KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon CloudNativeCon Europe 2022

Multi-Cloud Workload Identity With SPIFFE

Charlie Egan & Jake Sanders

Multi-Cloud Workload Identity With SPIFFE

KubeCon CloudNativeCon Europe 2022

We show how the SPIFFE standard can be the foundation for a seamless, multi-cloud workload identity system.

Jake Sanders
Senior Software Engineer
Jetstack

Charlie Egan
Senior Software Engineer
Jetstack

What is a Workload Identity?

An identity is a way for a workload to prove its authenticity to other workloads.

We believe…

- Every workload should be issued an identity automatically, just by existing.
- This identity must be represented by an unforgeable document.
- Workloads should not have to do or know anything to get their identity.

Identity icon - https://dannya.org/

State-of-the-art: Any Single Cloud Provider

- GKE Workload Identity, EKS Pod Identity & Azure AD pod-managed identities all provide unforgeable, short-lived tokens through their metadata services.
- Workloads using cloud SDKs automatically discover and use these identities transparently.
- Developers don’t have to handle secrets to call cloud APIs.

Digital Identity icon by elconomeno - OpenClipArt

Problem: Increased Lock-in, Worse Security

- Identities issued by a cloud are proprietary. You can't use easily this identity outside the issuing cloud.
- Creating additional access credentials for workloads outside the cloud becomes a security issue.
- Access credentials can't cryptographically **identify** the bearer - they're just another password.
- We wish there was a secure, production-ready identity standard for everyone…

Digital Identity icon by elconomeno - OpenClipArt

Enter SPIFFE

- Foundation for a cloud-agnostic identity control plane
- SPIFFE ID & SVID - A standardized identity and identity document (consisting of a X.509 Certificate)
  - `spiffe://trust.domain/app`
- CNCF Incubating project & open source
- Gaining adoption

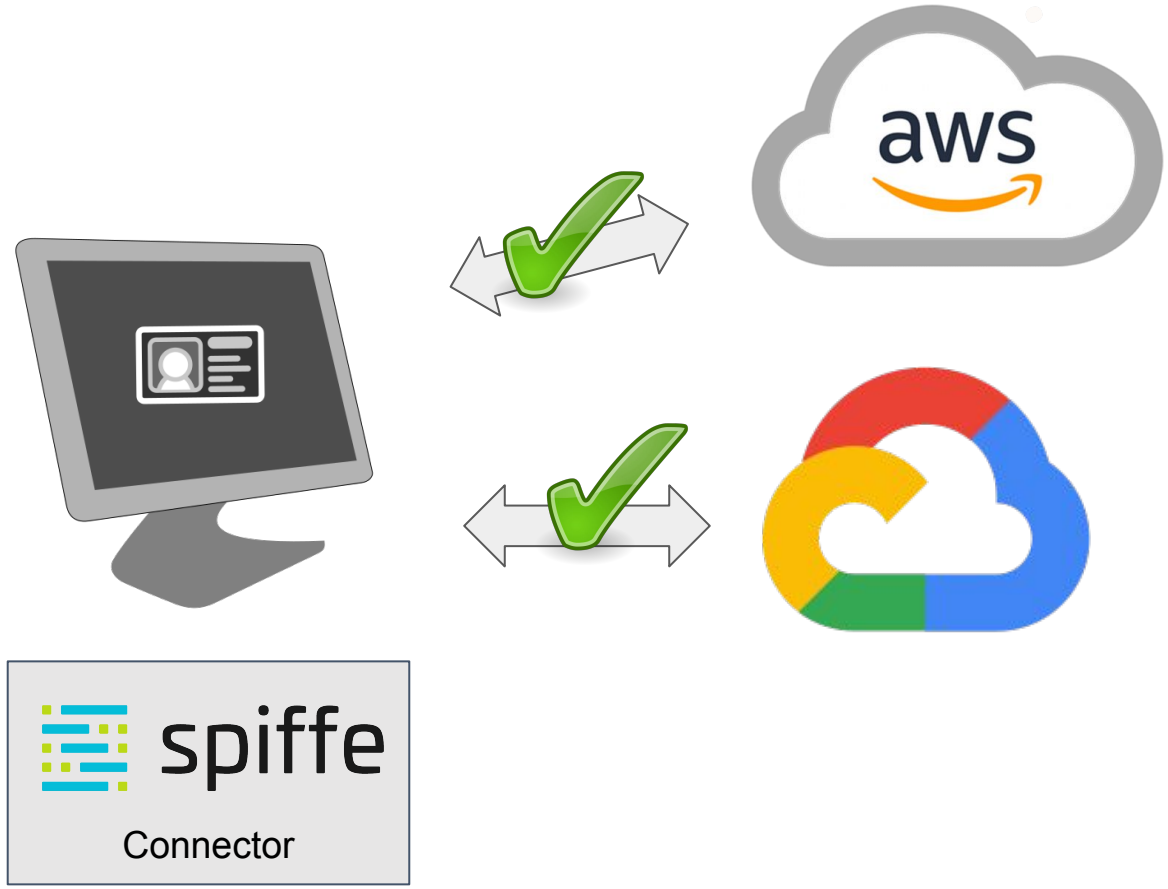
spiffe

Cloud-Native SVIDs

- cert-manager is a CNCF sandbox project dedicated to cloud-native X.509 certificate management.
- cert-manager/cert-manager - a popular Kubernetes operator that can issue X.509 certificates from almost any CA.
- cert-manager/csi-driver-spiffe - a CSI driver that delivers SPIFFE compliant X.509-SVIDs from cert-manager to pods using CSI.
- cert-manager/trust - Trust root distribution and management.

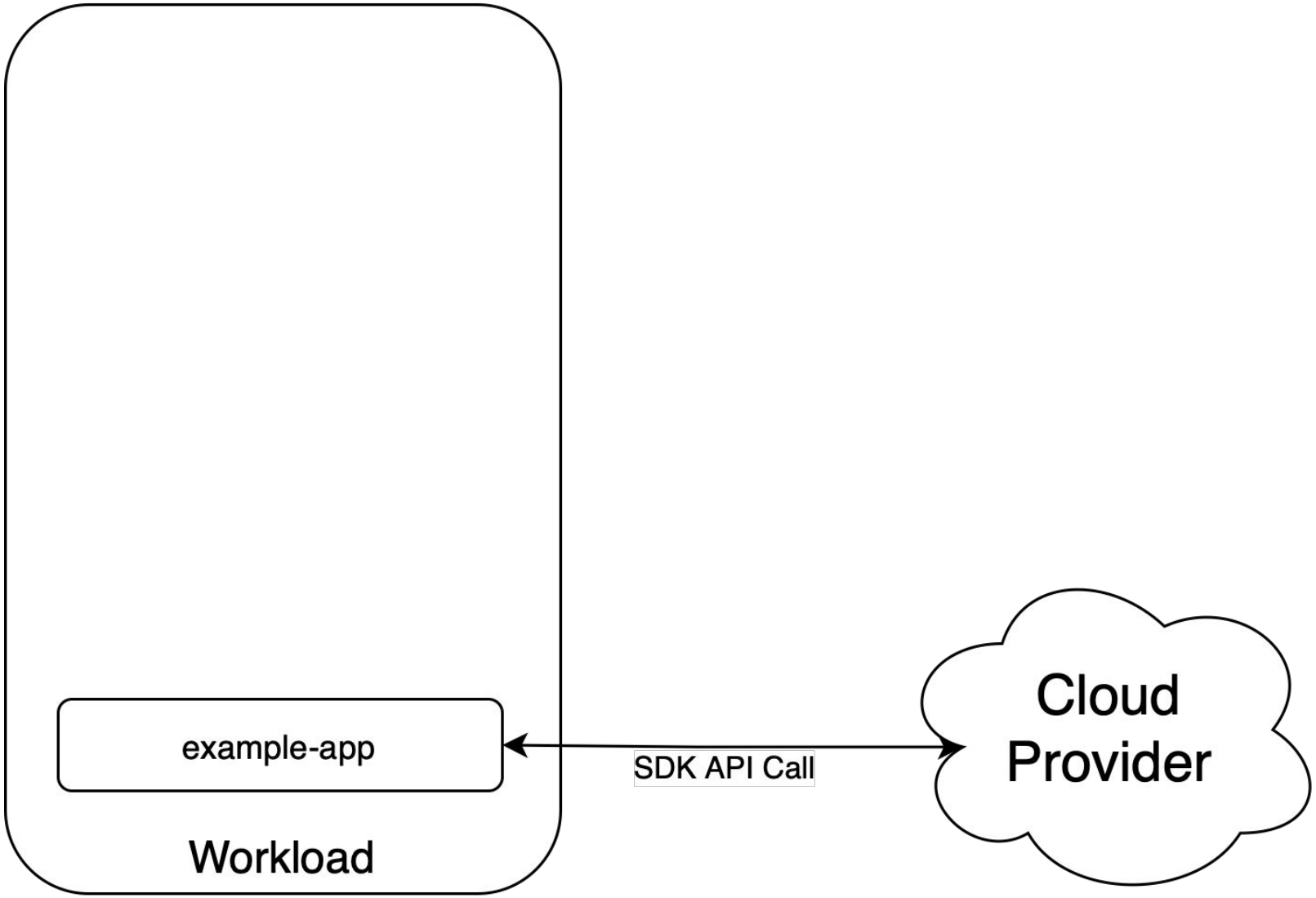
The missing link - SPIFFE-connector

- SPIFFE - Secure Production Identity Framework For ~~Everyone~~ *Envoy?*
- We think SPIFFE is a great standard, and in future we hope everything will utilize SVIDs natively.
- To demonstrate, we want to recreate the same seamless cloud provider identity UX, but backed by cryptographically verified SVIDs.

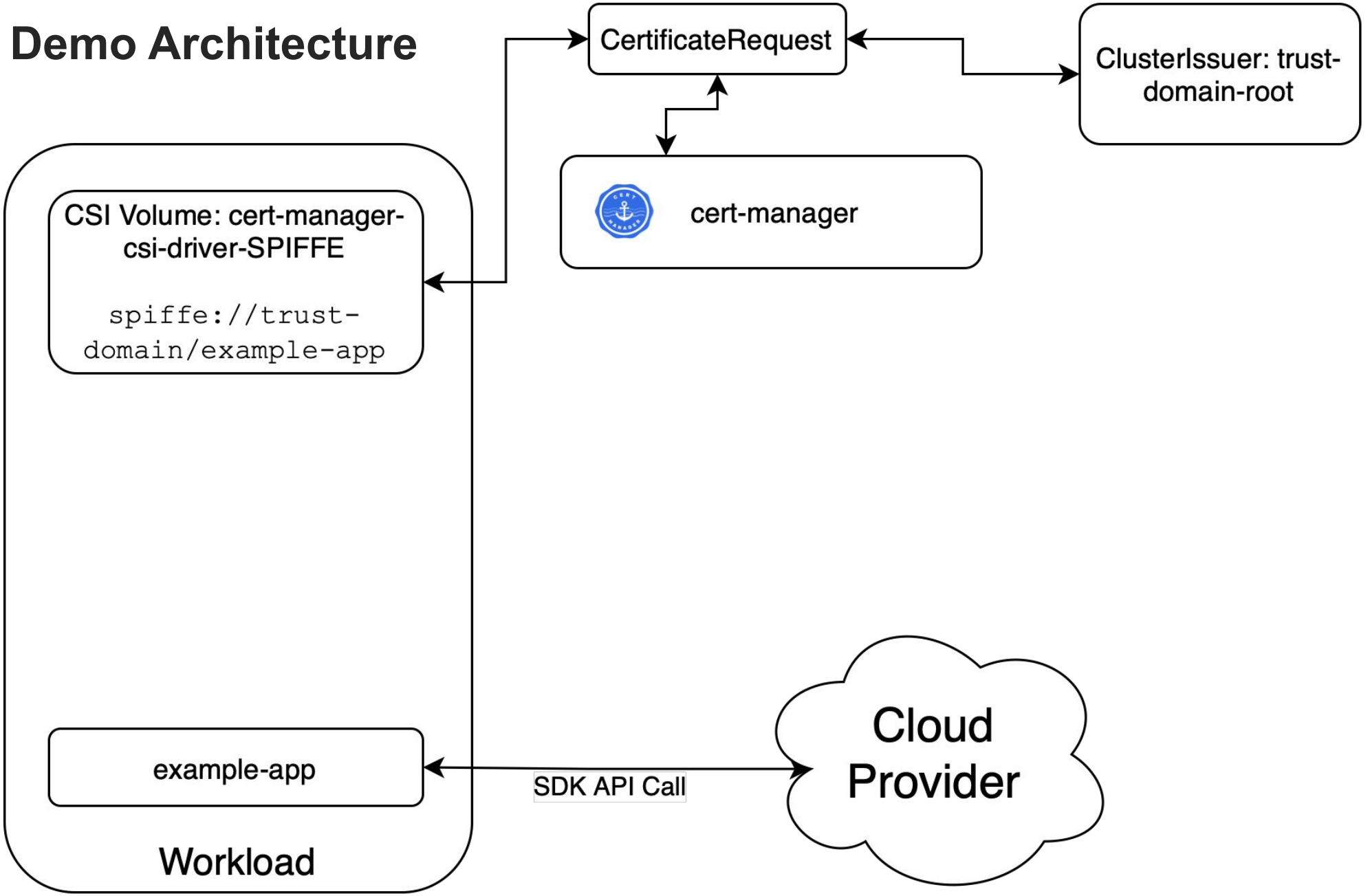


Digital Identity icon by elconomeno - OpenClipArt

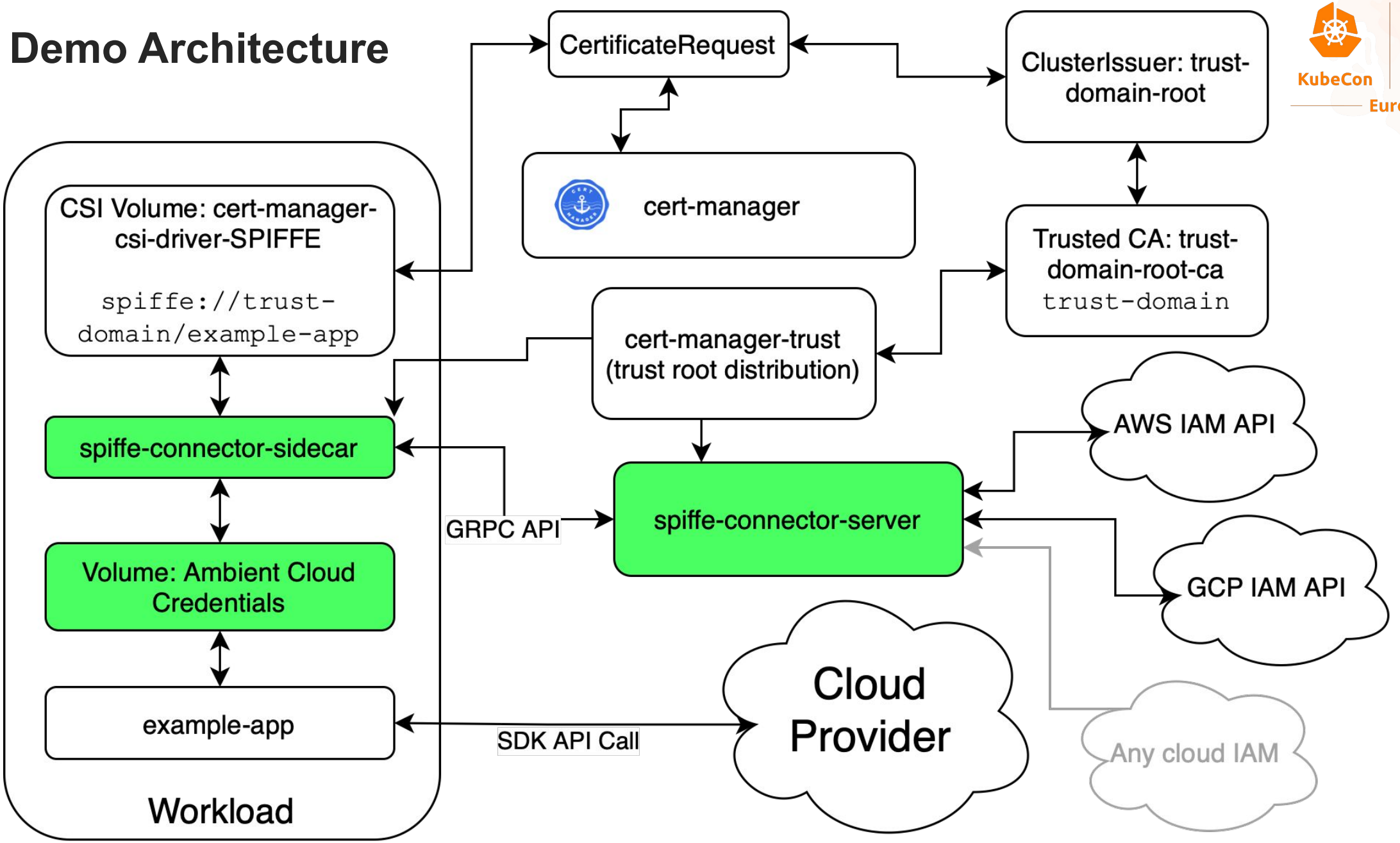
Demo Architecture



Demo Architecture



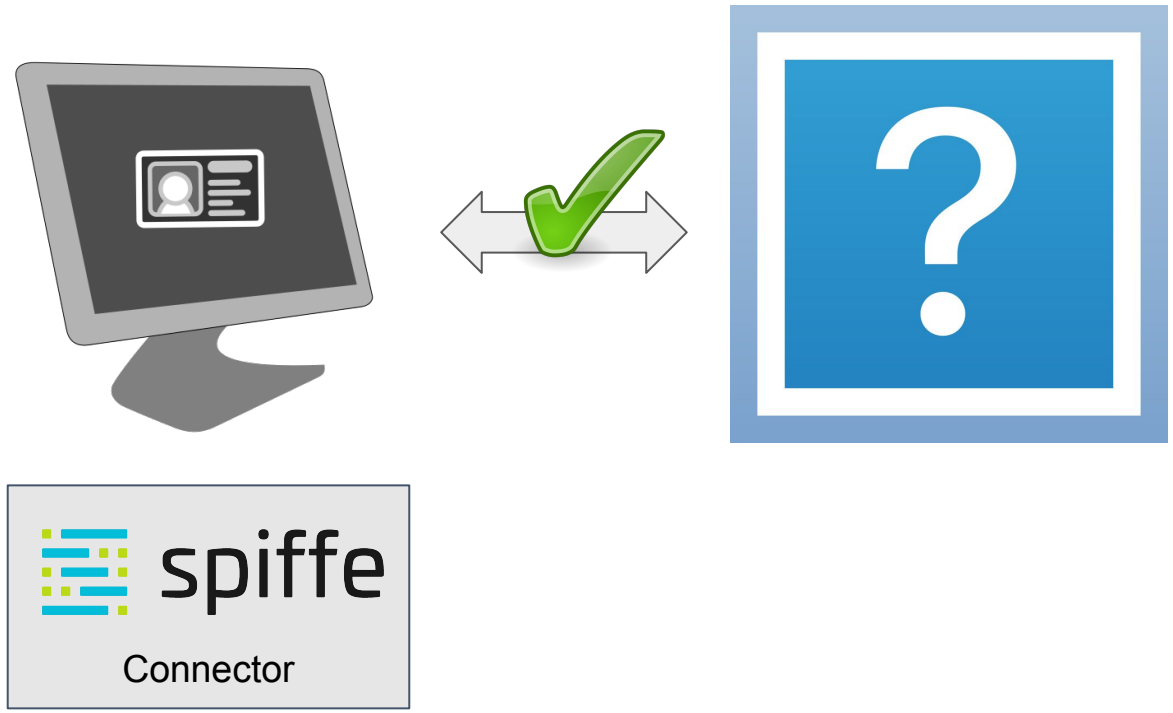
Demo Architecture



DEMO

Where Next?

- We have shown a proof of concept SPIFFE connector for cloud provider credentials.
- Lots of people asking how to manage identities for a replicated deployments - try SPIFFE out!
- We would like to build more SPIFFE-aware connectors to:
  - Databases
  - Message Queues
  - SaaS APIs
  - …



Missing icon by Lazur - OpenClipArt

Digital Identity icon by elconomeno - OpenClipArt

Multi-Cloud Workload Identity With SPIFFE

Please do ask us questions, now or later

charlie.egan@jetstack.io
jake.sanders@jetstack.io

Thanks to our colleague and teammate ***Josh van Leeuwen*** for collaborating with us on this project.

Further reading

https://github.com/jetstack/spiffe-connector
https://github.com/cert-manager/csi-driver-spiffe
https://spiffe.io