tetrate

POWERING THE WORLD'S APPLICATION NETWORKS

Ignasi Barrera

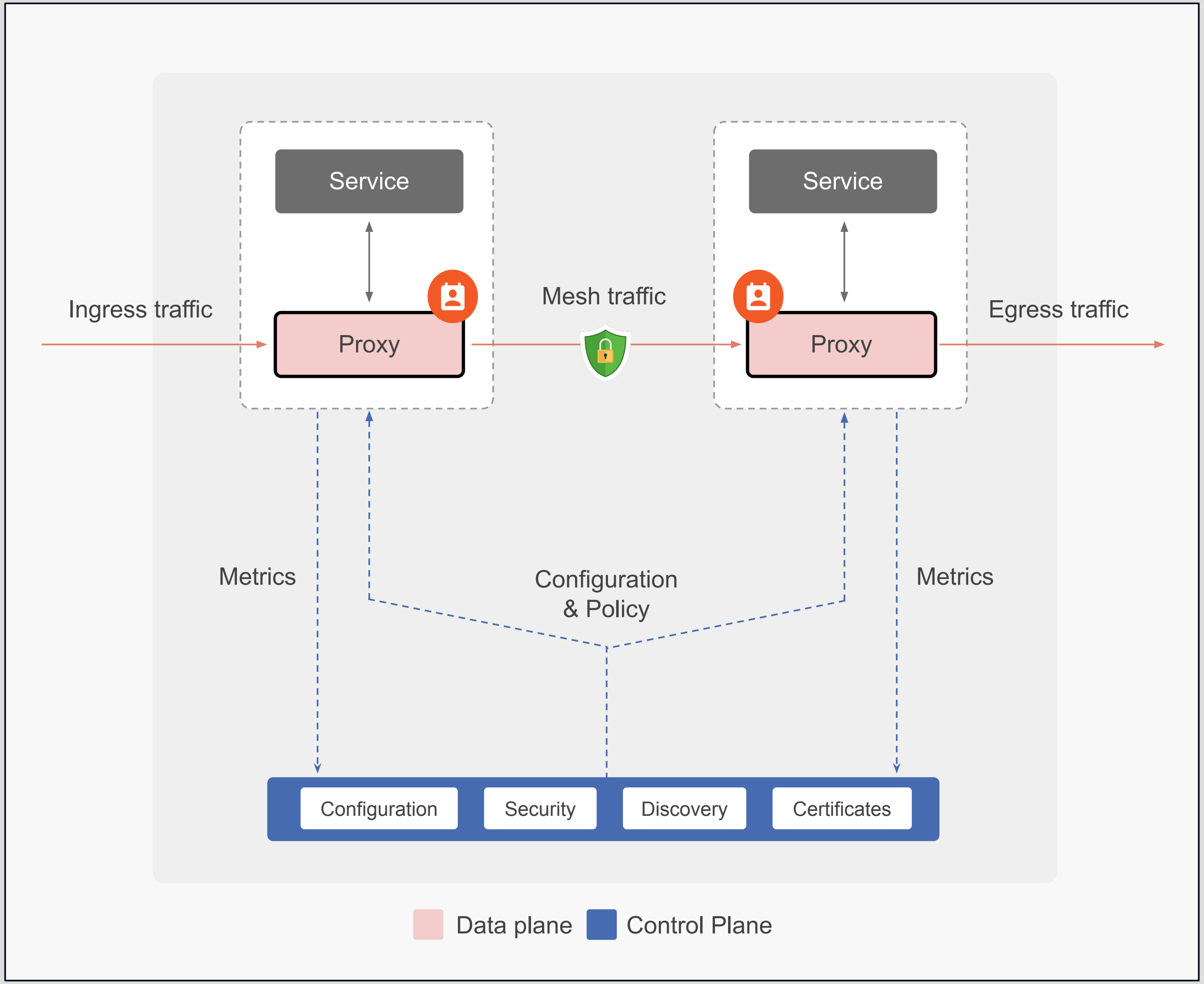
Founding Engineer

DevSecOps and Zero Trust Architecture (ZTA) for Multi-Cloud Environments
January 2021

Service Mesh

Offload network and authn/authz functionality to the sidecars

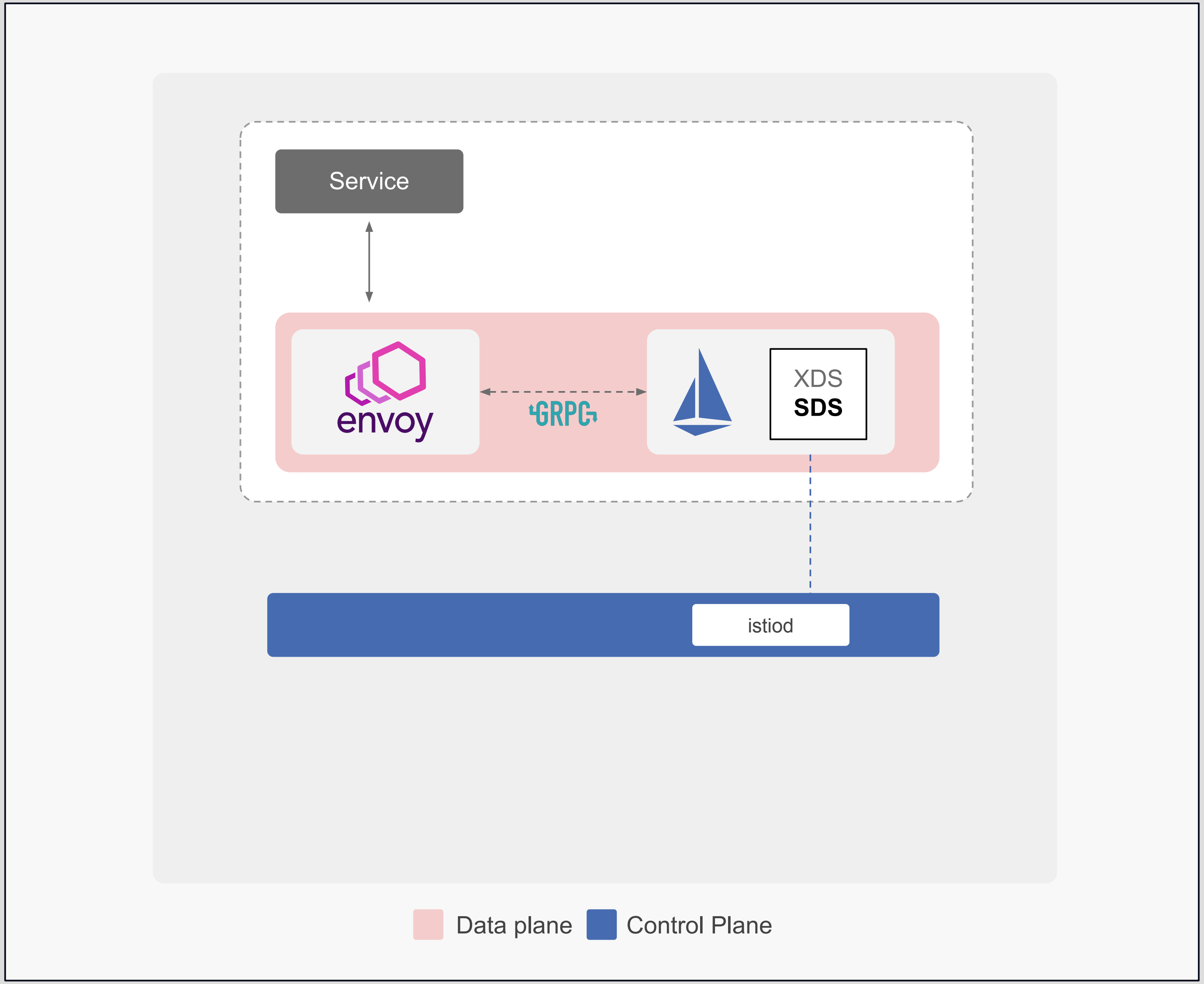
No application changes required !



Inside the sidecar

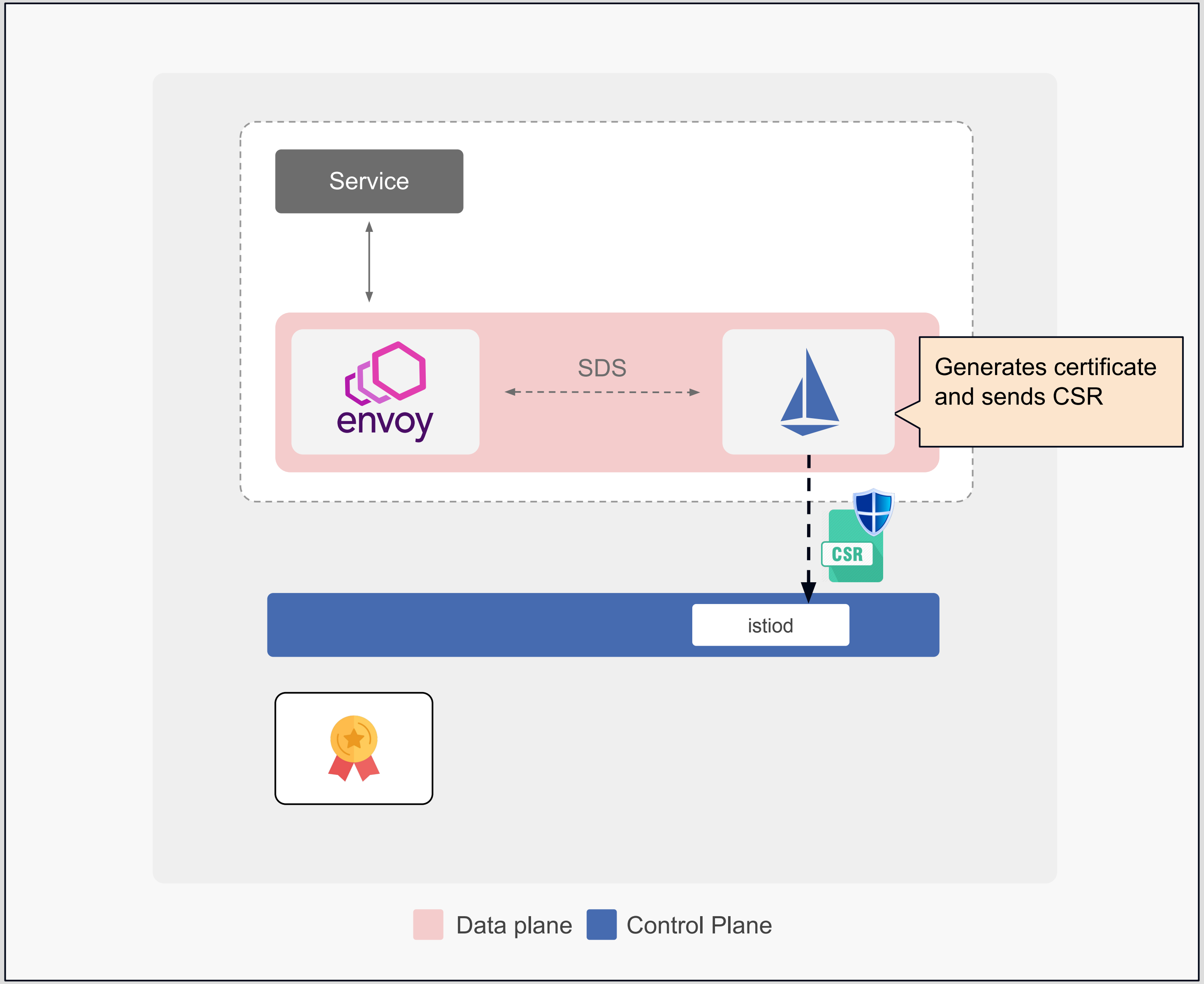
The sidecar container runs two processes:

- The Envoy proxy
- The istio-agent



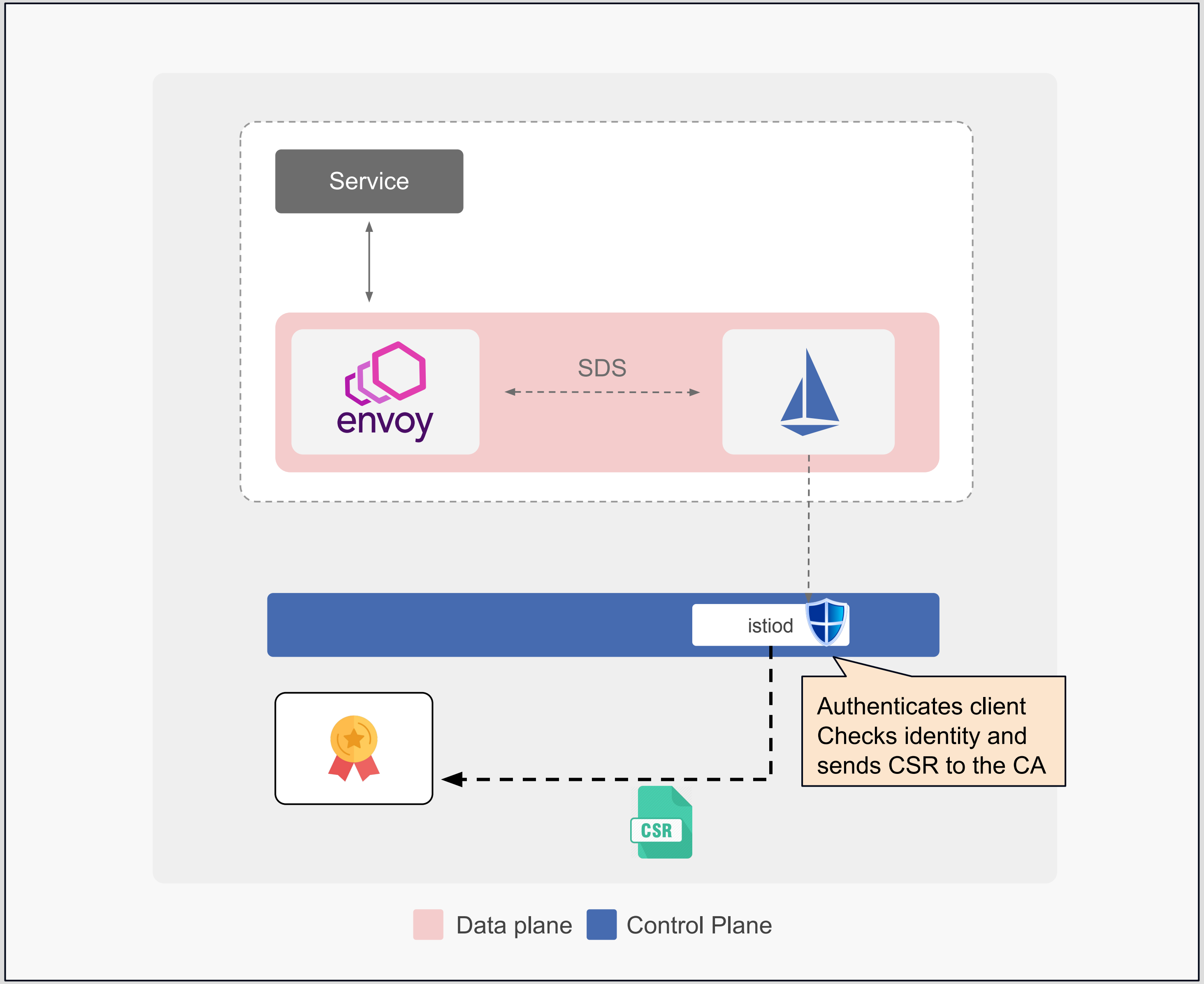
Identity flow

The agent generates an x.509 certificate with the SPIFFE identity, a private key, and sends a CSR for signing



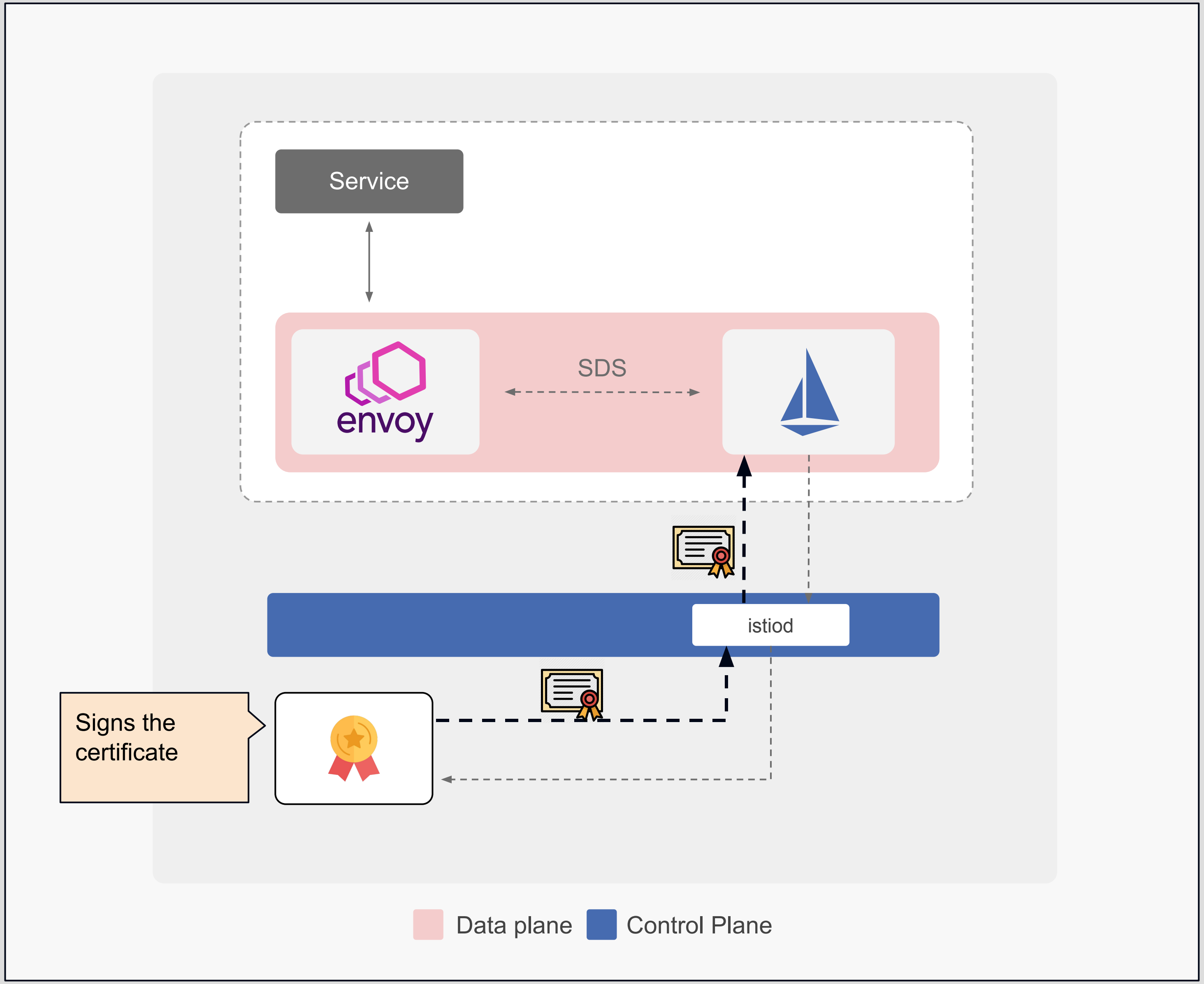
istiod as a Registration Authority

istiod validates the certificate and authenticates the client making the request, then forwards the CSR to the CA to have it signed



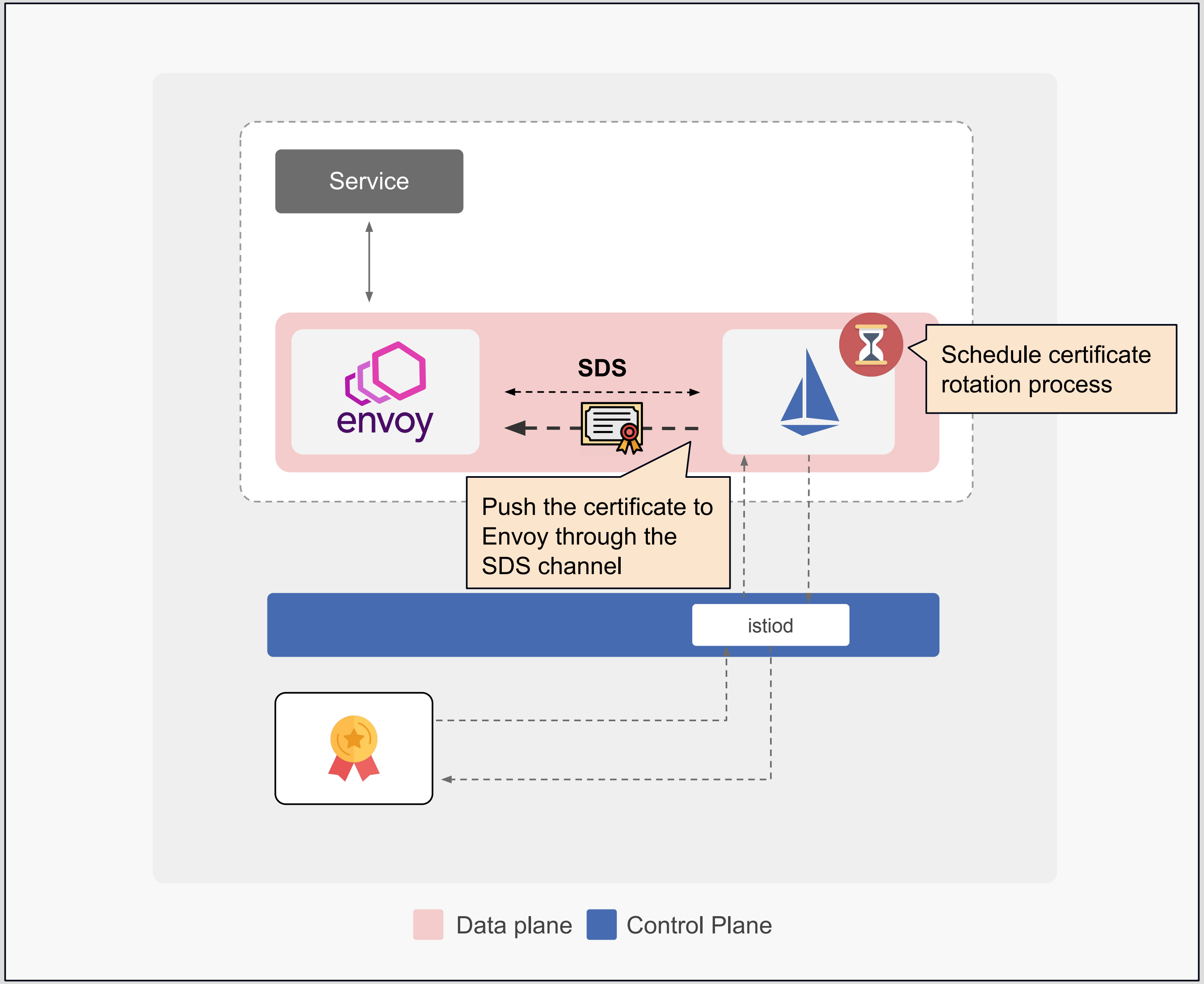
Certificate signing

The CA signs the certificate and returns it



Push certificate to the proxy

When the signed certificate is received, the agent pushes it to the proxy



Schedule certificate rotation process

Push the certificate to Envoy through the SDS channel

Demo time!

tetrate

Thank You

Contact

@tetrateio

Tetrate

www.tetrate.io

✉ For any further queries, feel free to contact us at info@tetrate.io