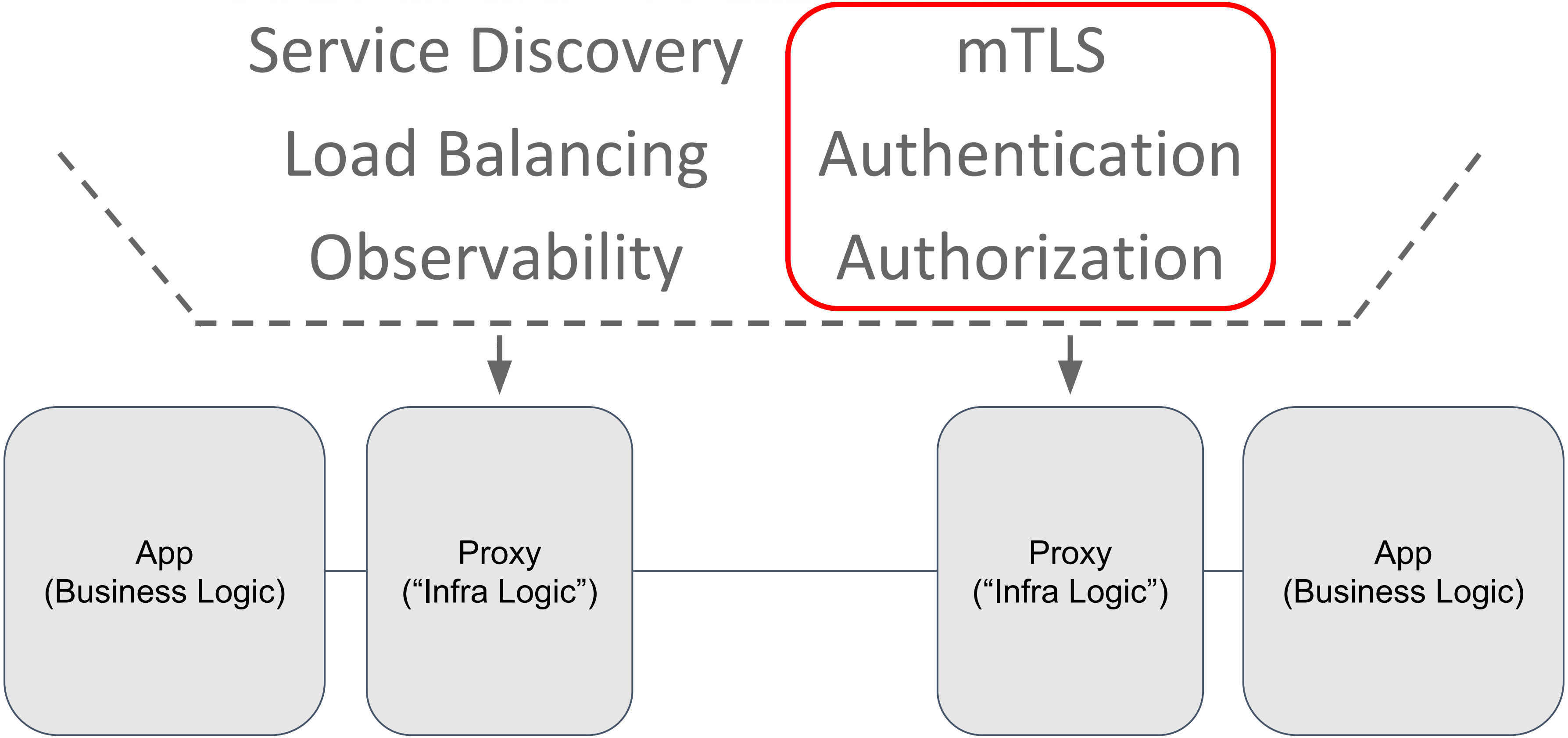
App
(Business Logic)

Proxy
(“Infra Logic”)

Proxy
(“Infra Logic”)

App
(Business Logic)

What is a Service Mesh?



Service Discovery

Load Balancing

Observability

mTLS

Authentication

Authorization

App
(Business Logic)

Proxy
(“Infra Logic”)

Proxy
(“Infra Logic”)

App
(Business Logic)

SPIFFE Identity

SPIFFE Identity

spiffe://cluster-1/my-special-workload

SPIFFE Identity

spiffe://cluster-1/my-special-workload

X509-SVID

SPIFFE Identity

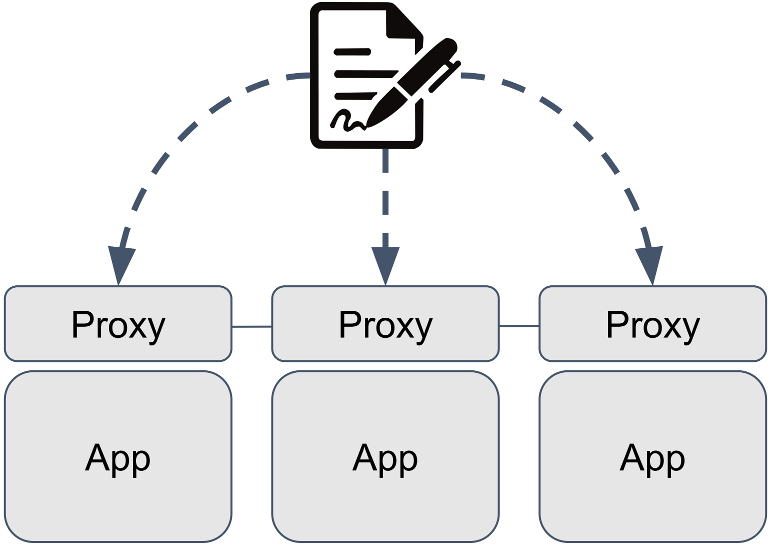
spiffe://cluster-1/my-special-workload

X509-SVID

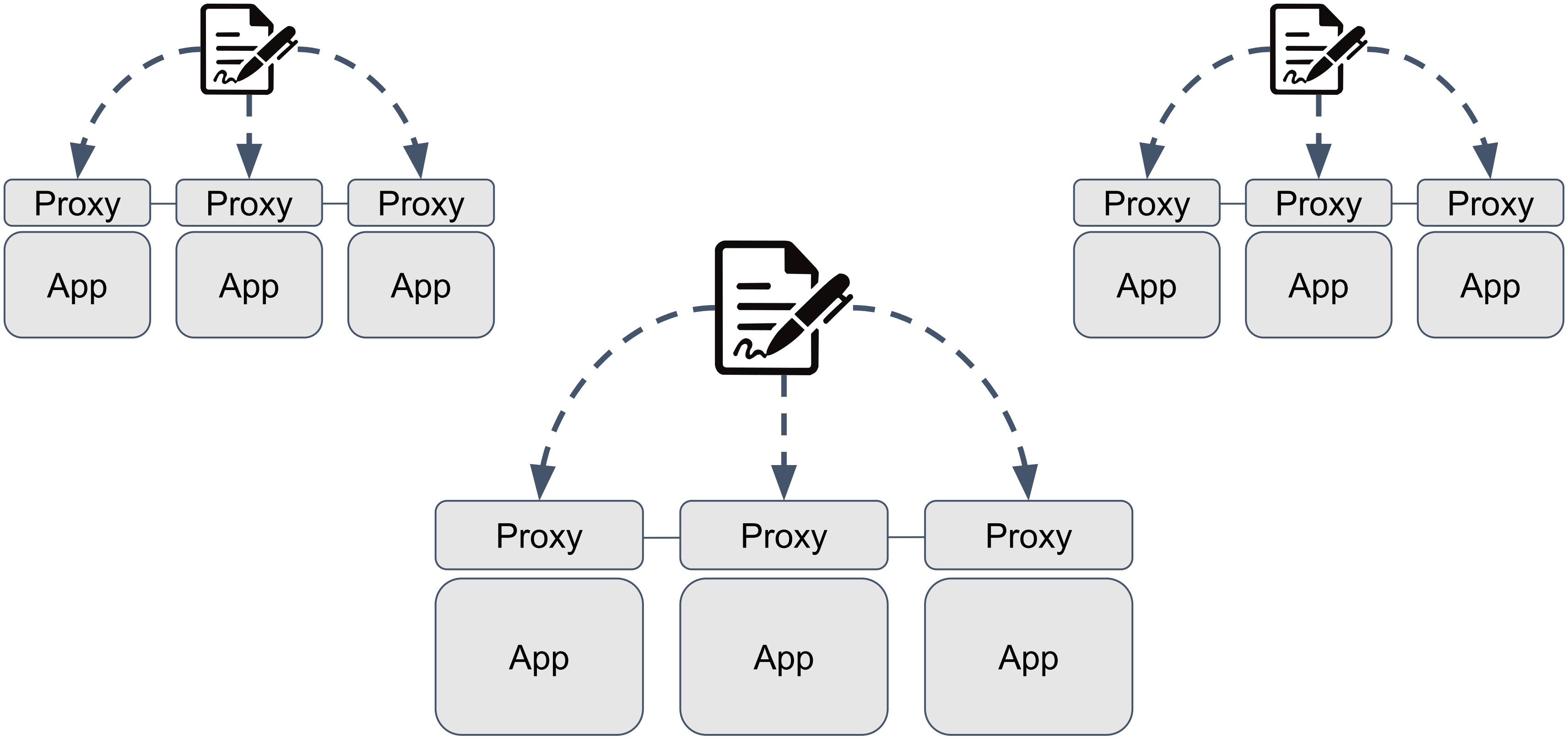
Identity in a Service Mesh

Central Authority

Common to All



Identity in a Service Mesh



Hybrid and Multi-Mesh Security Challenges

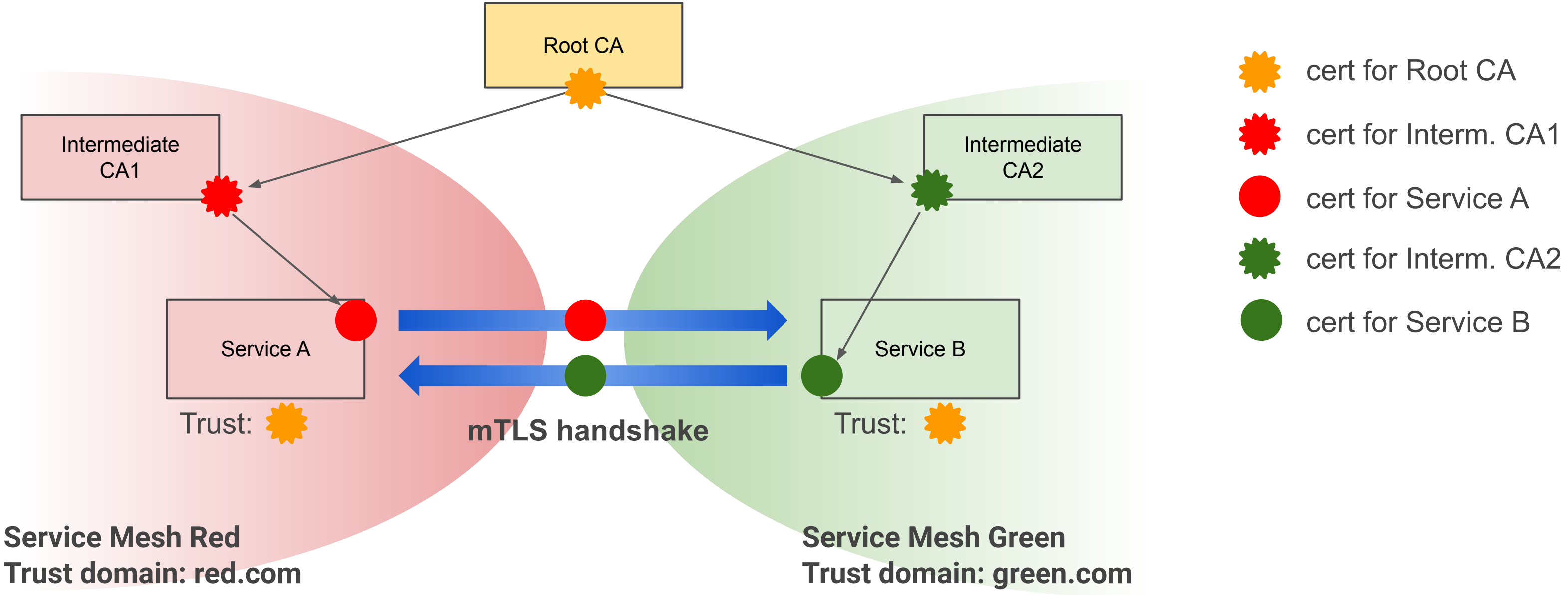
Hybrid and multi-mesh examples

- Two organizations, each owning a service mesh, want to expose selected services between each other
- A service provider exposes its services to the tenant services
- When partially migrating existing services to a new service mesh framework, the services in both service meshes need to talk to each other as before
- ...

Basic rules from the security lens

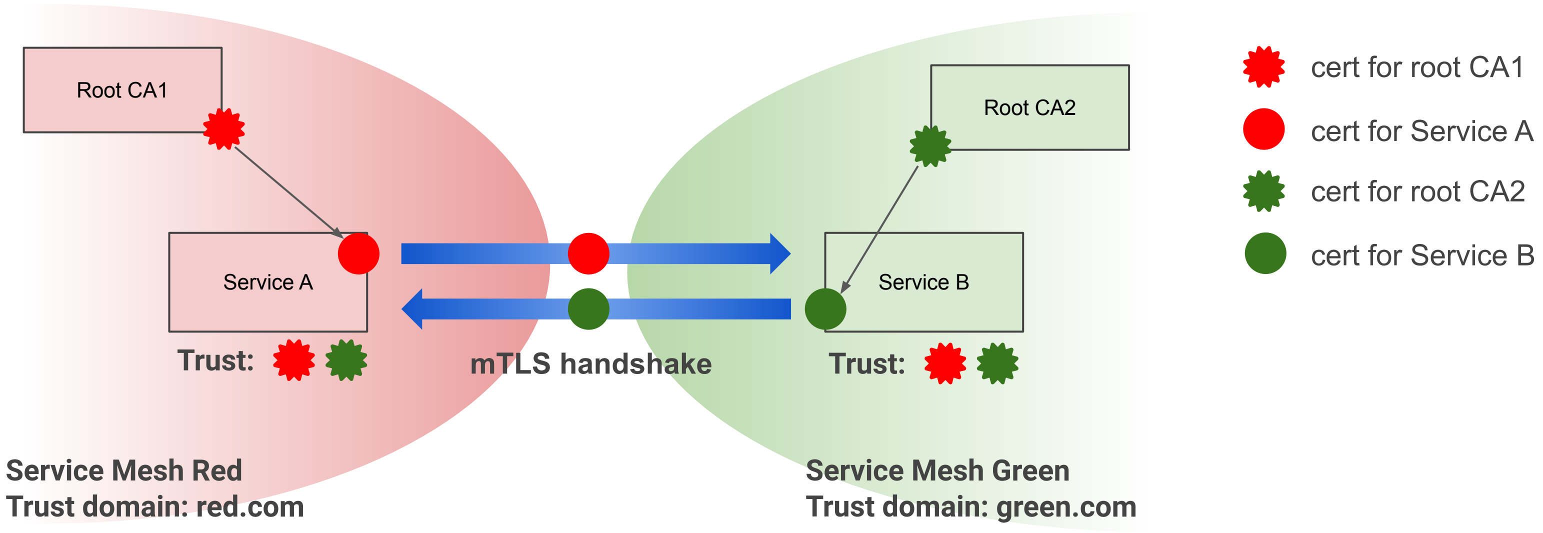
- All identities must be derived from trusted roots
  - Impersonation by untrusted PKI not possible
- Trust domain associated with parties/meshes
  - Cross-party impersonation not possible
- Transport + authn compatibility
  - Successful authentication between trusted services
- Security policies explicitly enforce external access control
  - Deny by default for calls from external meshes

Limitations of shared authority



- Independent parties not likely to share common root CA
- Name constraints on intermediate CAs are required

Multiple Independent Authorities



- How do meshes securely exchange roots of trust?
- How to prevent Root CA2 from issuing identities for Mesh Red (and vise versa)?

SPIFFE Federation

SPIFFE Federation API

“API” for Exchanging Authority Public Keys

Simple HTTPS GET + JWKS

a la OIDC `jwks_uri`

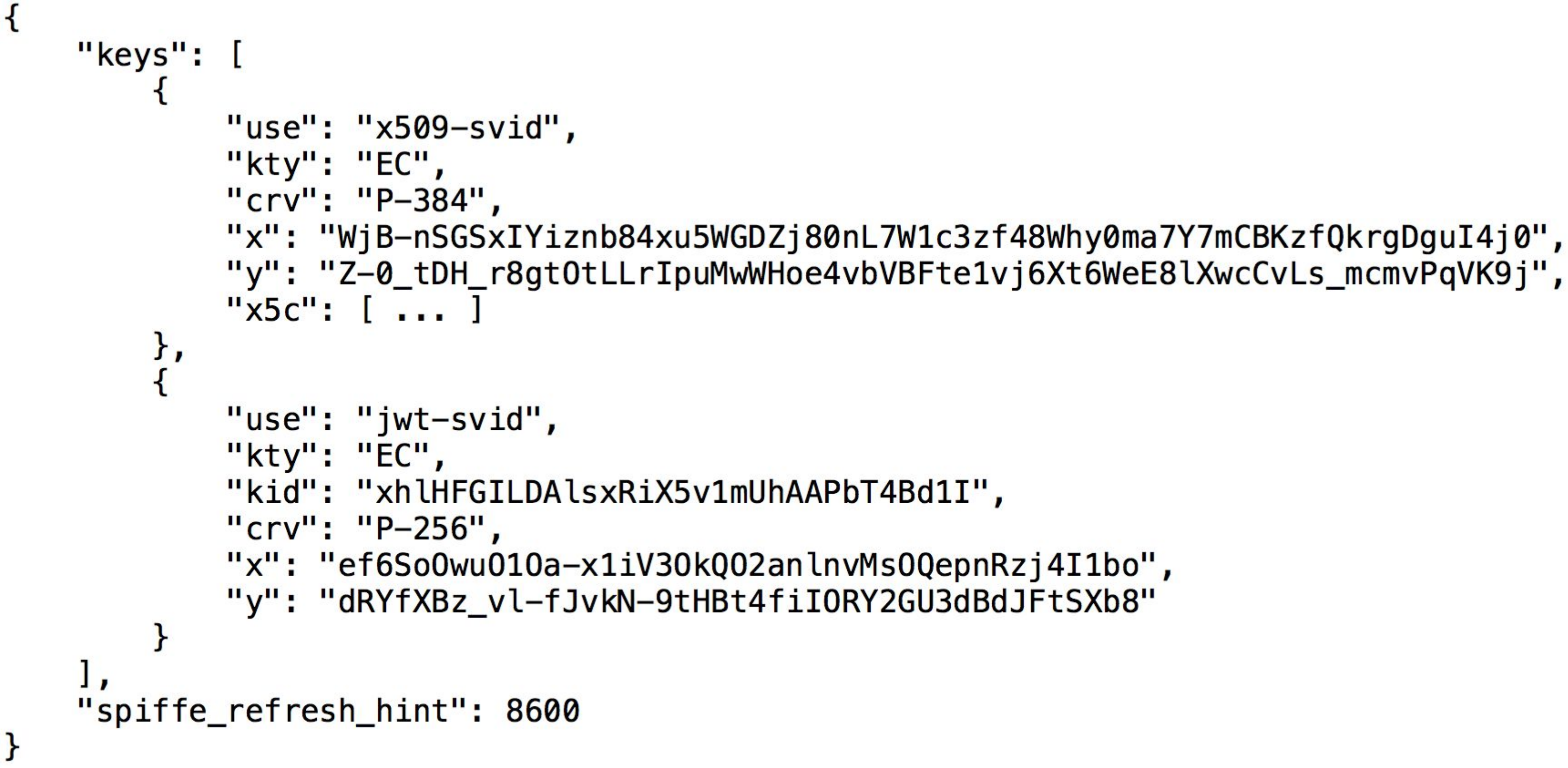
SPIFFE Federation API

“API” for Exchanging Authority Public Keys

Simple HTTPS GET + JWKS

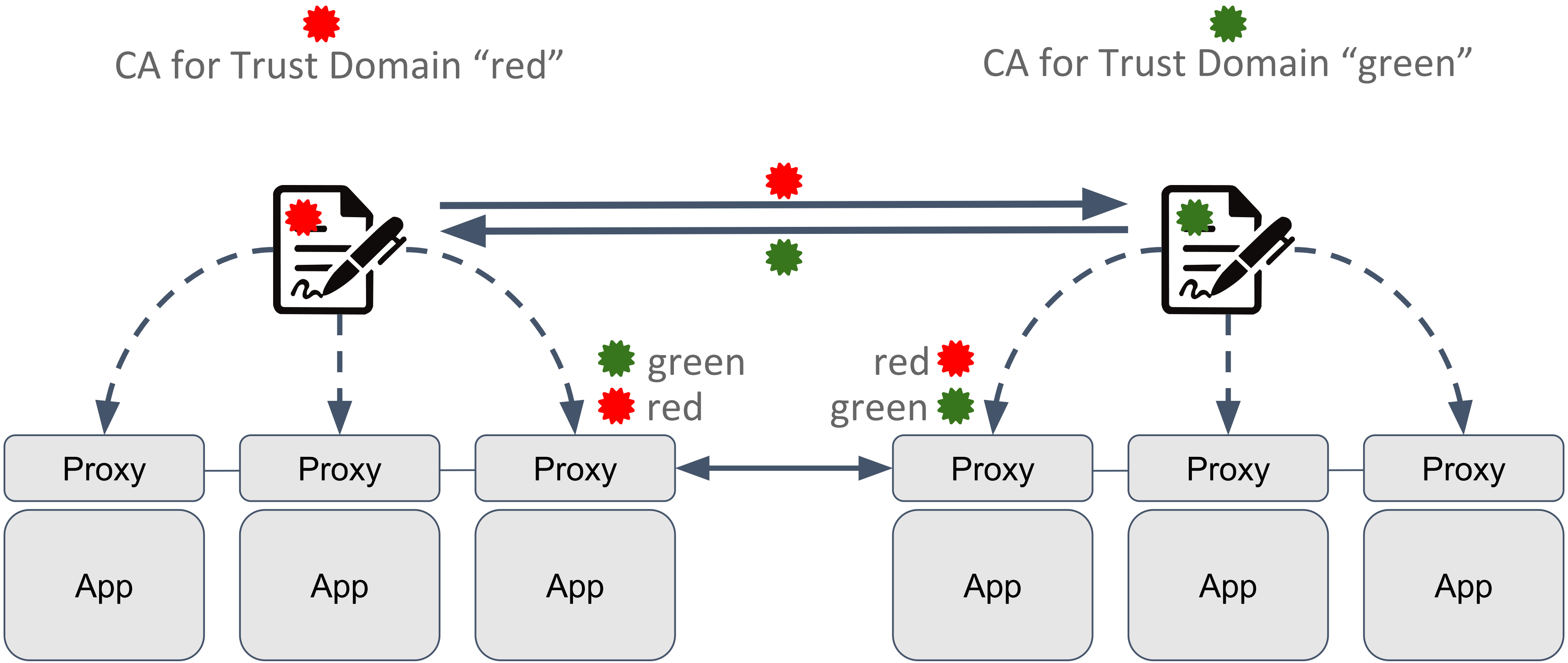
a la OIDC `jwks_uri`

SPIFFE Federation API

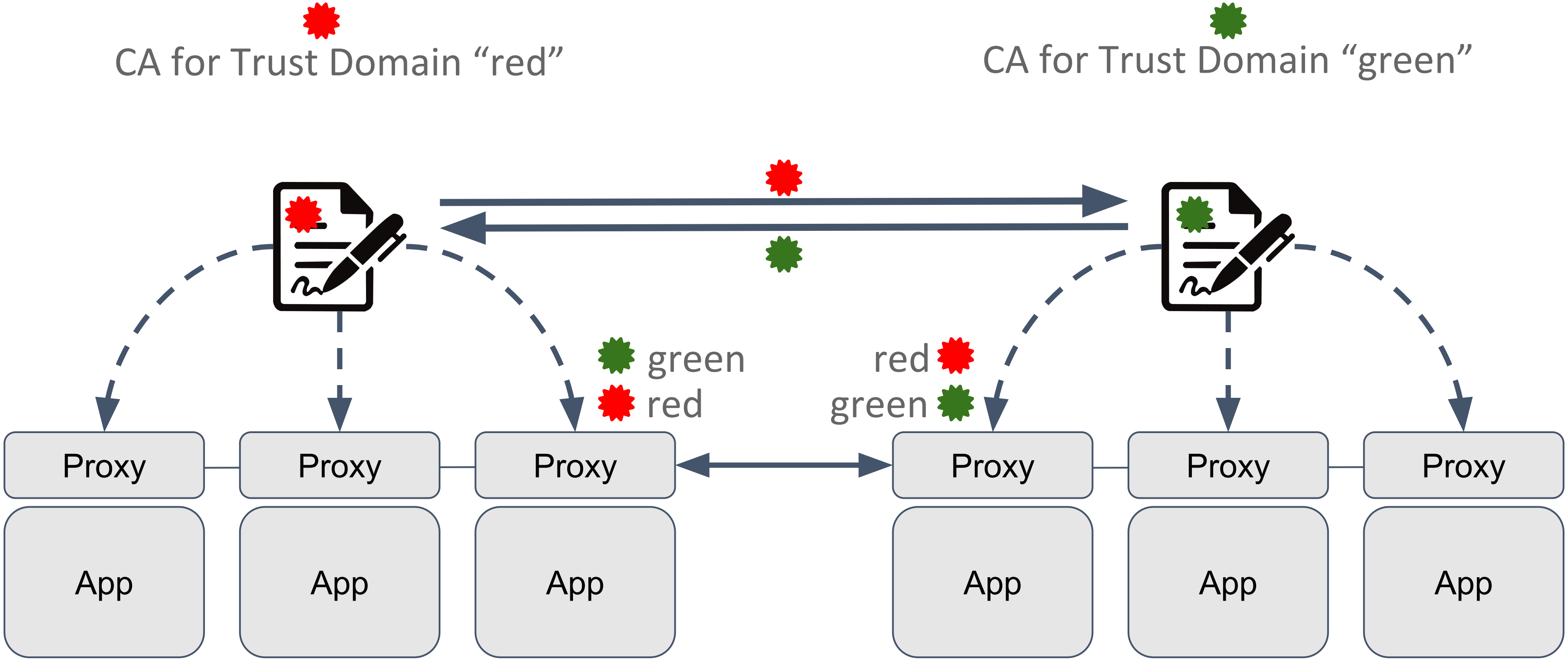


```
{
    "keys": [
        {
            "use": "x509-svid",
            "kty": "EC",
            "crv": "P-384",
            "x": "WjB-nSGSxIYiznb84xu5WGDZj80nL7W1c3zf48Why0ma7Y7mCBKzfQkrgDguI4j0",
            "y": "Z-0_tDH_r8gtOtLLrIpuMwWHoe4vbVBFte1vj6Xt6WeE8lXwcCvLs_mcmvPqVK9j",
            "x5c": [ ... ]
        },
        {
            "use": "jwt-svid",
            "kty": "EC",
            "kid": "xhlHFGILDAlsxRiX5v1mUhAAPbT4Bd1I",
            "crv": "P-256",
            "x": "ef6SoOwuO1Oa-x1iV3OkQO2anlnvMsOQepnRzj4I1bo",
            "y": "dRYfXBz_vl-fJvkN-9tHBt4fiIORY2GU3dBdJFtSXb8"
        }
    ],
    "spiffe_refresh_hint": 8600
}
```

SPIFFE Federation: An Example

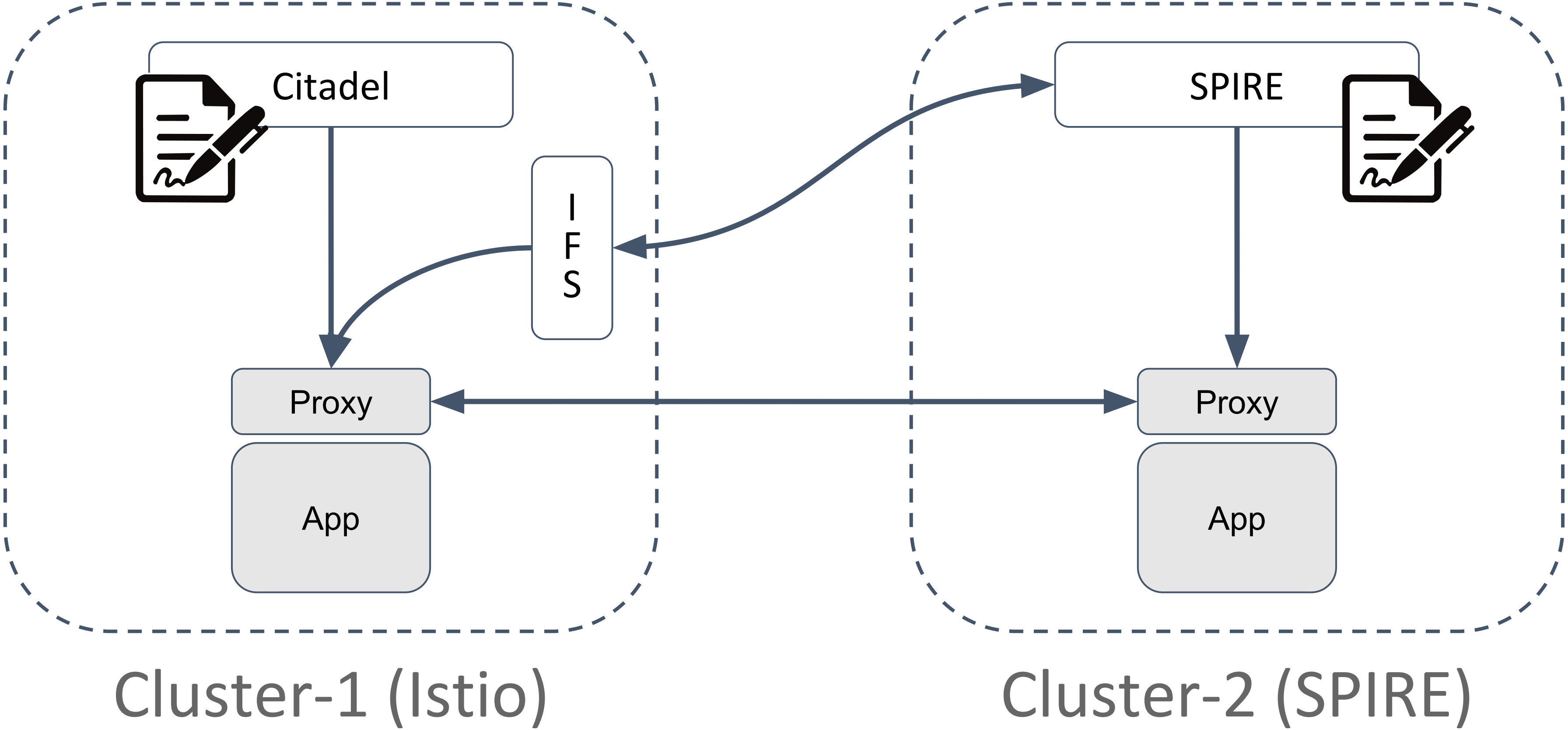


SPIFFE Federation: An Example

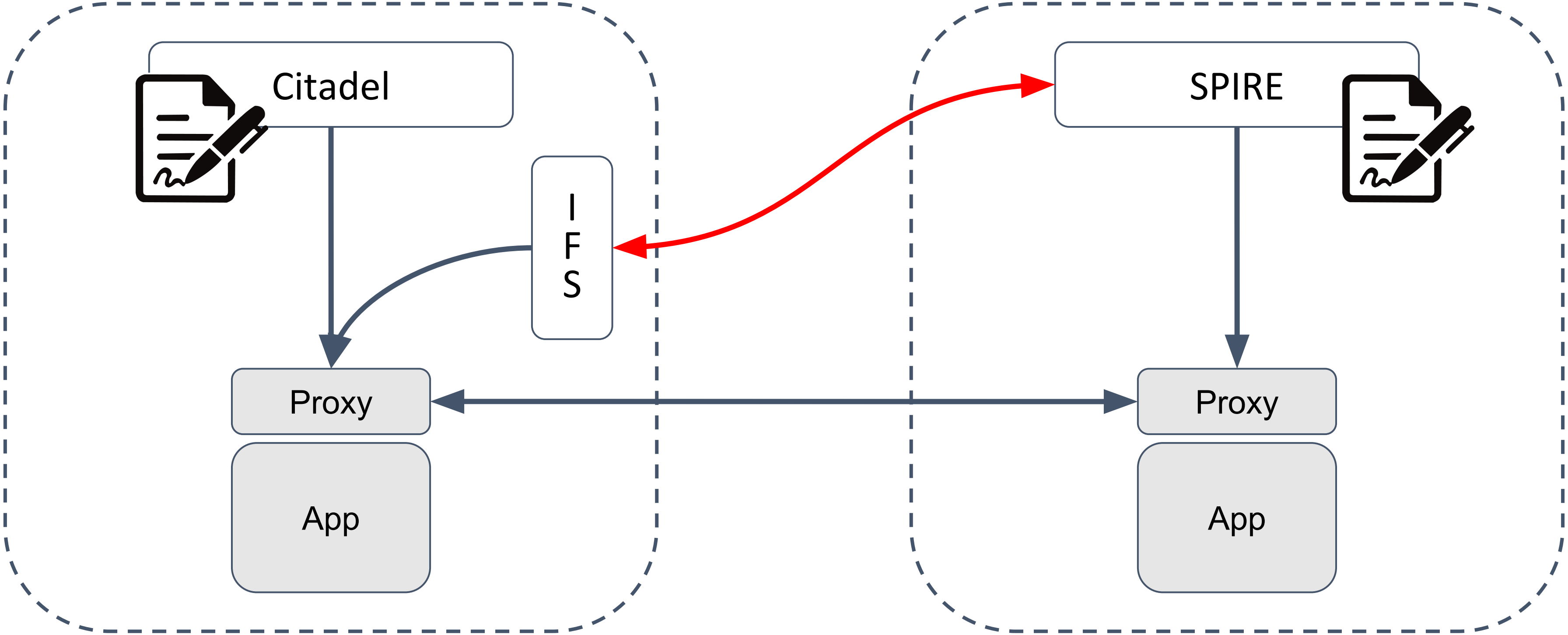


Istio and SPIRE

Federation Demo Architecture



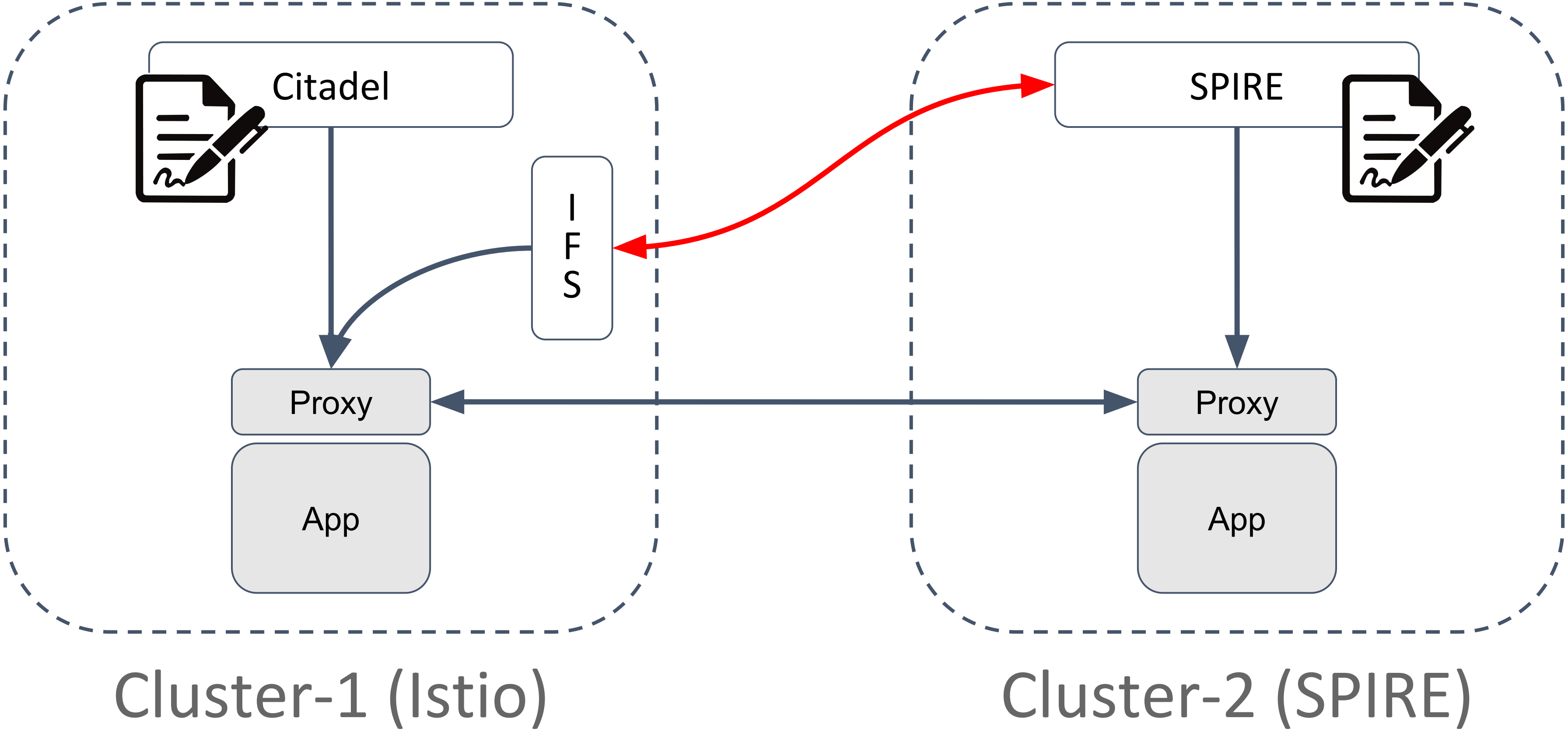
Federation Demo Architecture



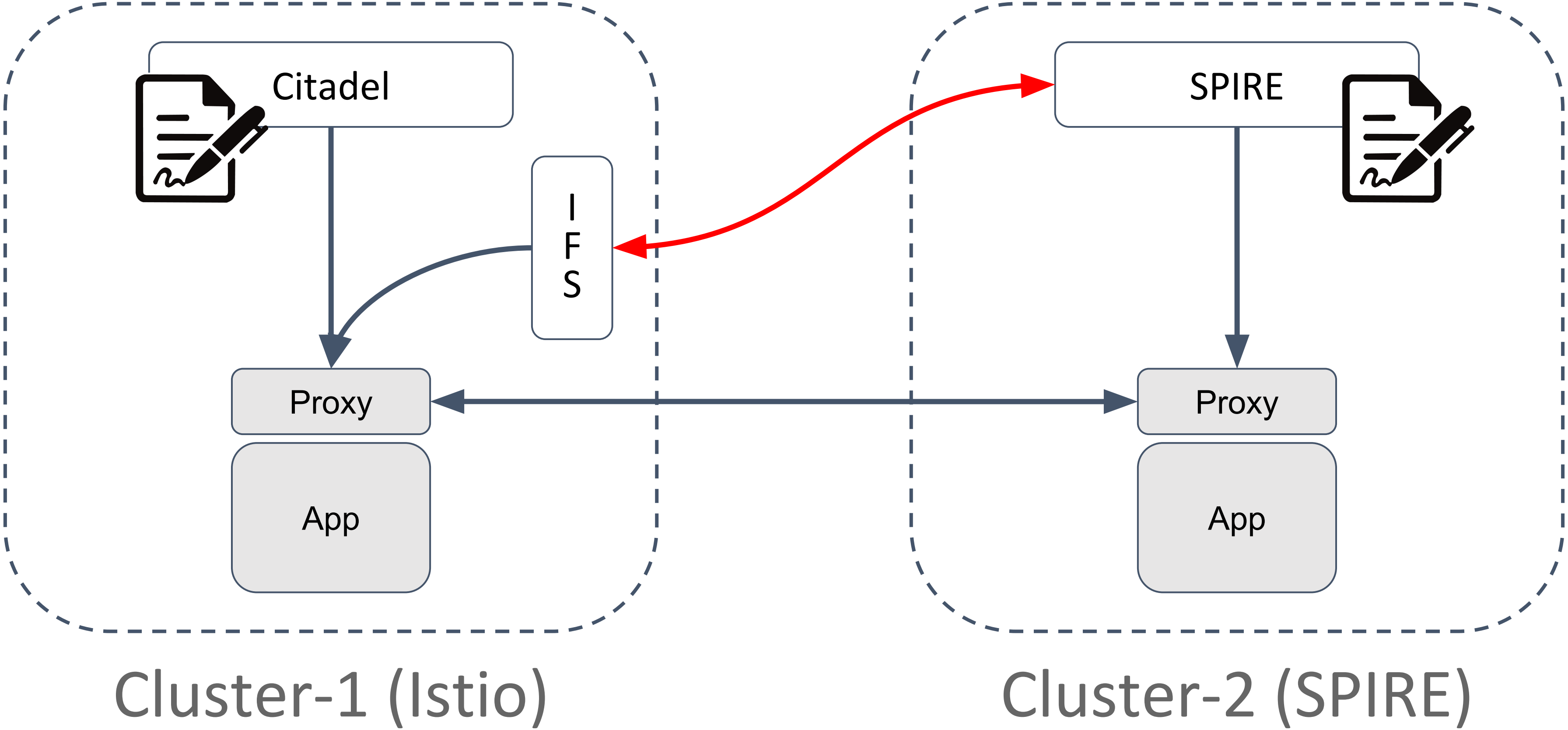
Cluster-1 (Istio)

Cluster-2 (SPIRE)

Federation Demo Architecture

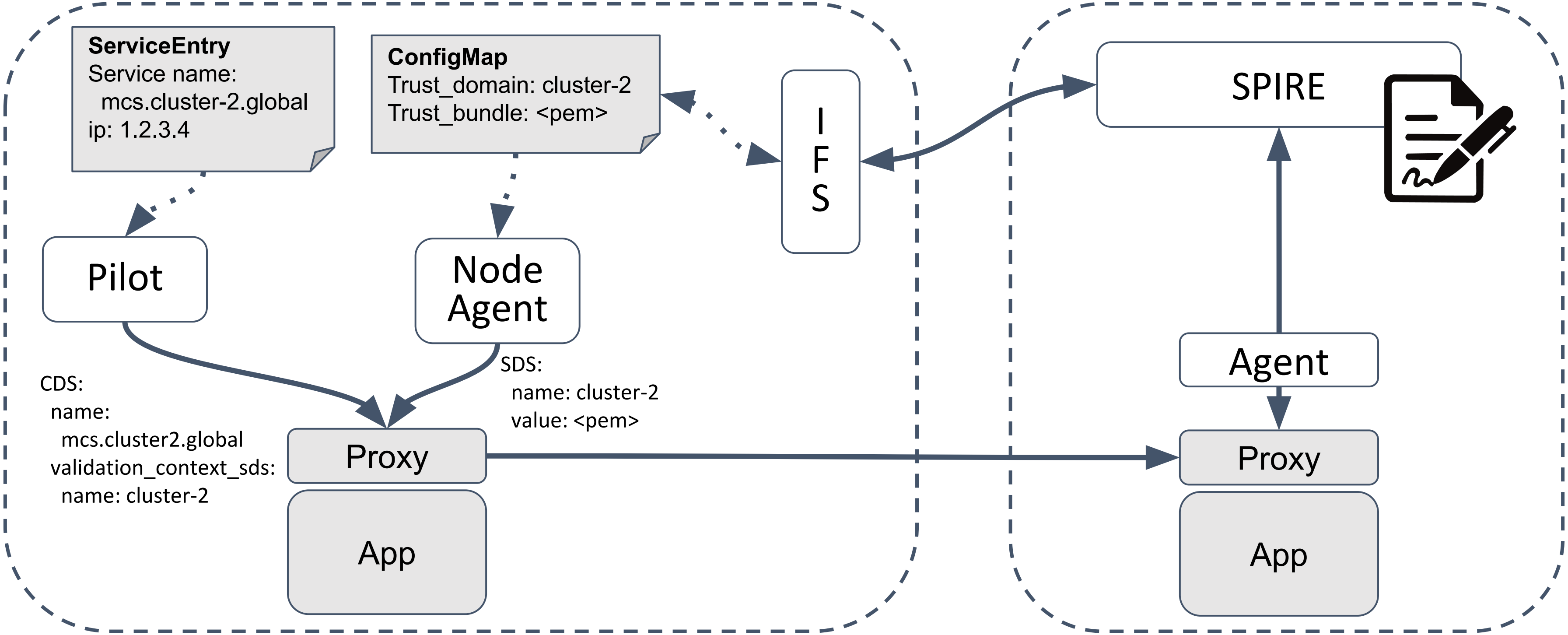


Federation Demo Architecture



Demo Time!

Full Disclosure



Cluster-1 (Istio)

Cluster-2 (SPIRE)

Learn More

istio/istio

spiffe/spire

istio.slack.com

slack.spiffe.io

evan2645/istio-federation-server

evan2645/kubecon-2019-federation-demo

KubeCon | CloudNativeCon

North America 2019

Fundamentals for multi-mesh solutions

- Network
  - Through ingress/egress
  - Flat network
- Service discovery
  - KubeDNS / CoreDNS / Global DNS for DNS
  - Define service entries for external service routing
- Security
  - No conflicts of identities across different meshes
  - Roots of trust are shared across meshes
  - Authorization policies involve external identities