
CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Zero Trust Workload Identity in Kubernetes

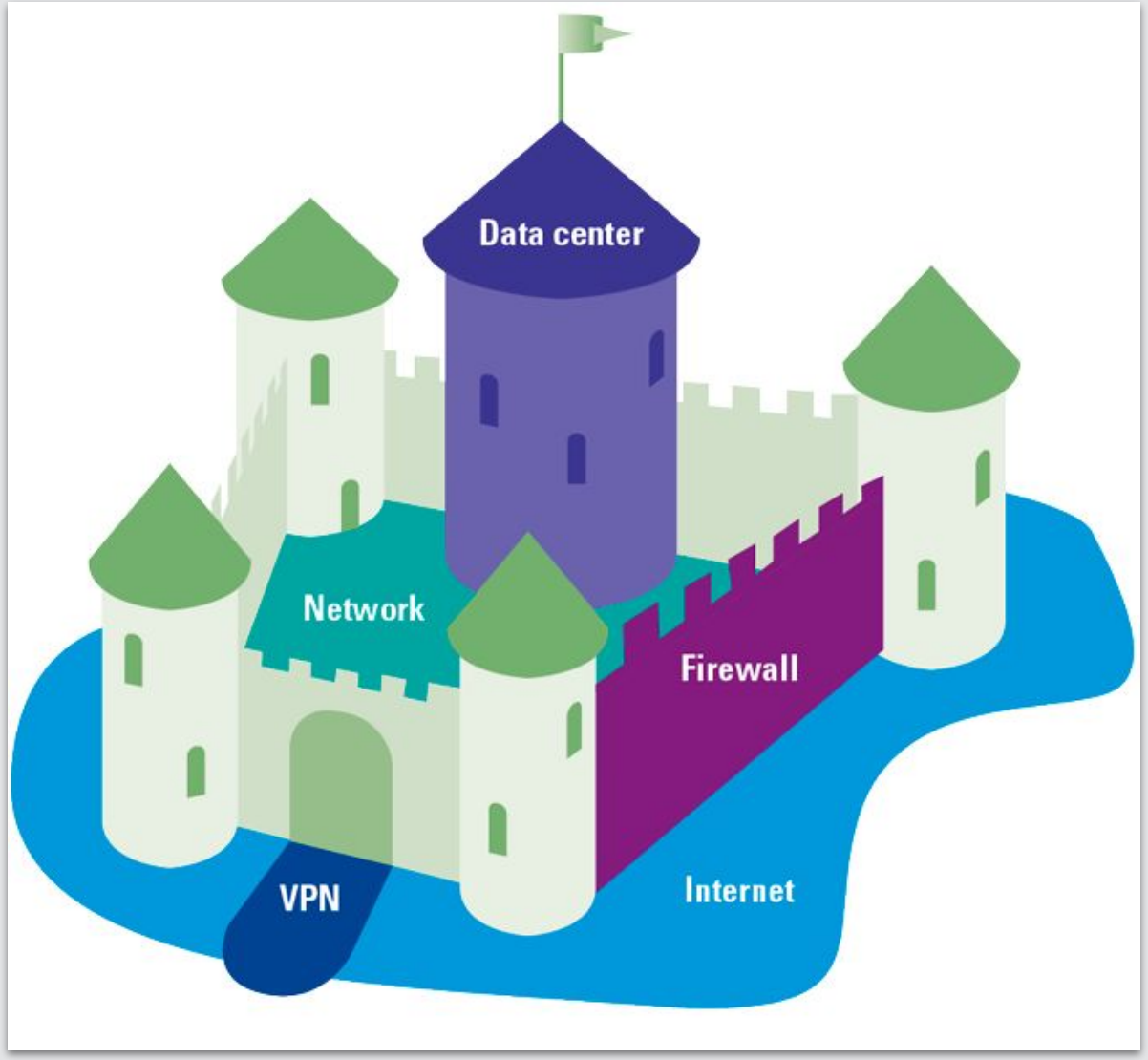
Michael Peters - Red Hat

Zero Trust?

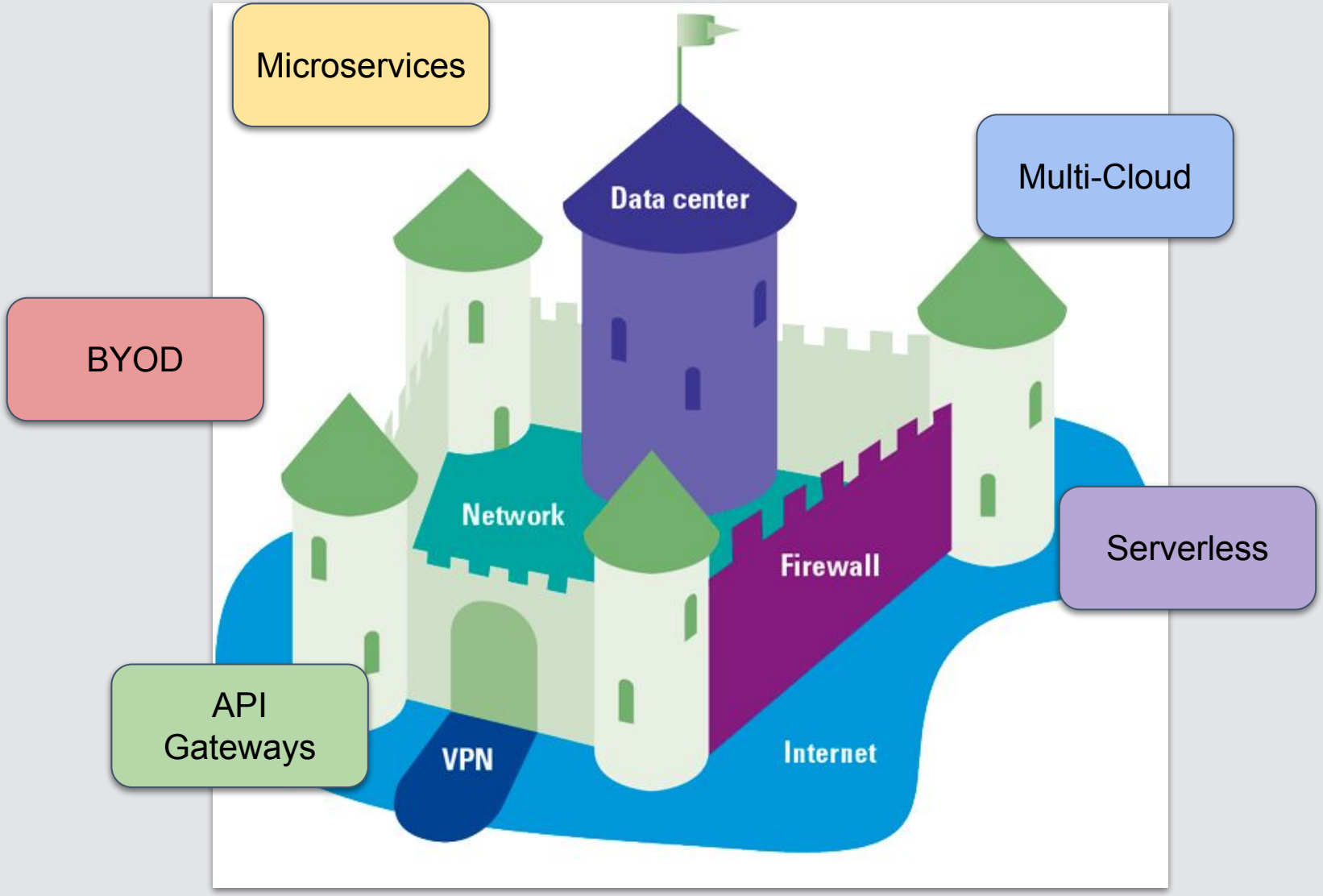
^ *Implicit*

- Architectural Pattern
- Security applied at the asset level
- Not the location (network)

Zero Trust?



Zero Trust?


Microservices
Multi-Cloud
BYOD
Serverless
API Gateways
Data center
Network
Firewall
VPN
Internet

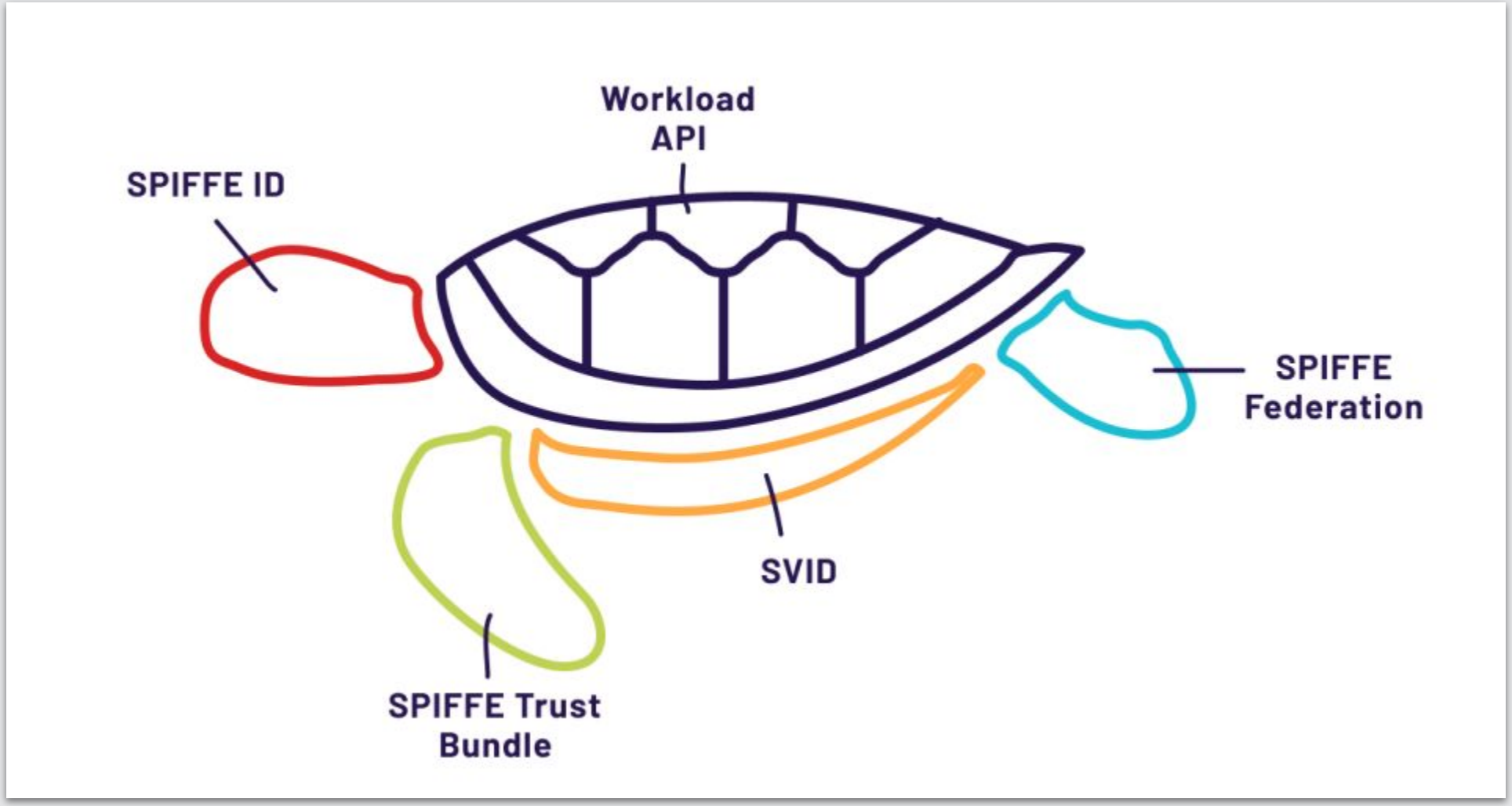
Zero Trust?

SPIFFE?

SPIFFE?

Root of Trust

SPIFFE?


Workload API
SPIFFE ID
SPIFFE Federation
SVID
SPIFFE Trust Bundle

SPIFFE ID?

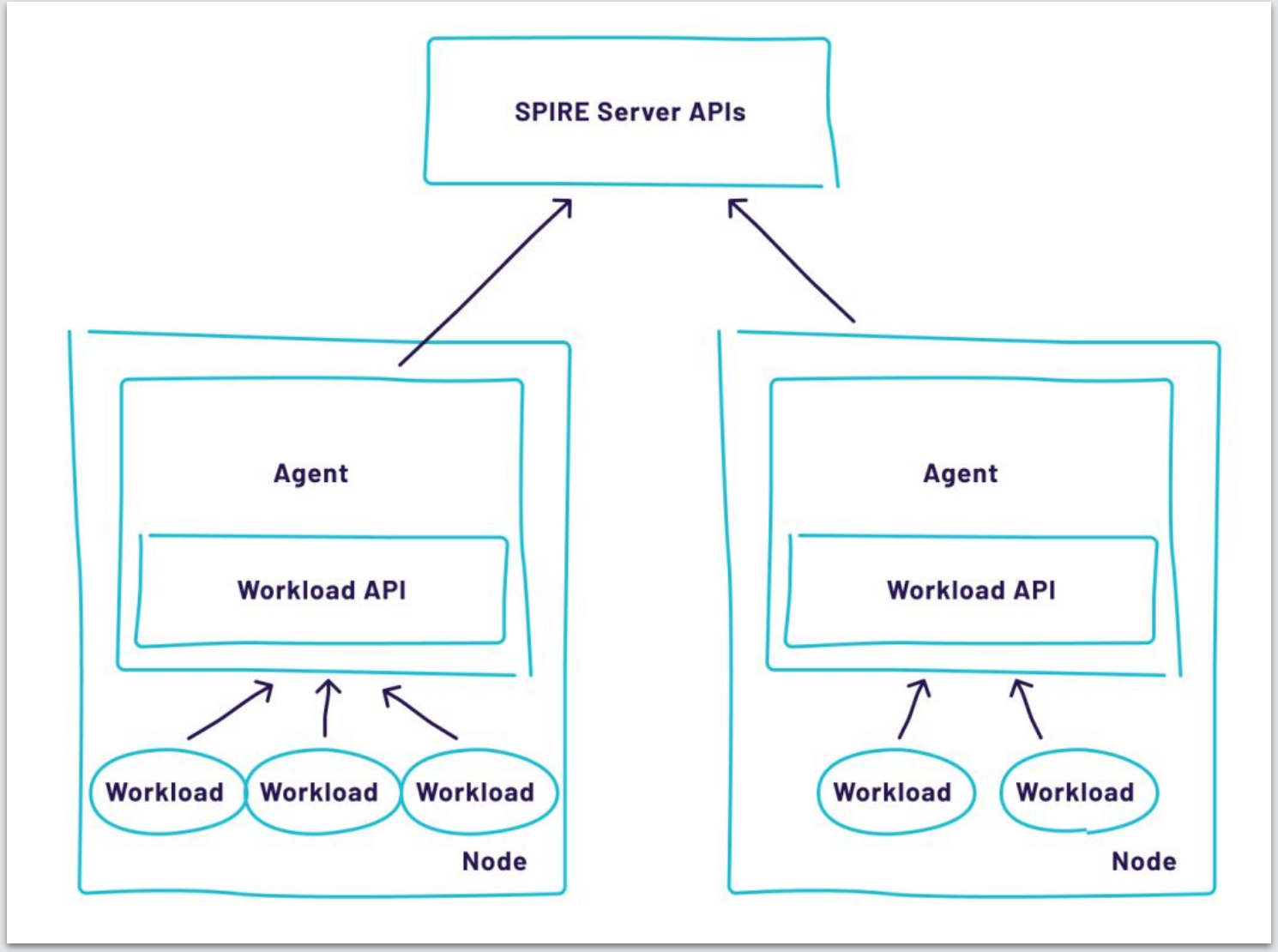
spiffe://example.com/bizops/hr/taxrun/withholding

SPIFFE ID?

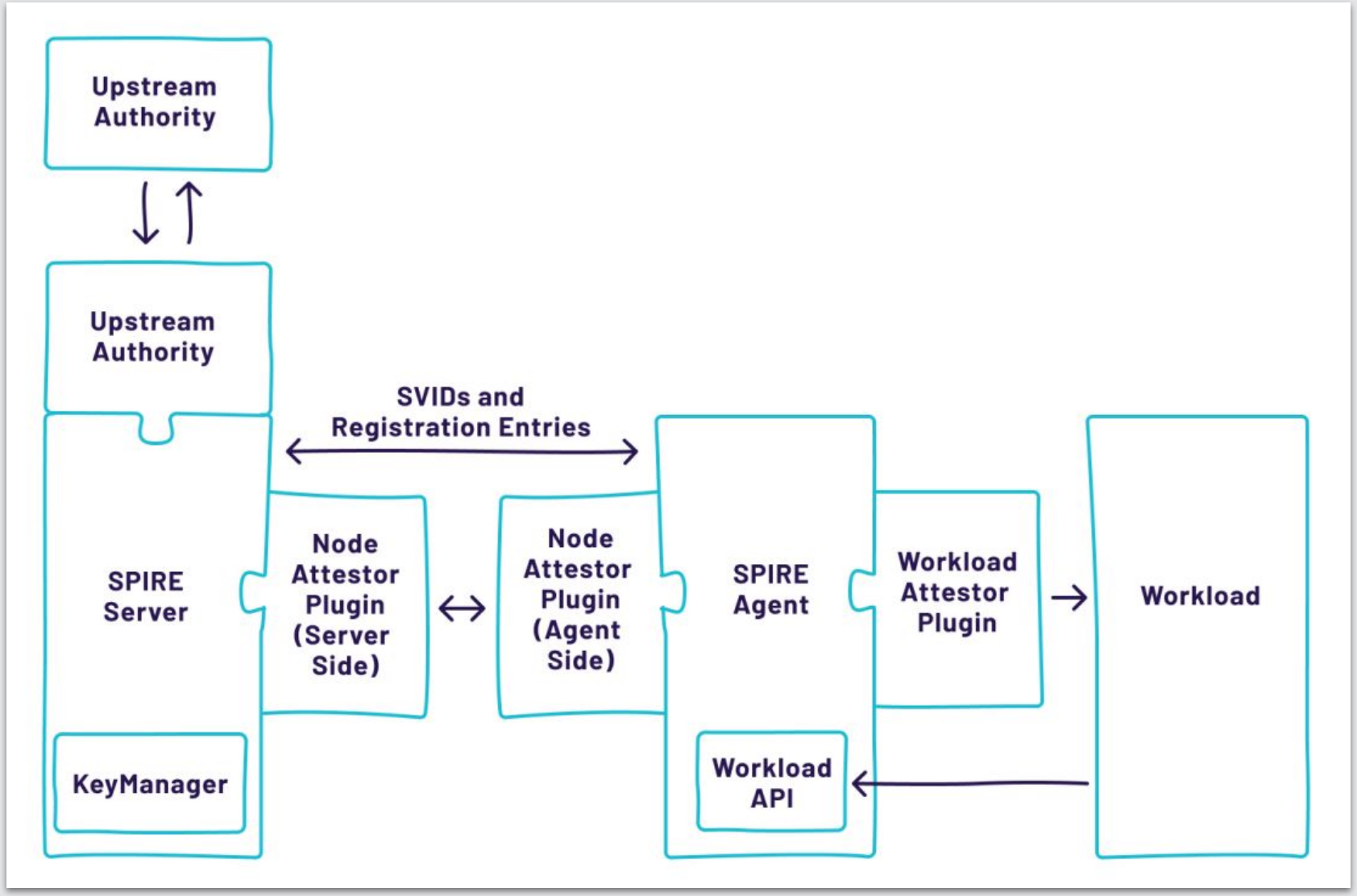
spiffe://{cluster-name}/ns/{ns}/sa/{service-account}

SPIRE?

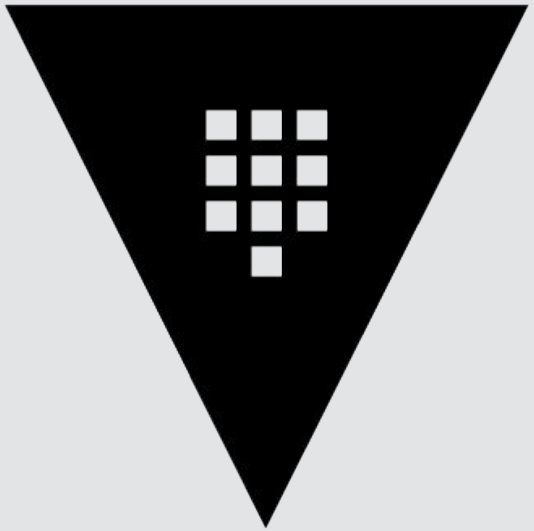
SPIRE?



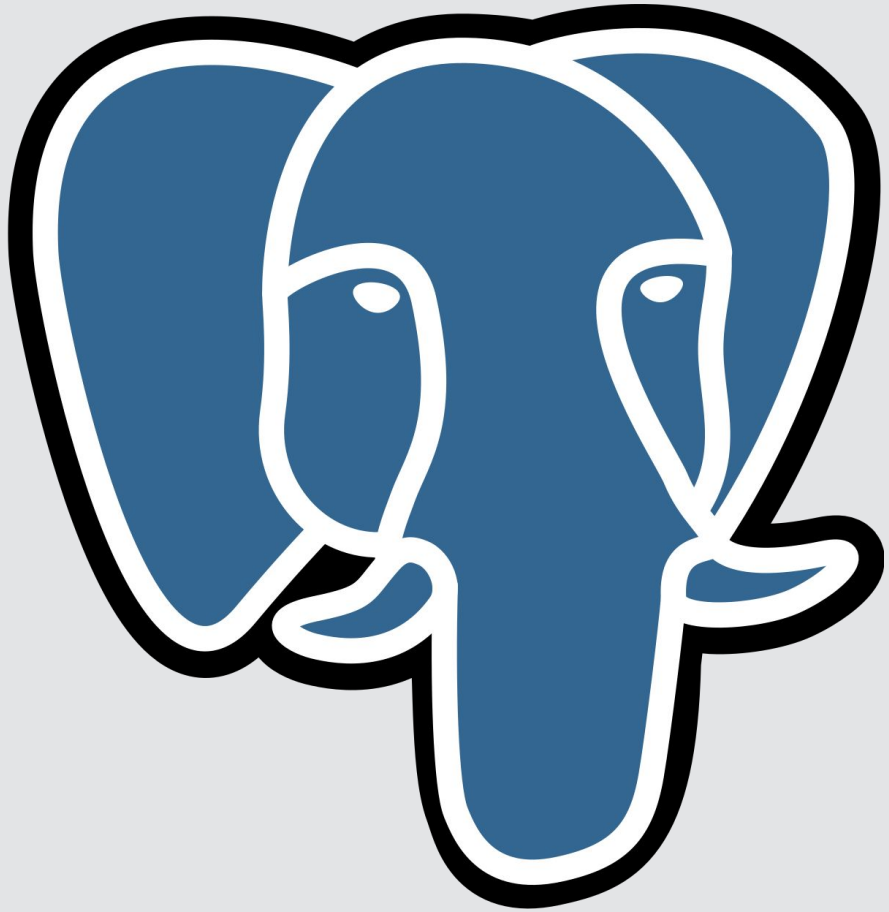
SPIRE?



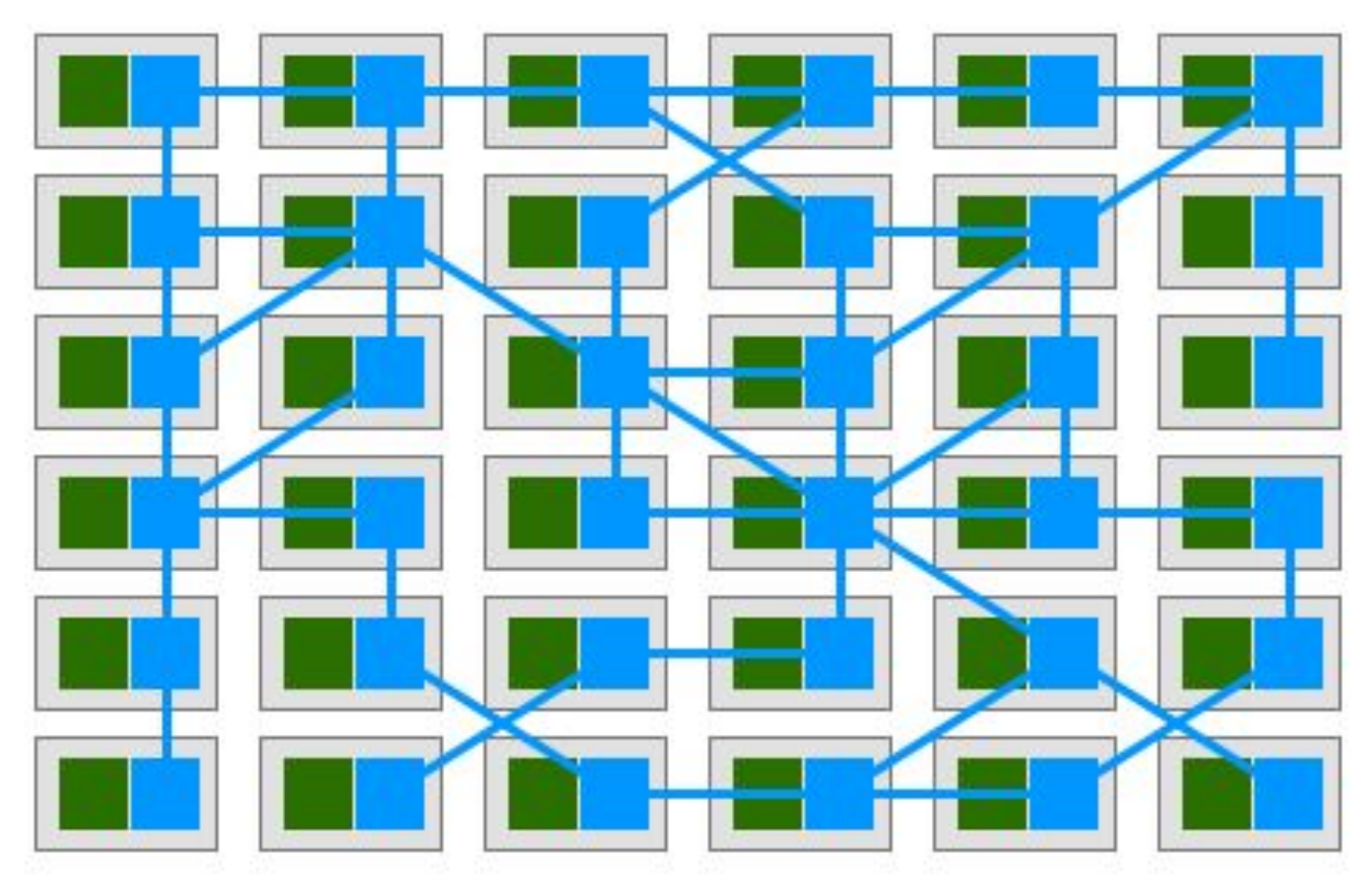
SPIFFE + Vault



SPIFFE + Databases

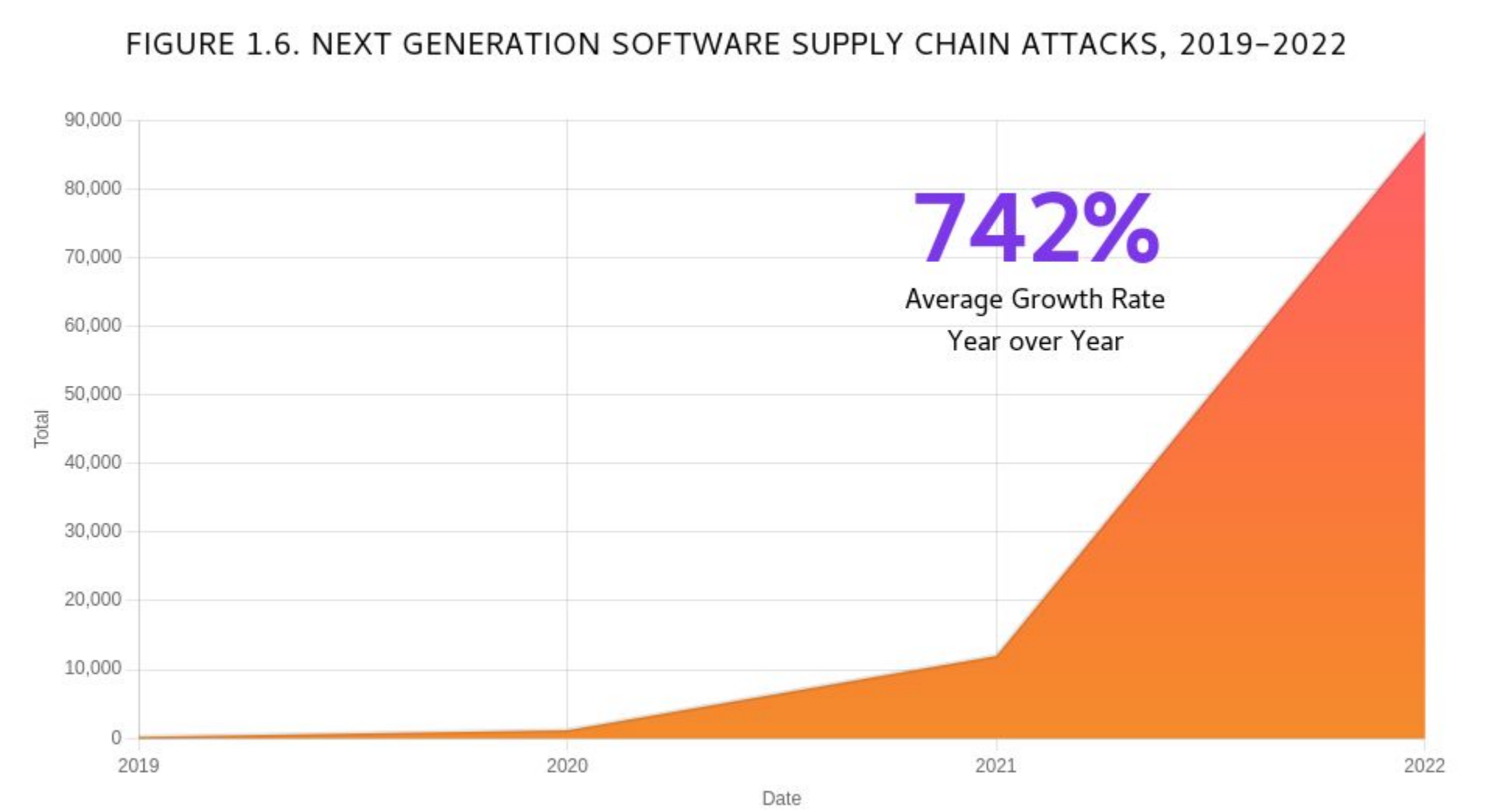


Service Mesh?



SPIFFE + Istio

Software Supply Chain?

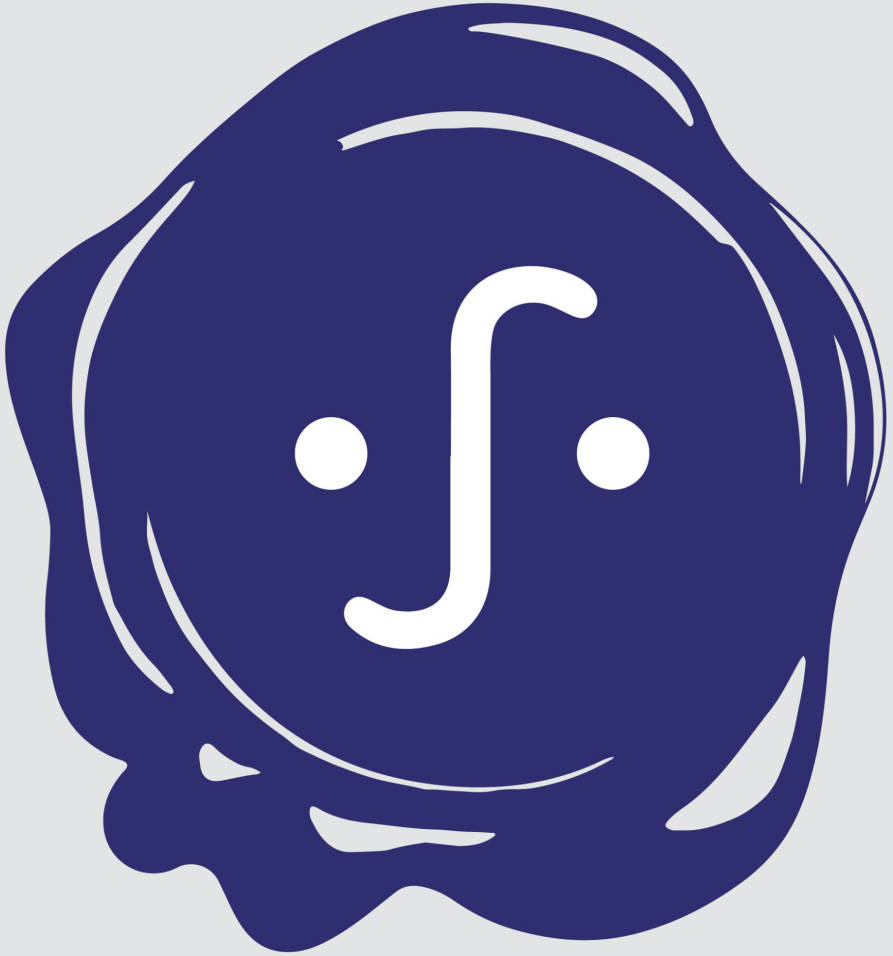


Tekton?

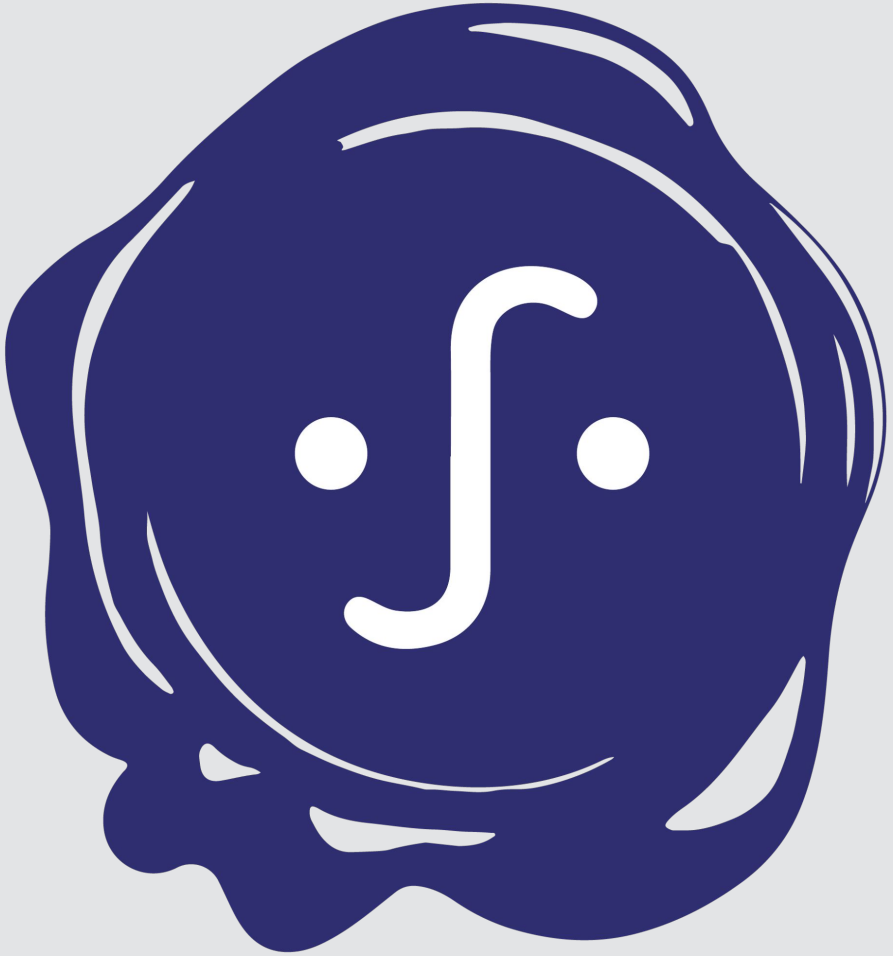
SPIFFE + Tekton

- SLSA Level 3 - Requires Non-Falsifiable Provenance
- TEP-0089 - Proposes leveraging SPIFFE/SPIRE for workload identity and signing

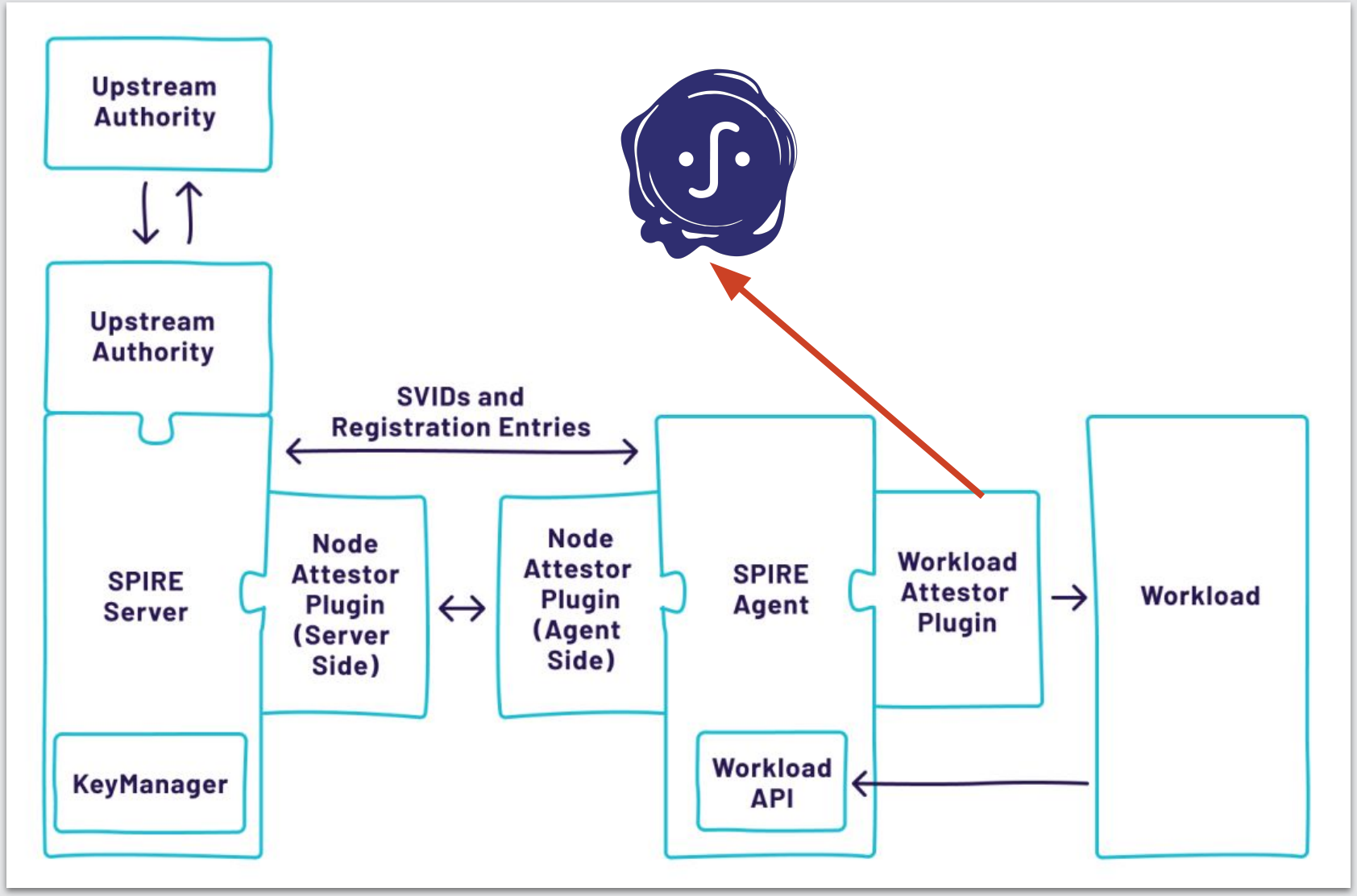
Sigstore?



SPIFFE + Sigstore



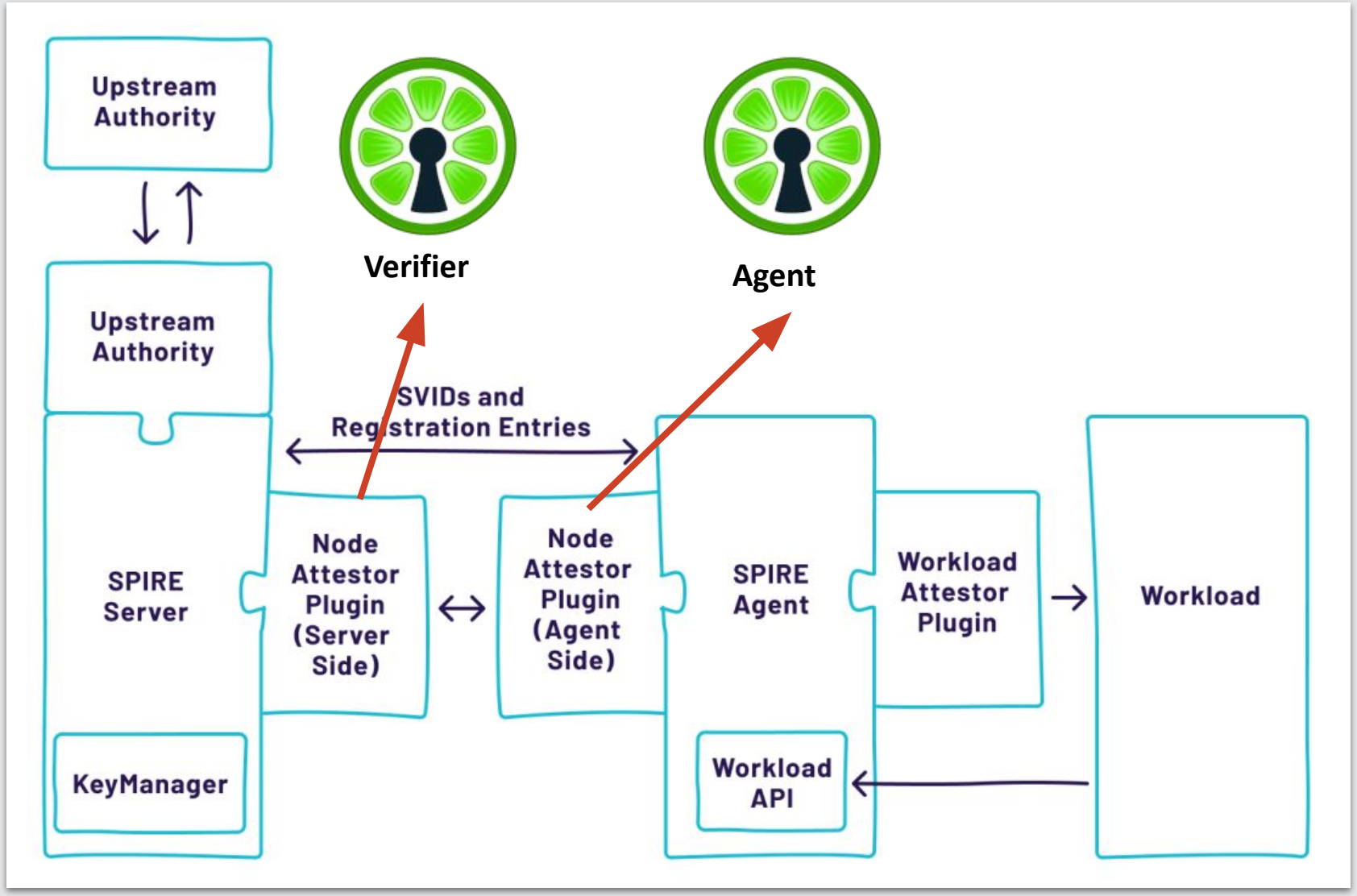
SPIFFE + Sigstore



Keylime?

SPIFFE + Keylime

SPIFFE + Keylime



Thanks!

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Please scan the QR Code above to leave feedback on this session