



CLOUDNATIVE **SECURITYCON**

NORTH AMERICA 2023





CLOUDNATIVE
SECURITYCON

NORTH AMERICA 2023

Zero Trust Workload Identity in Kubernetes

Michael Peters - Red Hat

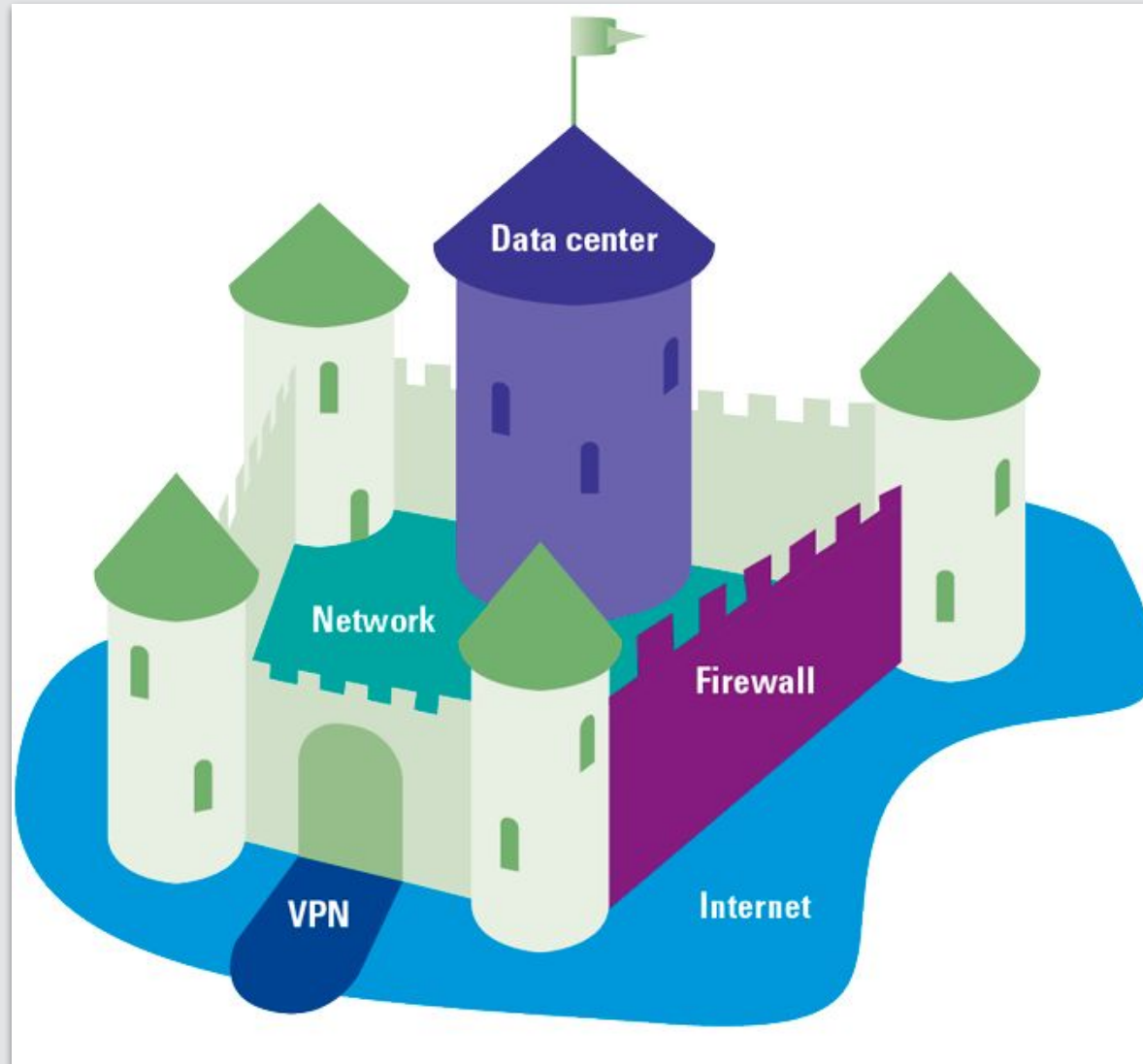


Zero Trust?

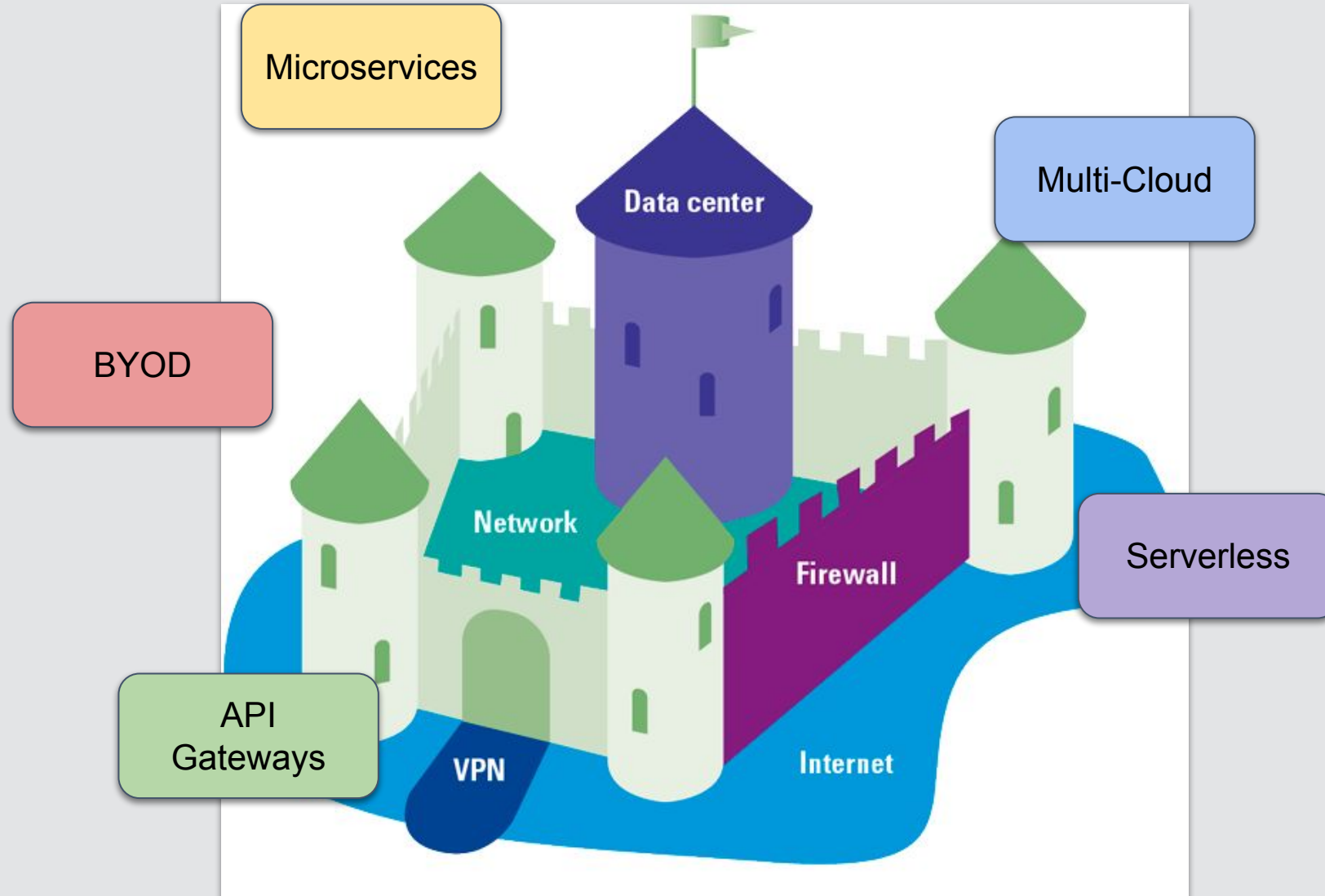
[^] *Implicit*

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

Zero Trust?



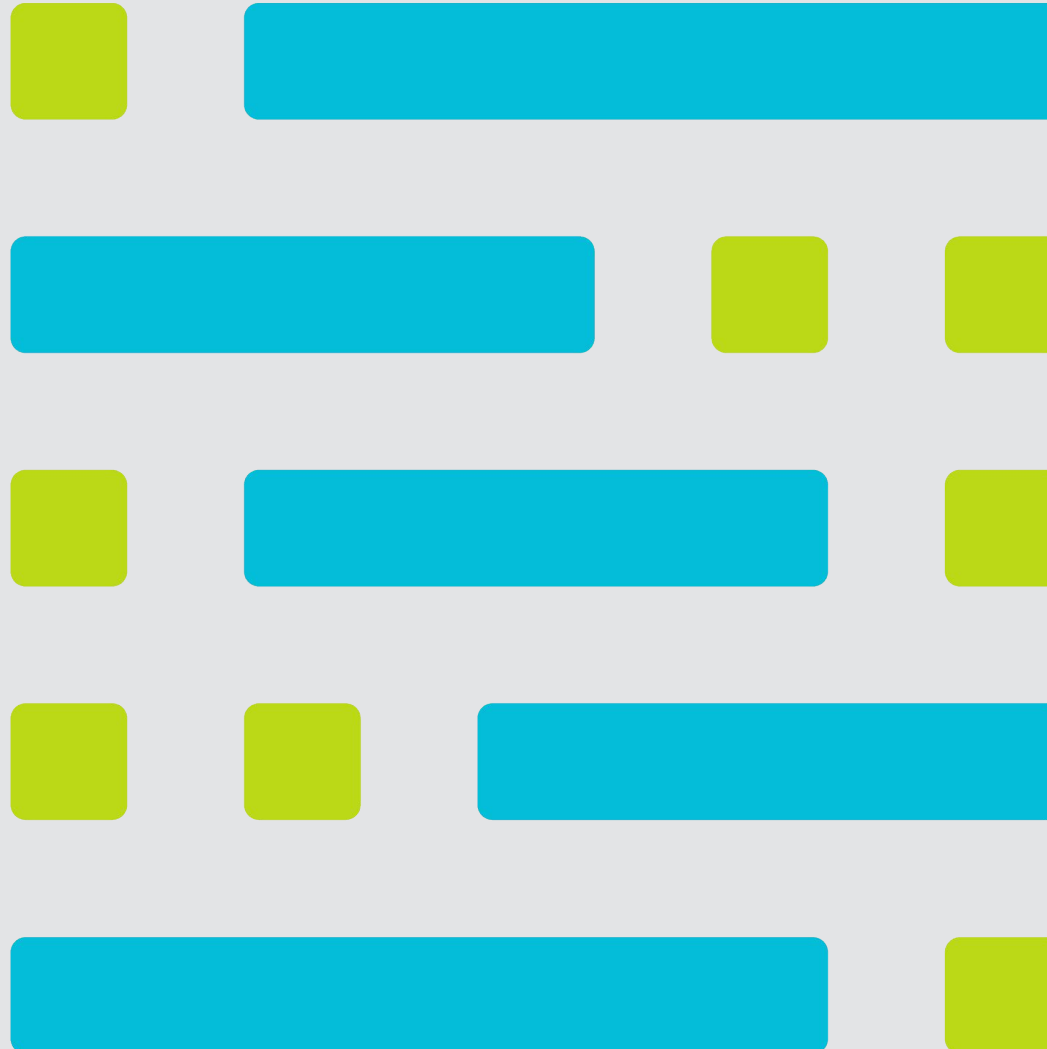
Zero Trust?



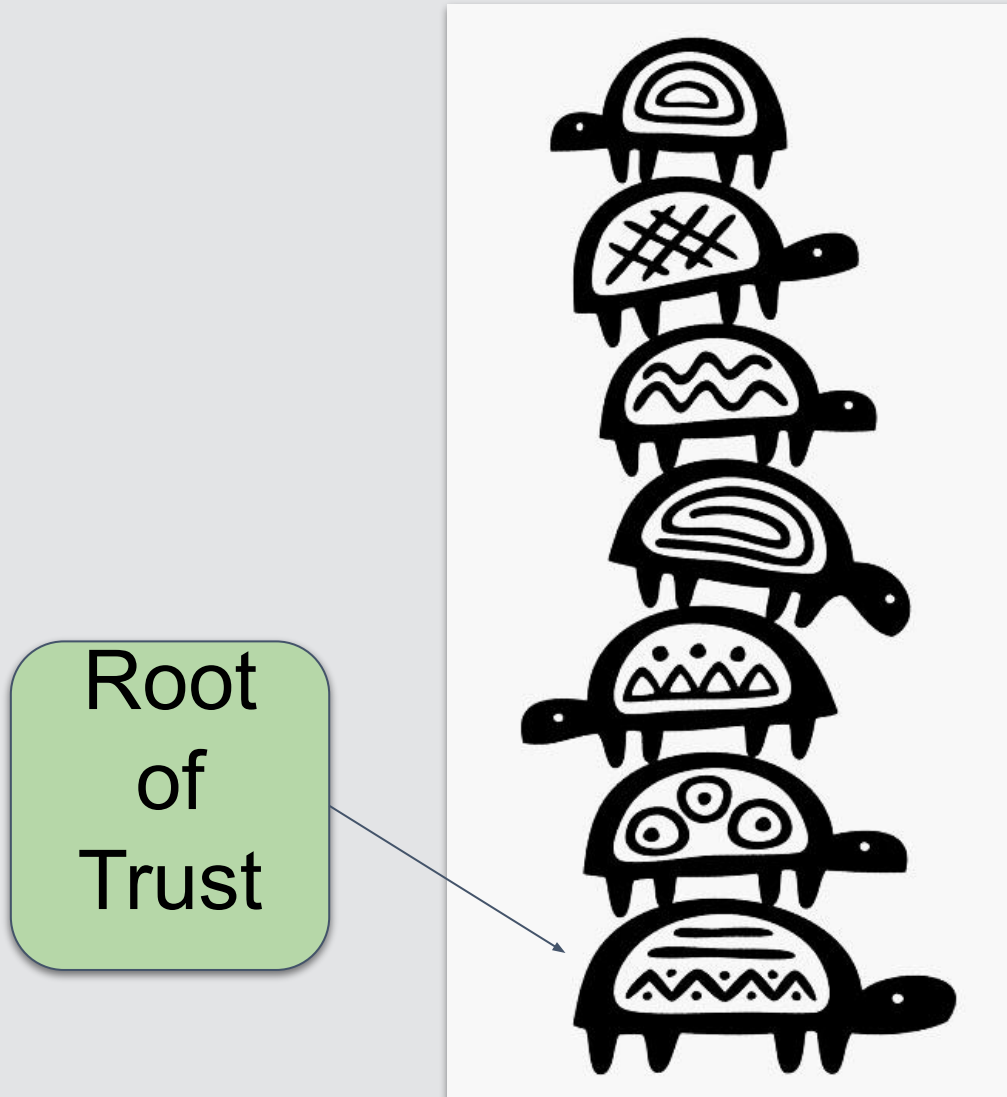
Zero Trust?



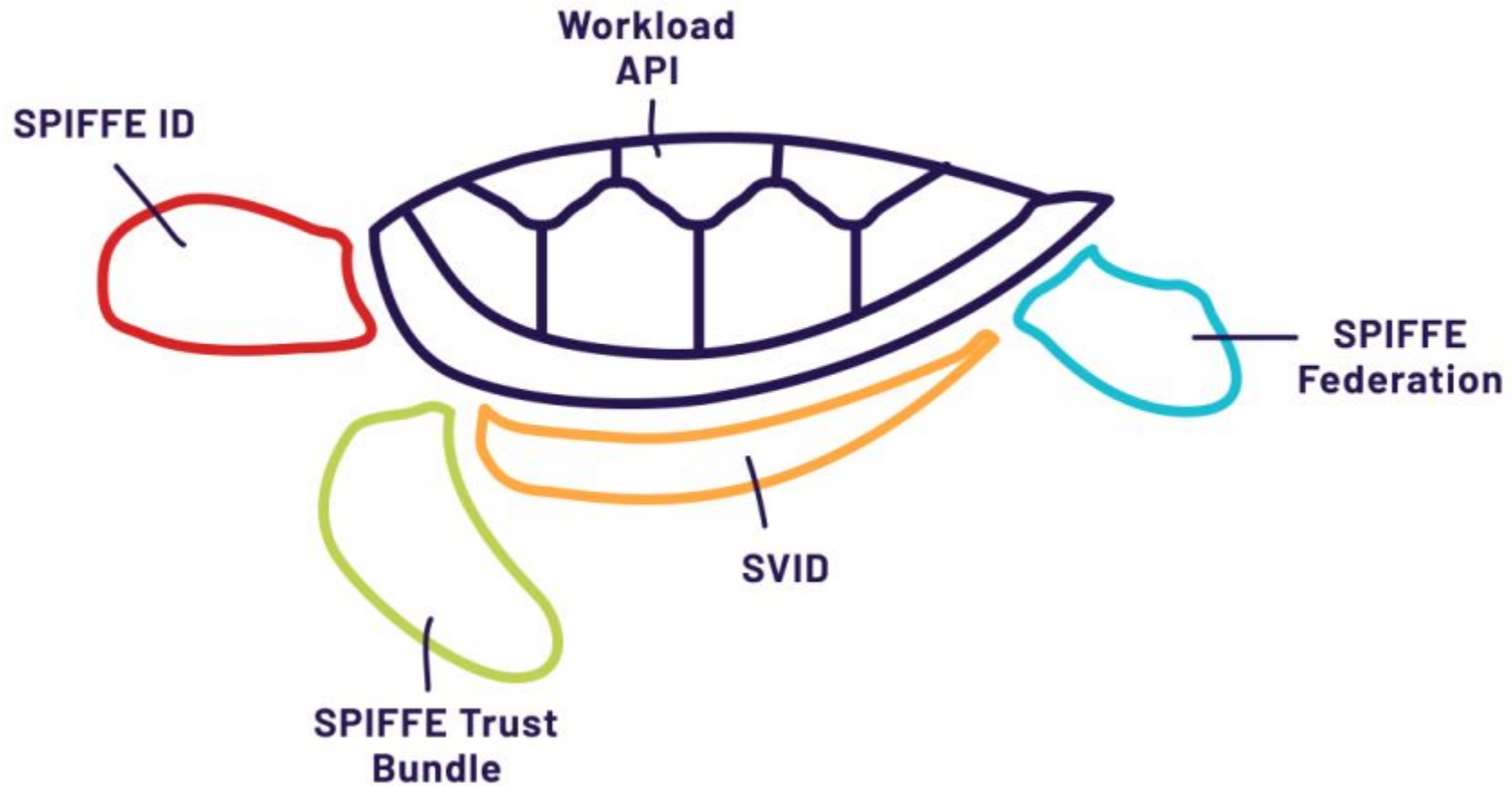
SPIFFE?



SPIFFE?



SPIFFE?



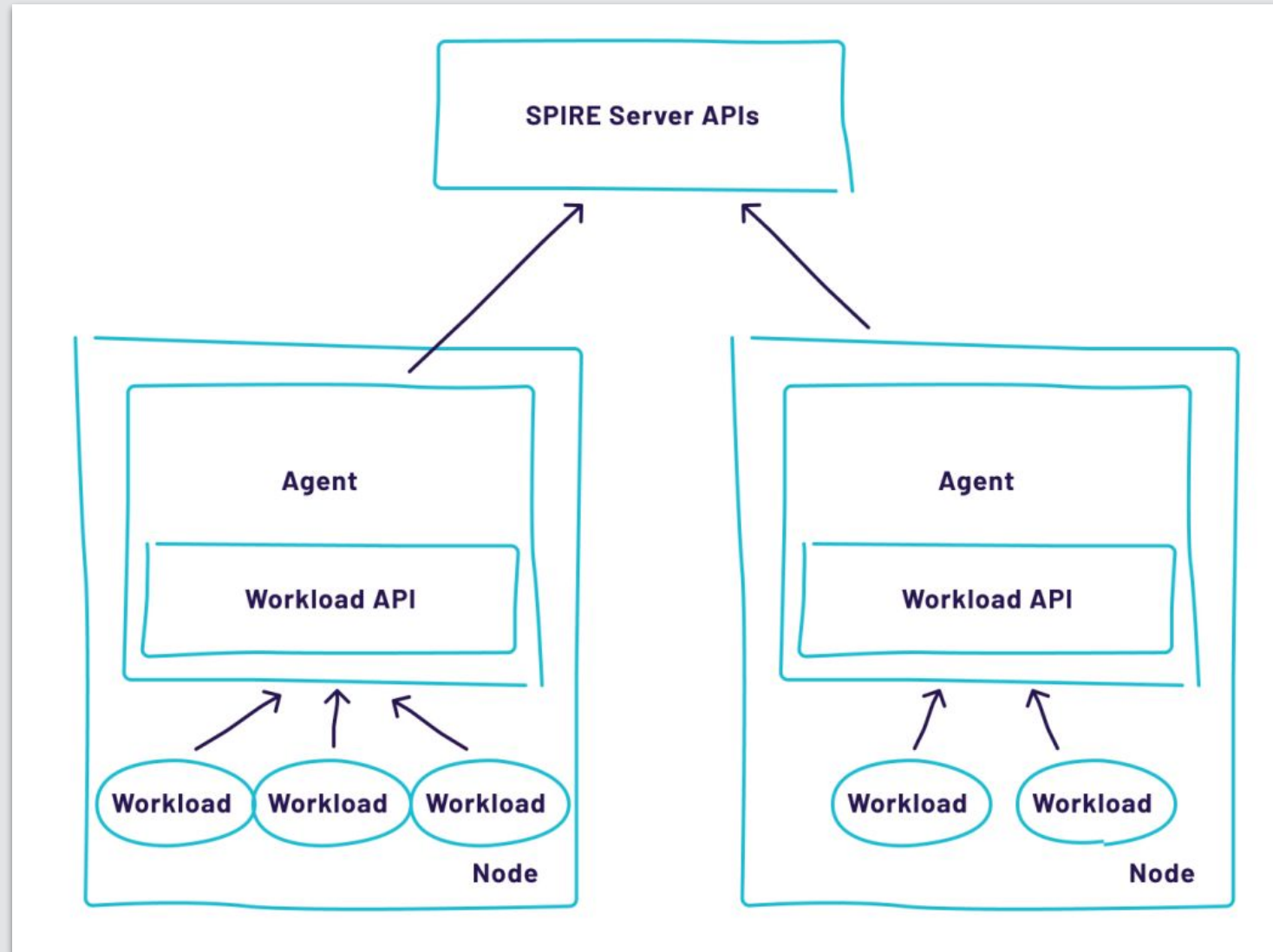
SPIFFE ID?

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

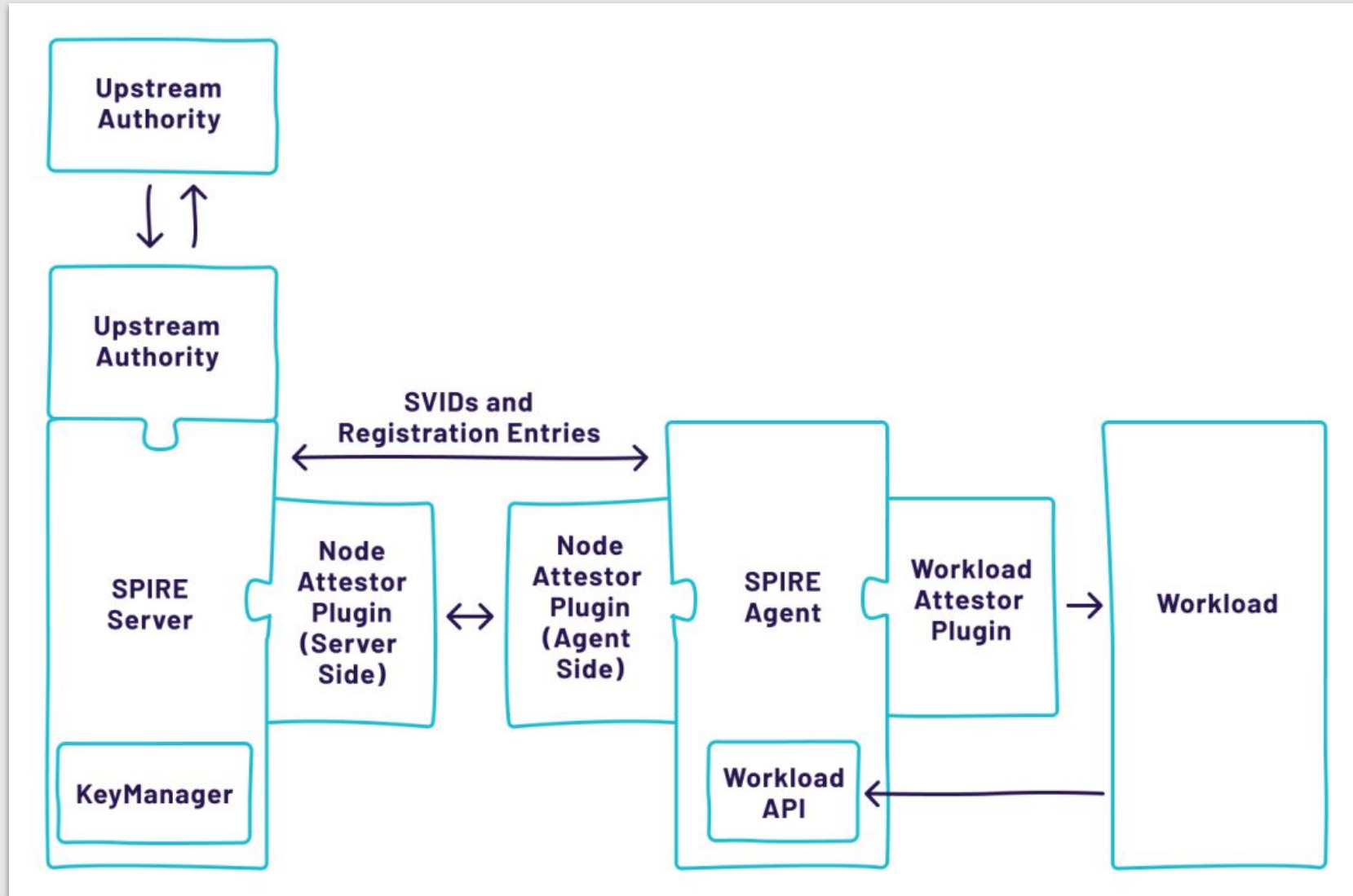
SPIRE?



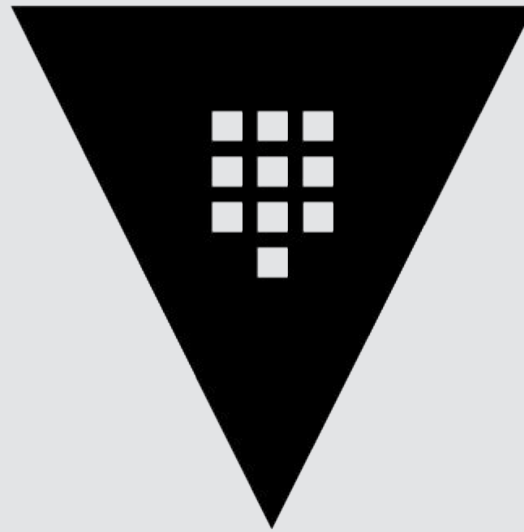
SPIRE?



SPIRE?

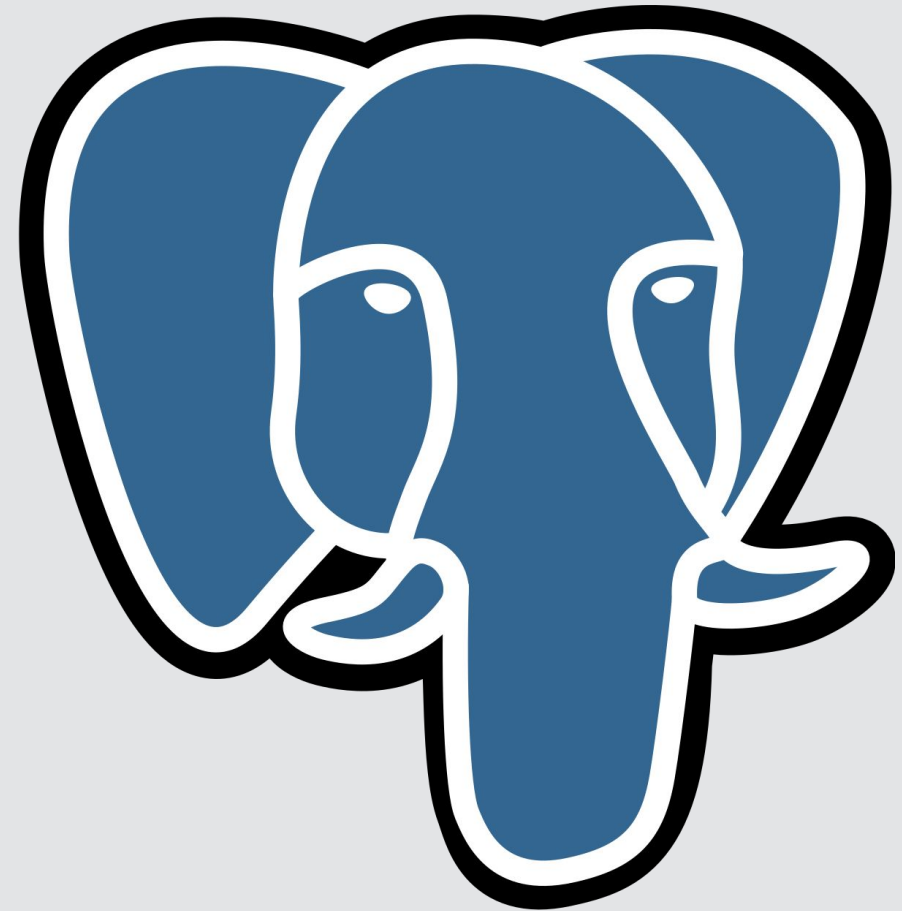
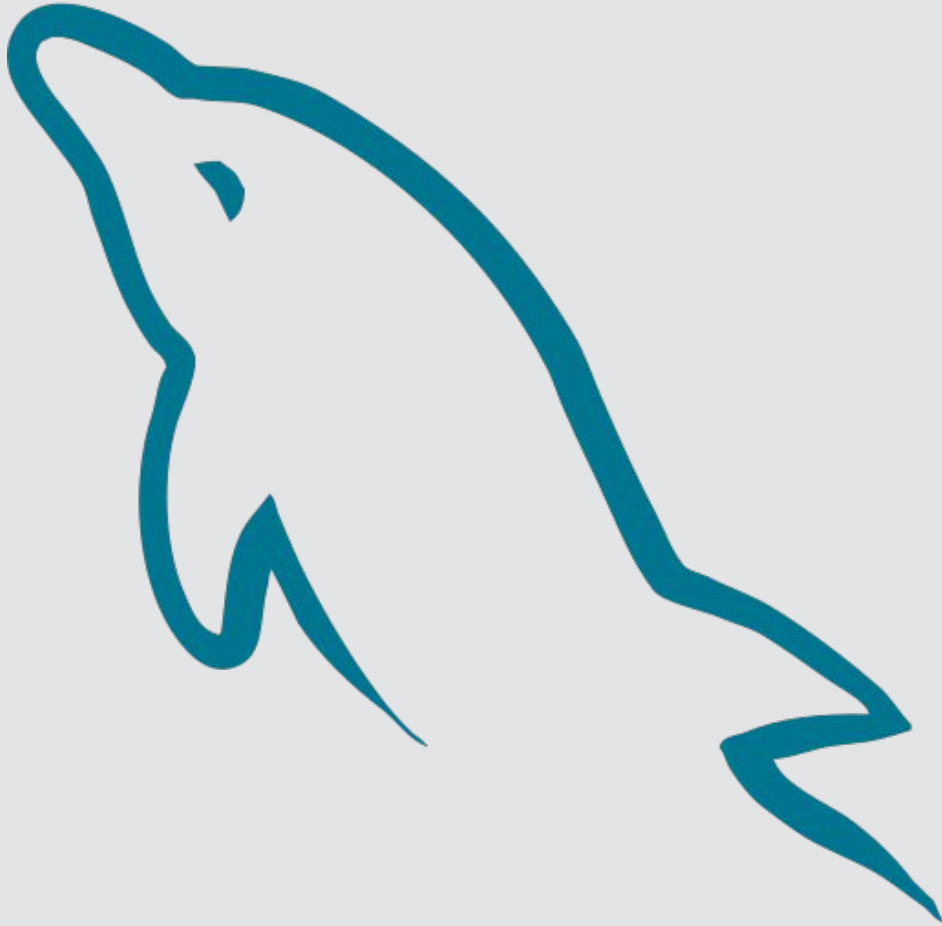


SPIFFE + Vault

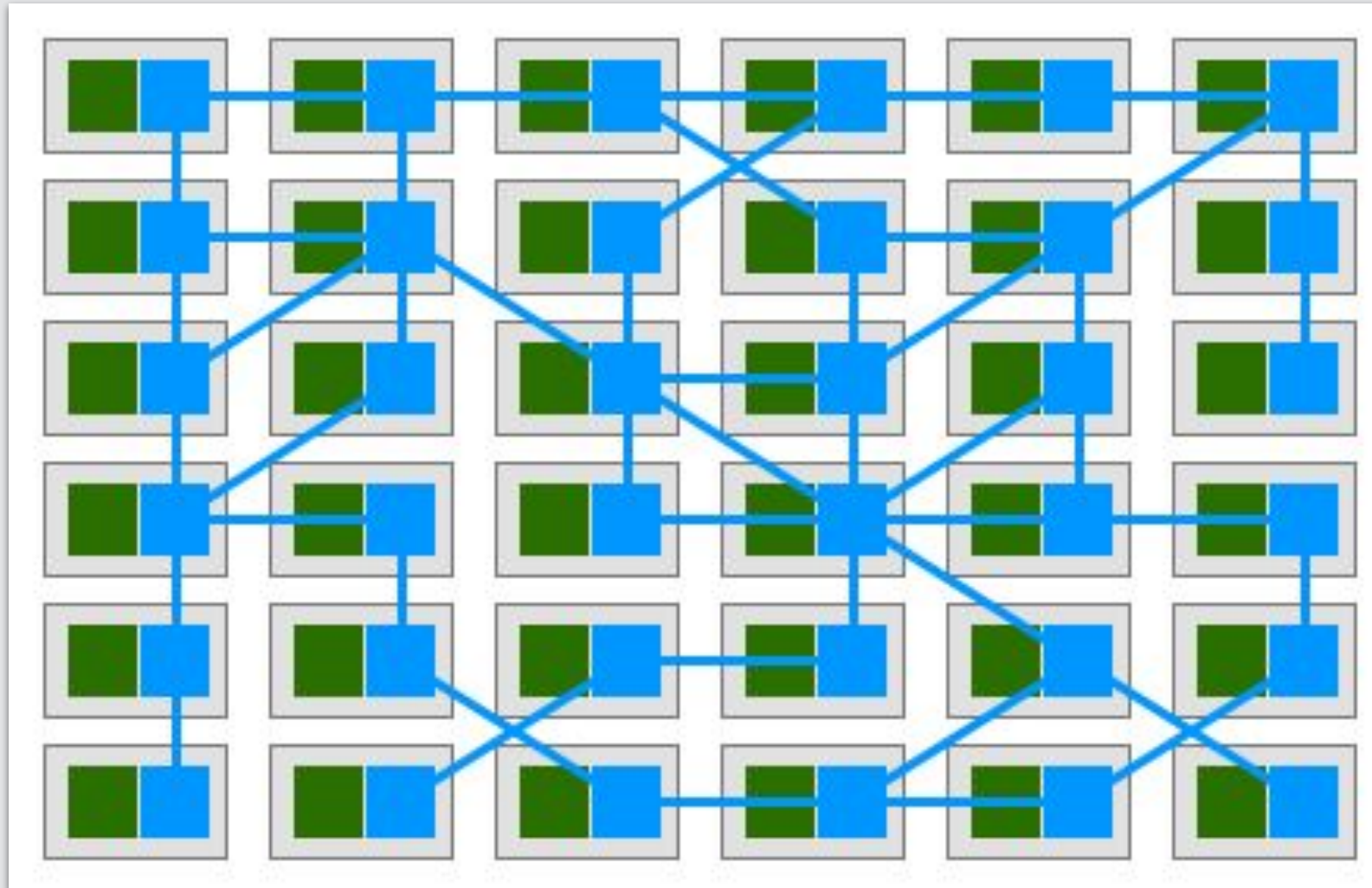


HashiCorp
Vault

SPIFFE + Databases



Service Mesh?

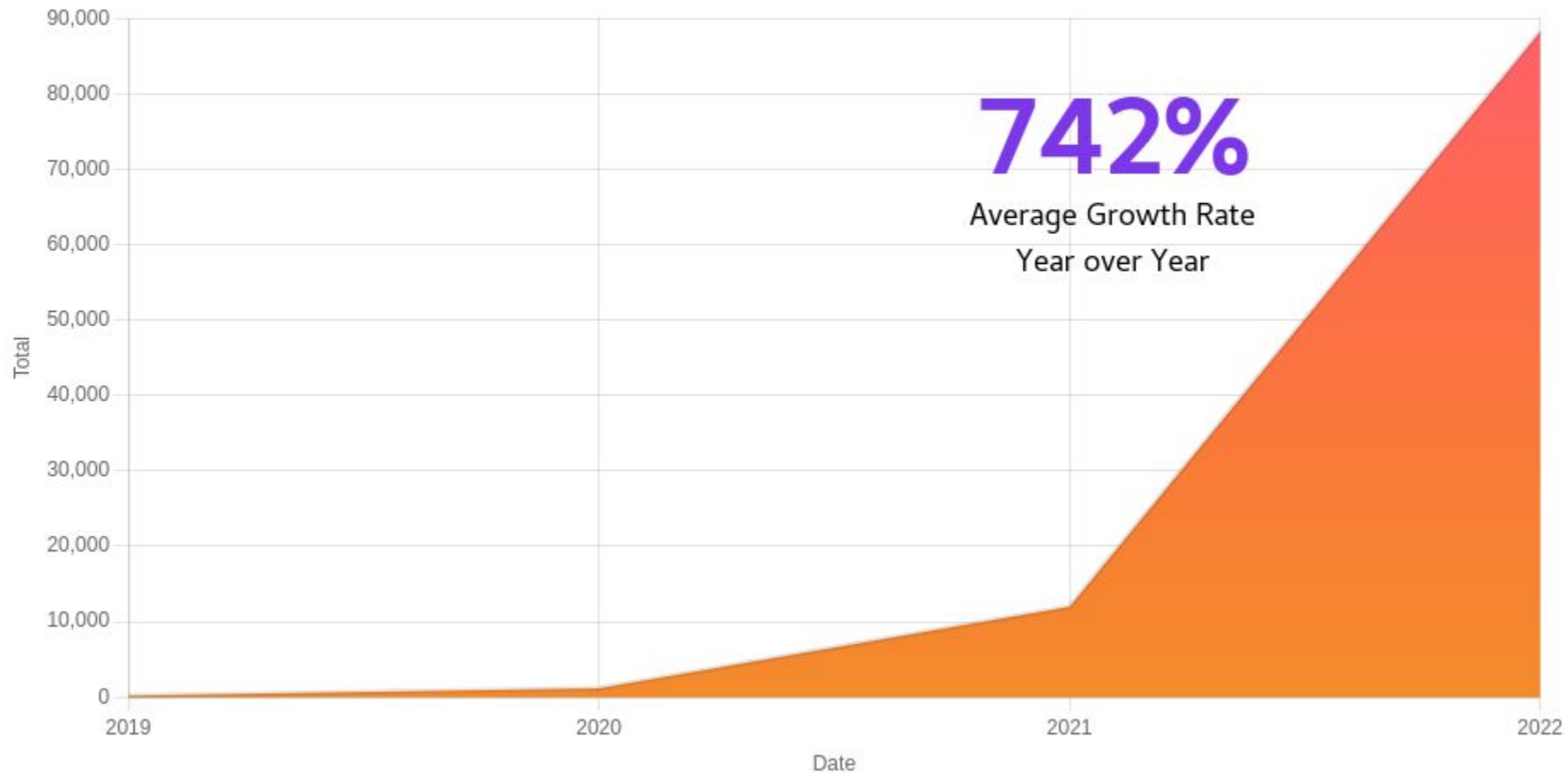


SPIFFE + Istio



Software Supply Chain?

FIGURE 1.6. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019-2022



Tekton?

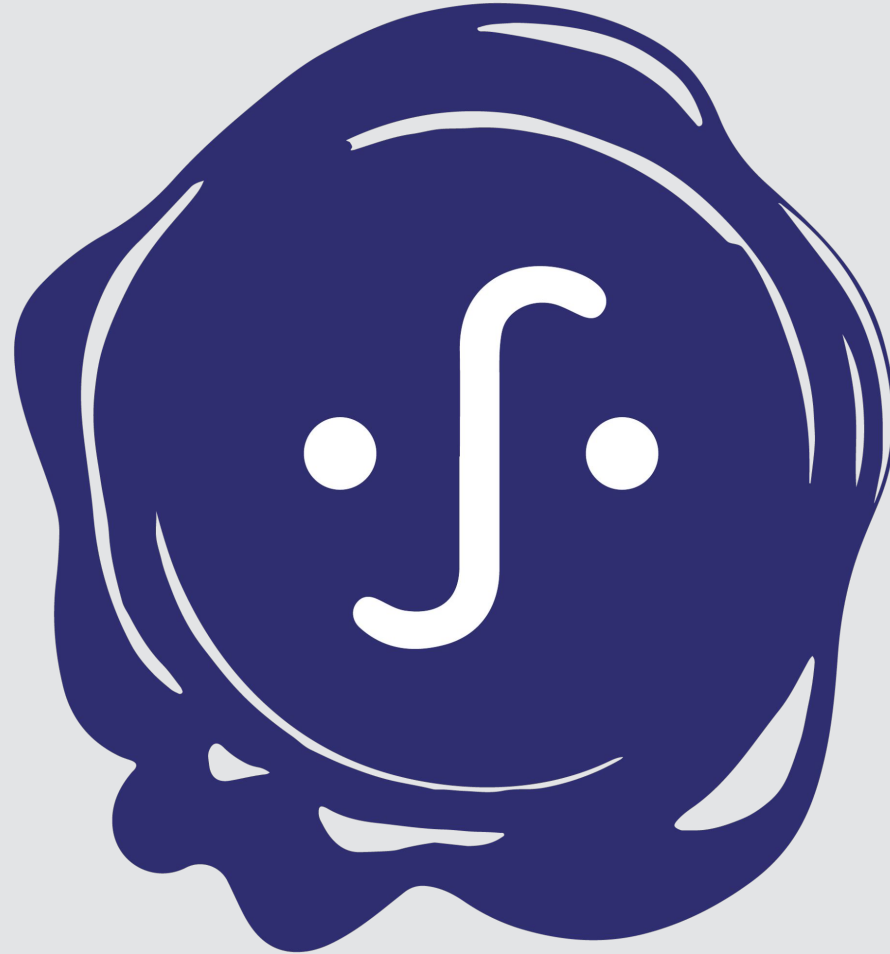


SPIFFE + Tekton

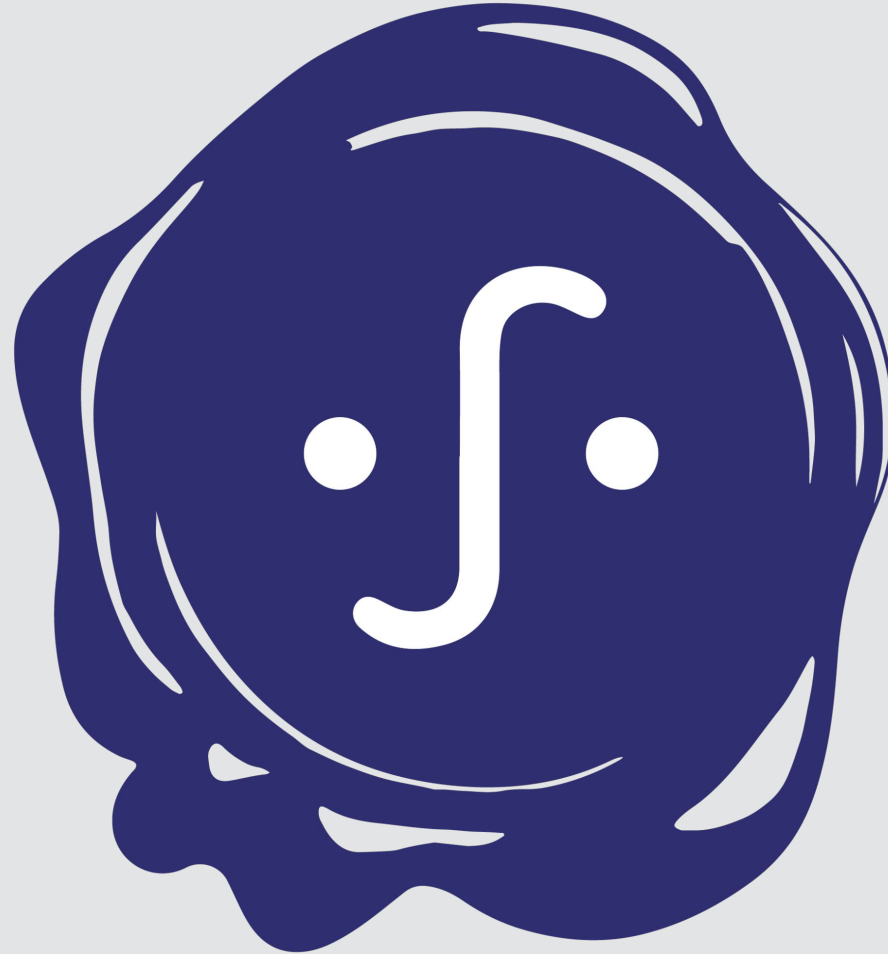


- SLSA Level 3 - Requires Non-Falsifiable Provenance
- TEP-0089 - Proposes leveraging SPIFFE/SPIRE for workload identity and signing

Sigstore?



SPIFFE + Sigstore



Keylime?



SPIFFE + Keylime



Thanks!



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