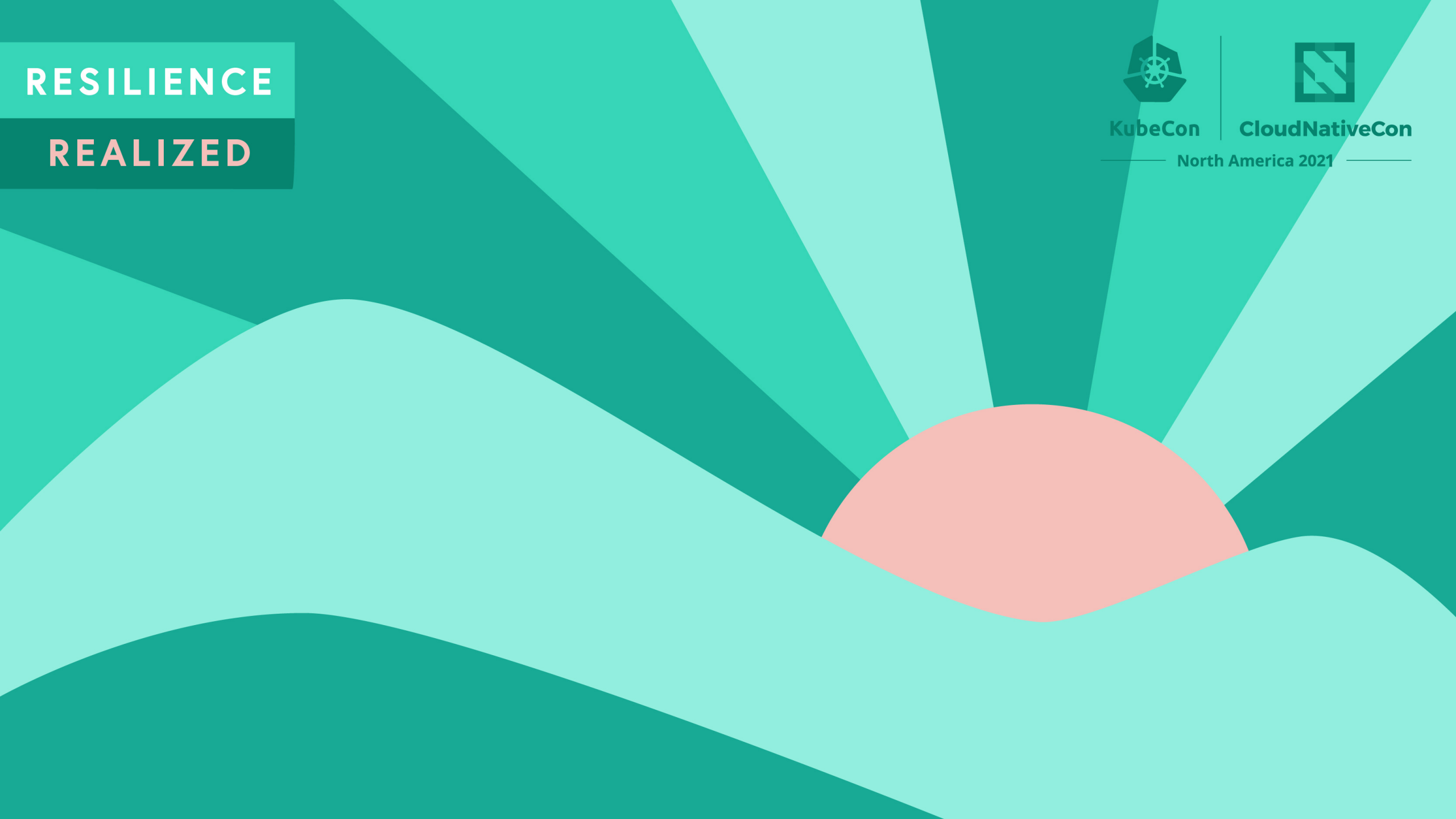
RESILIENCE REALIZED




KubeCon | CloudNativeCon

North America 2021

RESILIENCE
REALIZED

Untangling the Multi-Cloud Identity and Access Problem With SPIFFE Tornjak

Brandon Lum (@lumjjb), IBM
Mariusz Sabath (@mrsabath), IBM

Introduction

Brandon Lum
IBM Research
CNCF TAG-Security

@lumjjb

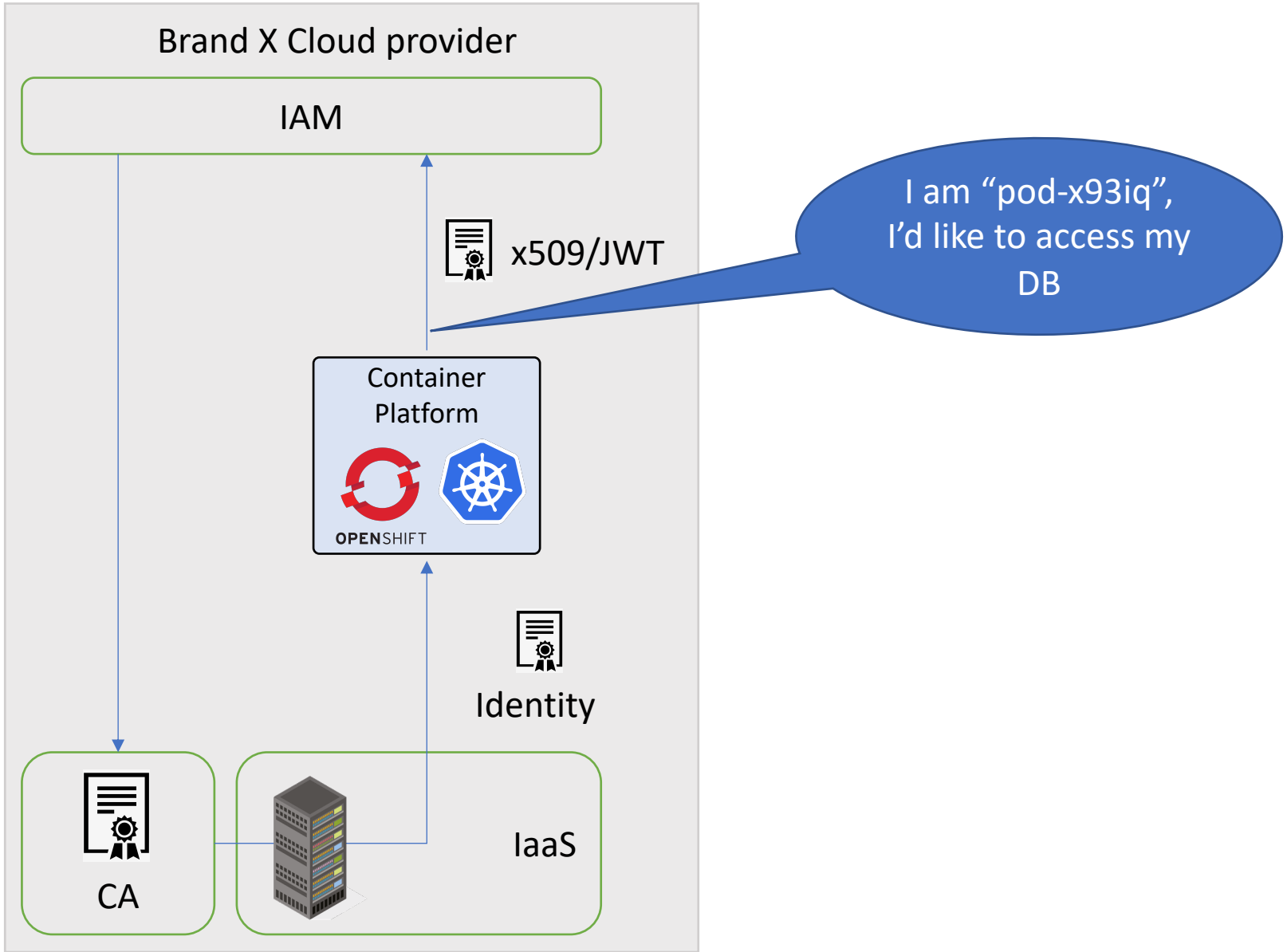
Mariusz Sabath
IBM Research

@mrsabath

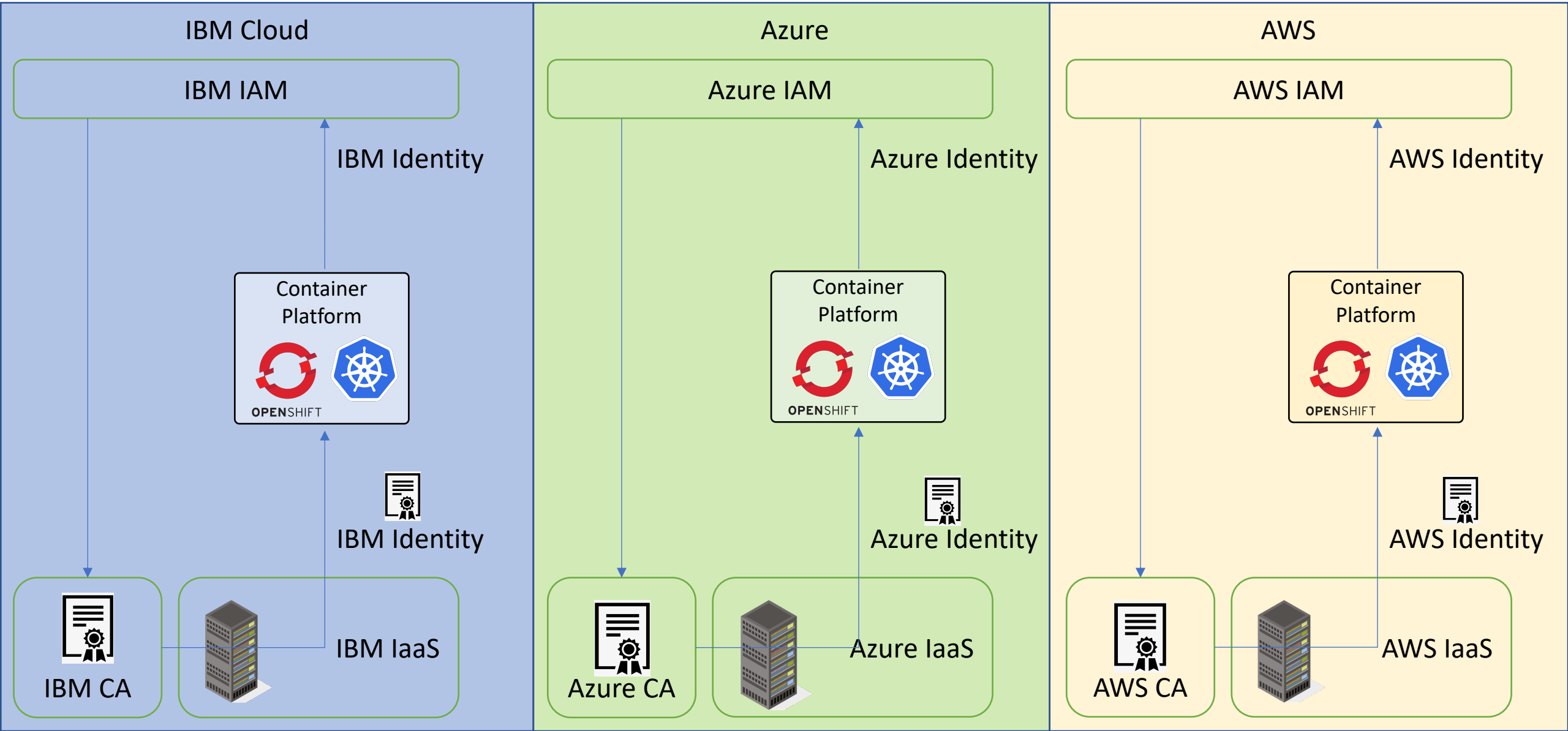
Overview

- Workload Identity
- The Multi Cloud access problem
- Solutions – with more problems!
- Universal/Organization-wide Workload Identity

Anatomy of Cloud Workload Identity



Workload Identity in Multi-cloud Scenarios



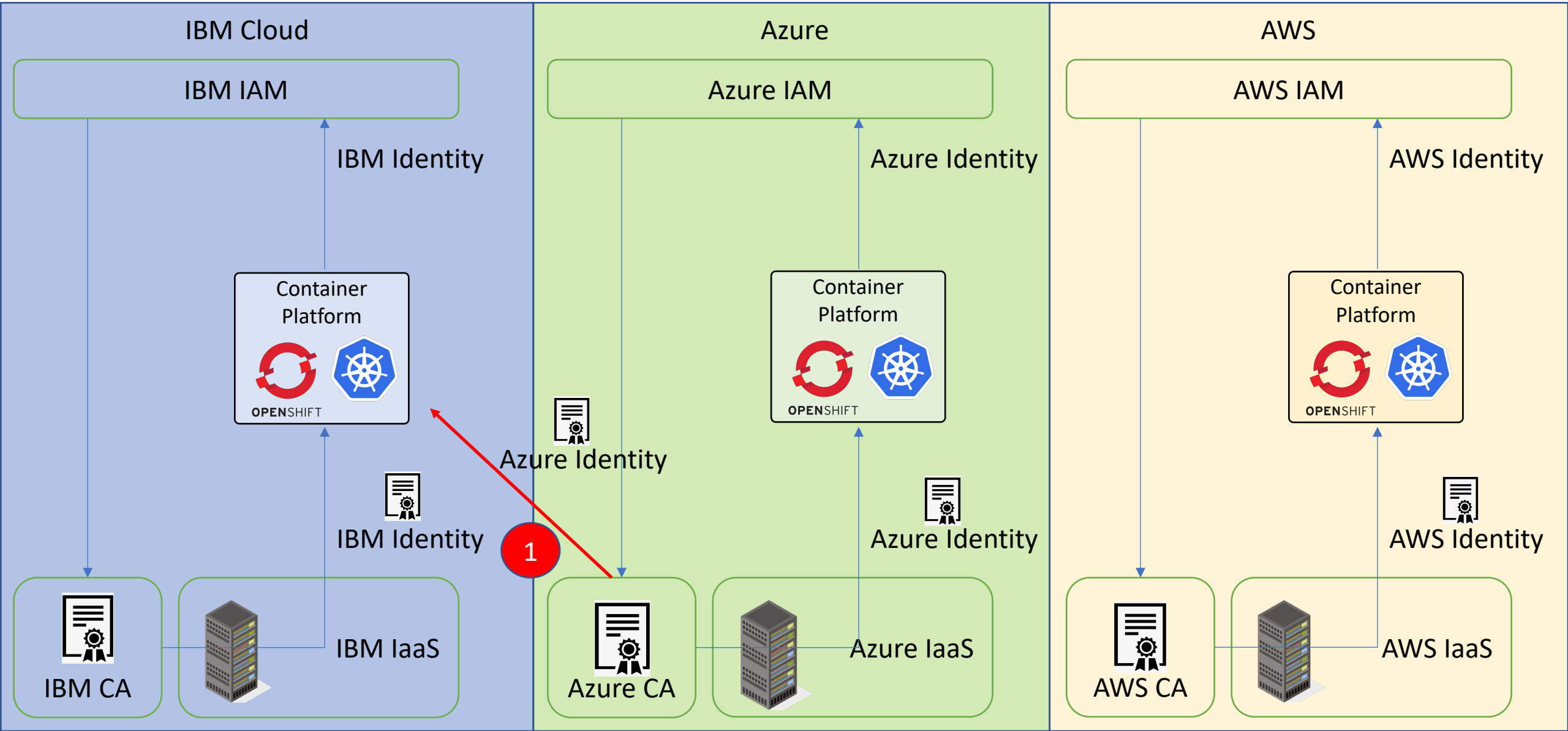
Status Quo

- Today, clouds provide workload identity and policy frameworks within their own domain which allows **strong authentication of workloads**, as well as **access control management**.

- Problem: I want to be able to access resources from one cloud to another, in a secure fashion.

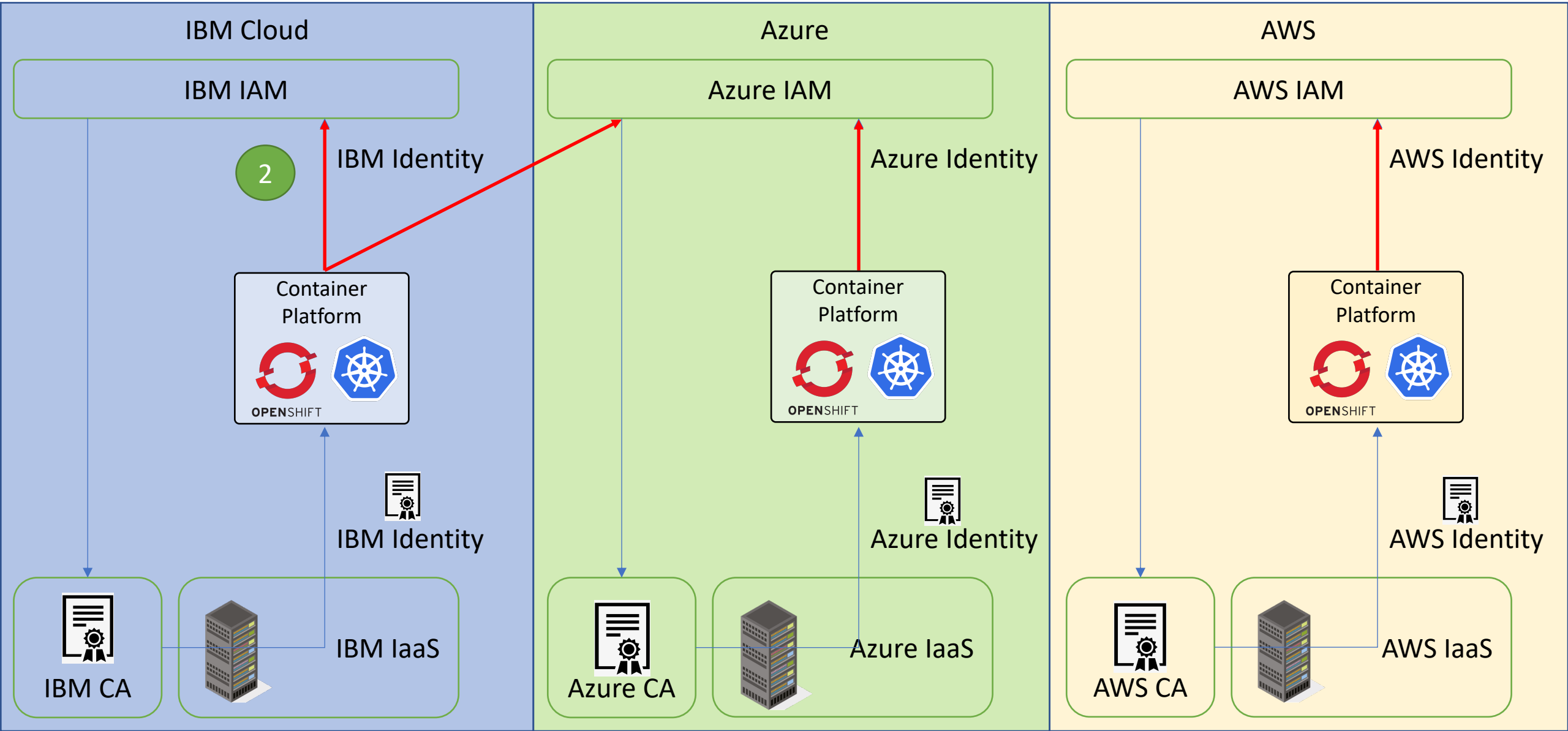
To configure cross cluster access can either:

1. Long-lived credentials (**simple**, **difficult to account blast radius**, **trusted intermediary required**)



To configure cross cluster access can either:

1. Long-lived credentials (**simple**, **difficult to account blast radius**, **trusted intermediary required**)
2. Cloud to cloud federation (**short-lived credentials**)



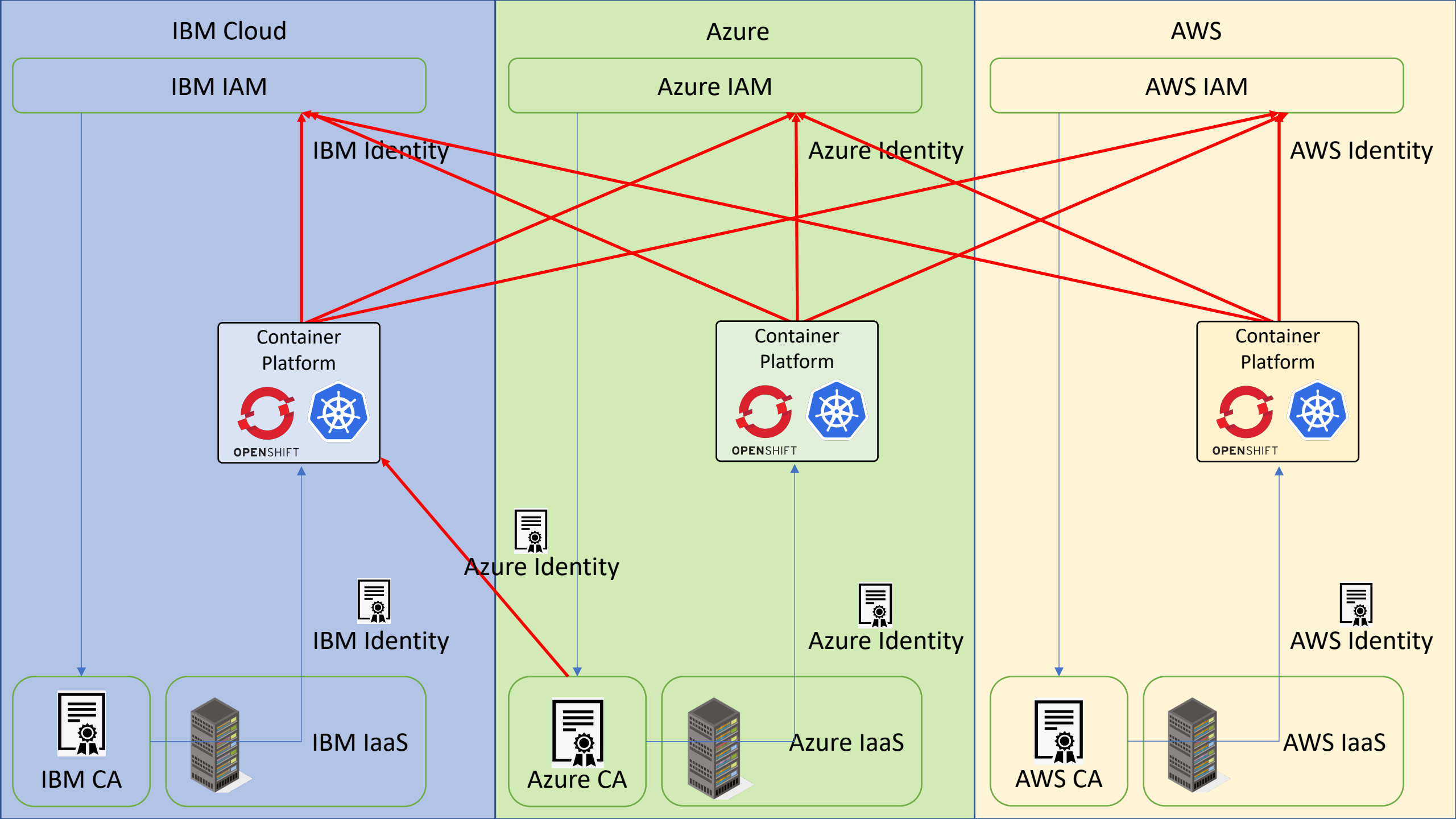
Solutions, and more problems

- I want to be able to access resources from one cloud to another

- Today's Solutions:
  - Most commonly: Naive (and non-secure) Approach: IAM long-term credentials
  - More secure approach: Pair-wise configuration of OIDC federation between all clouds

Solutions, and more problems

- Problems with secure approach
  - Support for this varies between clouds
    - AWS → gcloud easy
    - Gcloud → AWS hard
  - Schemas of identity are not consistent, require custom mapping and maintaining the trust relationship between pair-wise clouds
  - Pair-wise, unmaintainable at scale (quadratic complexity)


IBM Cloud
Azure
AWS
IBM IAM
Azure IAM
AWS IAM
IBM Identity
Azure Identity
AWS Identity
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Azure Identity
IBM Identity
Azure Identity
AWS Identity
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS

Question?

In our organizations, how do we manage user identities?

(Answer: org. wide/universally)

Why don’t we treat our workload identities the same way?

Universal Workload identity

- For all workloads, there is a single organizational identity scheme
- 1 federation point - “Organization” authority

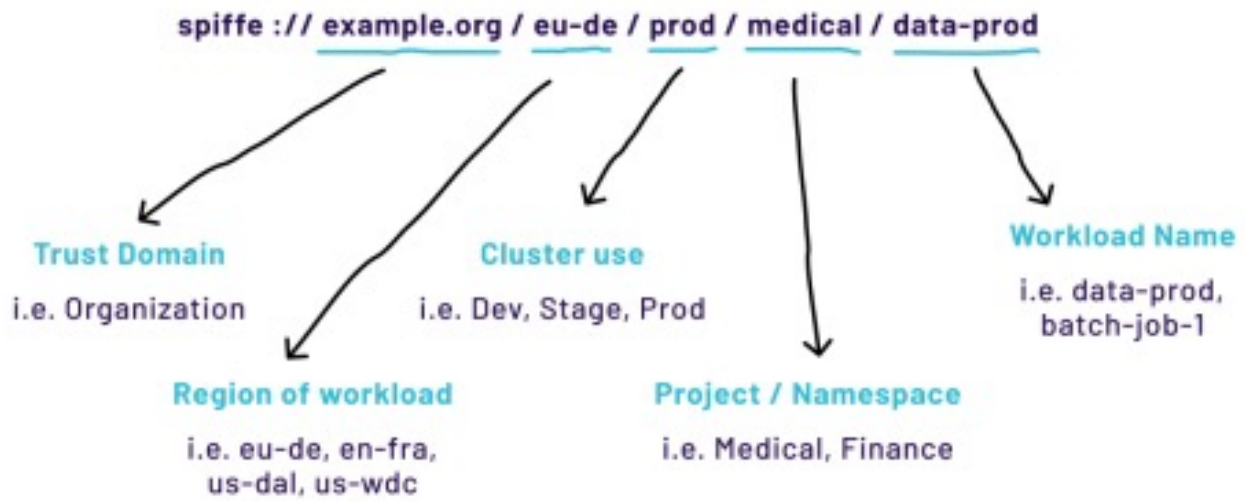
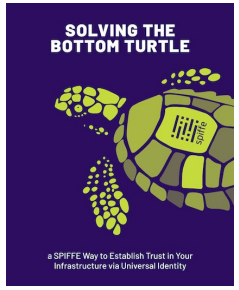
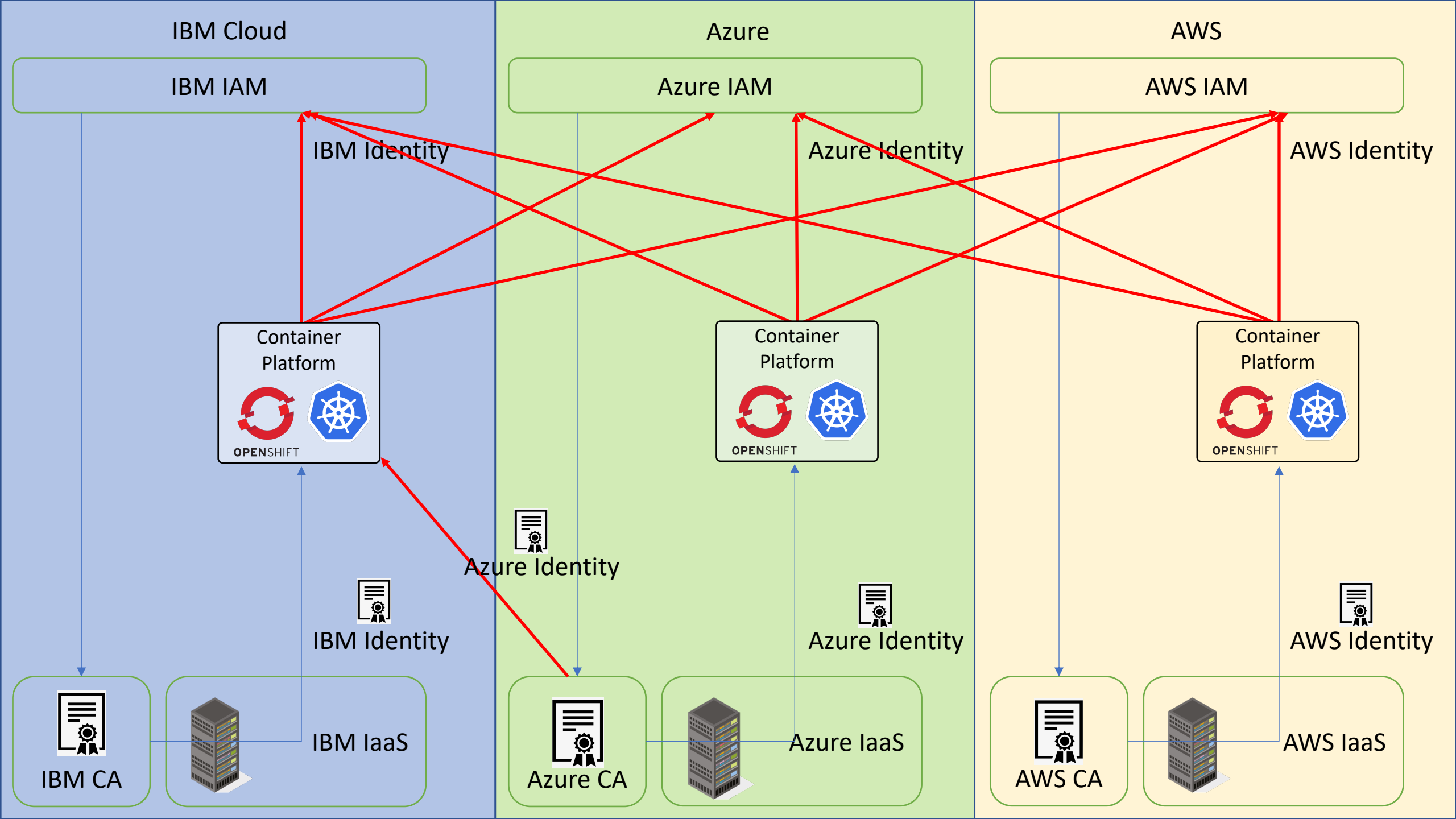
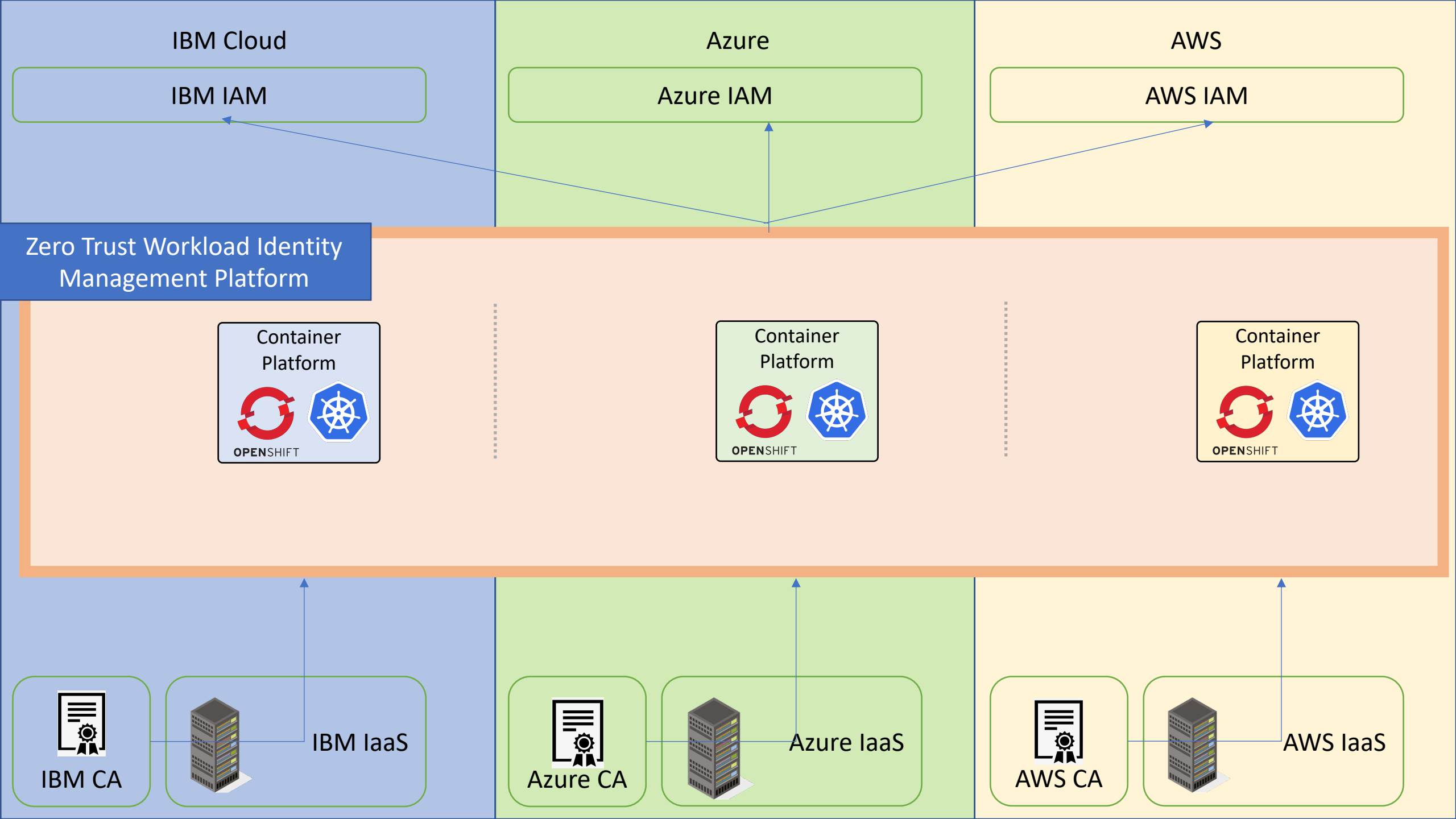


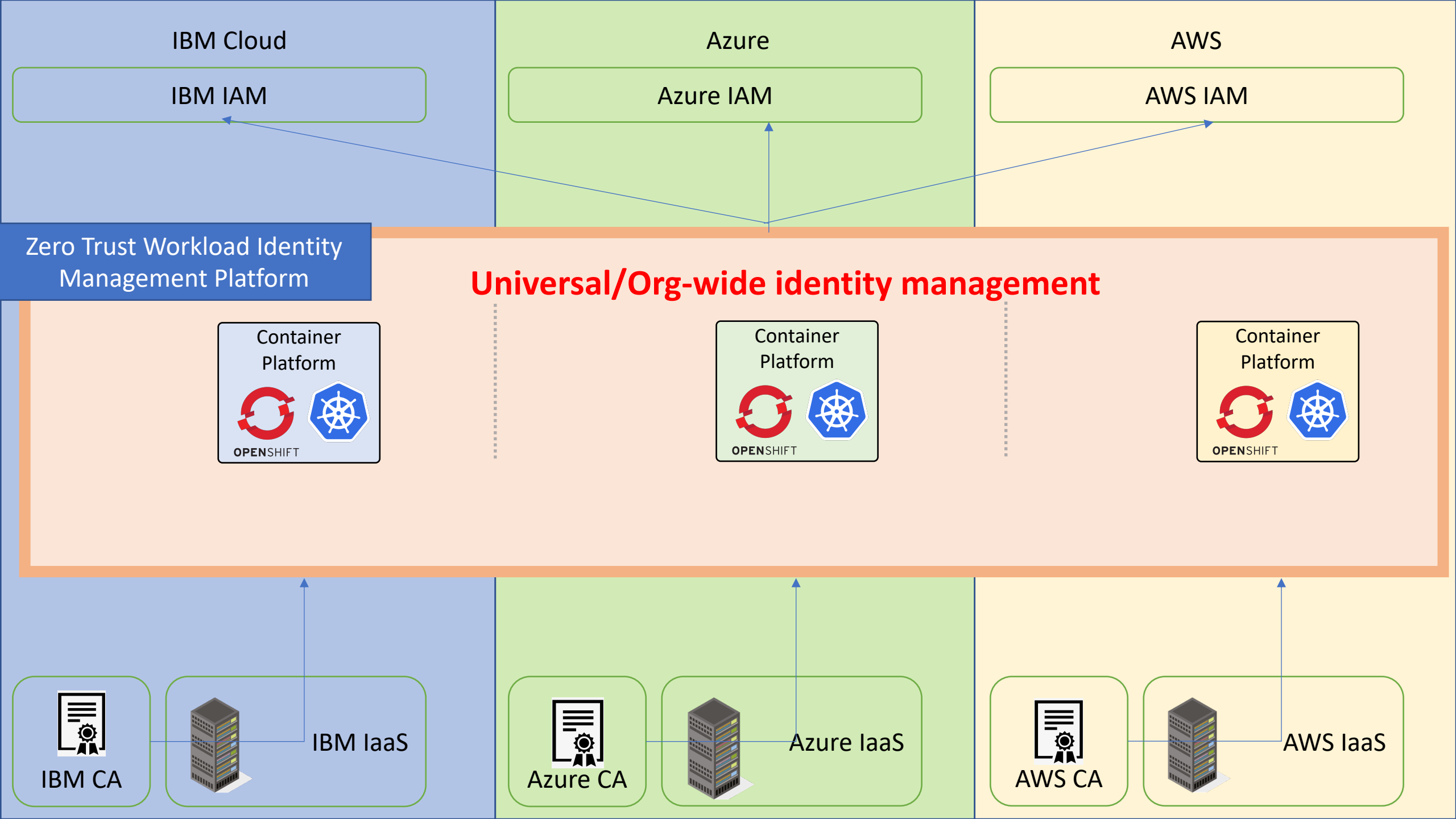
Fig. 8.1: Components of a SPIFFE ID and potential meanings at one organization.

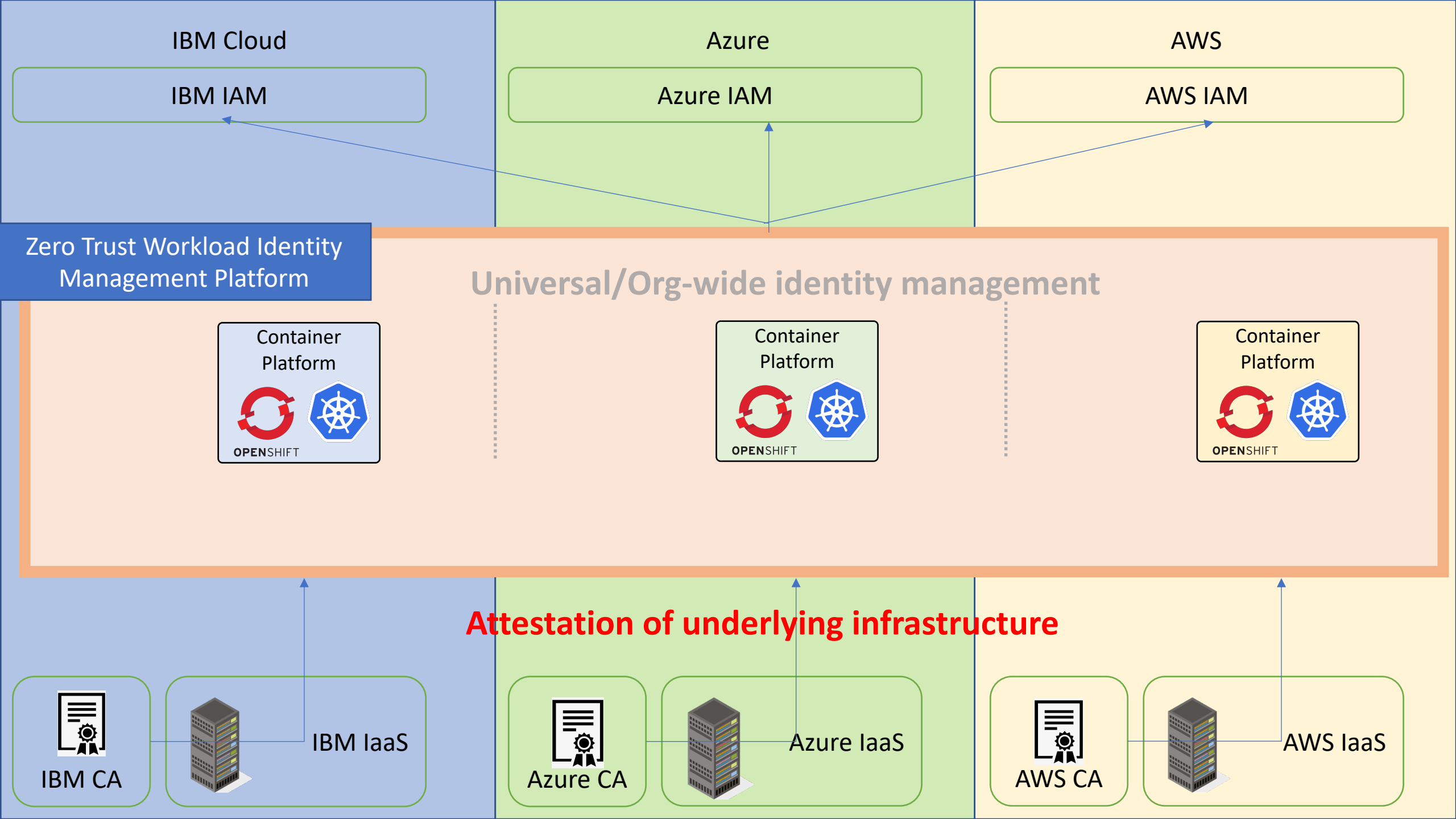
Adapted from https://spiffe.io/book:

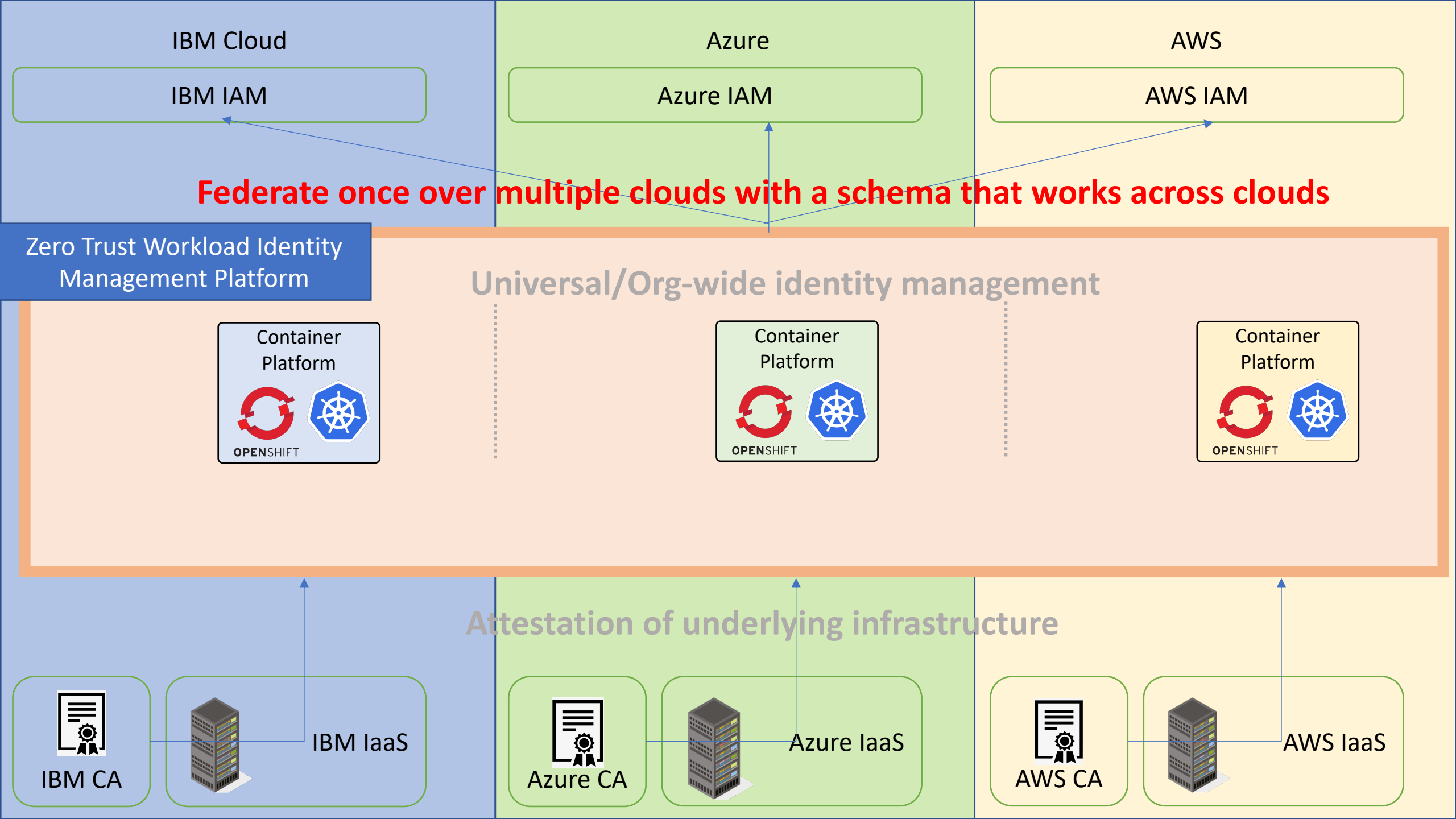



IBM Cloud
Azure
AWS
IBM IAM
Azure IAM
AWS IAM
IBM Identity
Azure Identity
AWS Identity
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Azure Identity
IBM Identity
Azure Identity
AWS Identity
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS


IBM Cloud
IBM IAM
Azure
Azure IAM
AWS
AWS IAM
Zero Trust Workload Identity Management Platform
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS


IBM Cloud
IBM IAM
Azure
Azure IAM
AWS
AWS IAM
Zero Trust Workload Identity Management Platform
Universal/Org-wide identity management
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS


IBM Cloud
IBM IAM
Azure
Azure IAM
AWS
AWS IAM
Zero Trust Workload Identity Management Platform
Universal/Org-wide identity management
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Attestation of underlying infrastructure
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS


IBM Cloud
Azure
AWS
IBM IAM
Azure IAM
AWS IAM
Federate once over multiple clouds with a schema that works across clouds
Zero Trust Workload Identity Management Platform
Universal/Org-wide identity management
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Container Platform
OPENSHIFT
Attestation of underlying infrastructure
IBM CA
IBM IaaS
Azure CA
Azure IaaS
AWS CA
AWS IaaS

IBM Cloud

IBM IAM

Azure

Azure IAM

AWS

AWS IAM

Federate once over multiple clouds with a schema that works across clouds

Zero Trust Workload Identity Management Platform

Universal/Org-wide identity management

Container Platform

Container Platform

Container Platform


spiffe


SPIRE

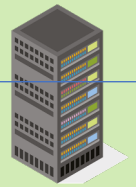

tornjak

Attestation of underlying infrastructure

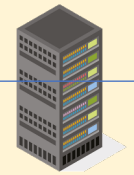

IBM CA


IBM IaaS


Azure CA


Azure IaaS


AWS CA


AWS IaaS

Zero Trust workload identity framework

CLOUD NATIVE COMPUTING FOUNDATION

spiffe

- Defines identity format
- Specifies how workloads securely obtain identity

SPIRE

- Implementation of SPIFFE
- Issuance/rotation of x509/JWT
- Provide zero trust attestation of workload & infrastructure
- Provide single point of federation with OIDC discovery

tornjak

- Control plane/UI for SPIRE
- Provides visibility/management for workload identities
- Together with k8s registrar, provides universal workload identity

Trade offer

- **You install:**
  - Zero Trust workload identity framework

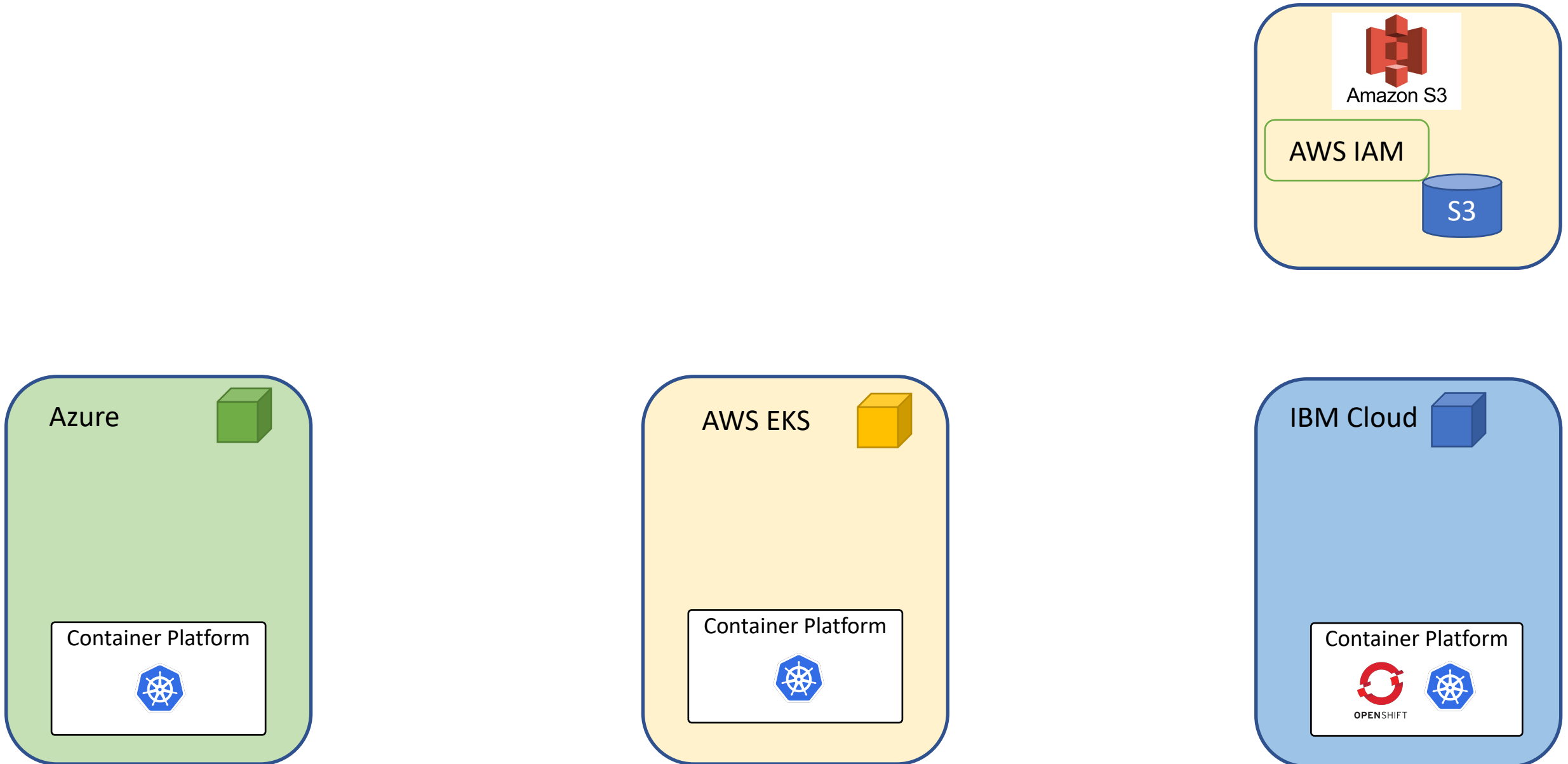
tornjak

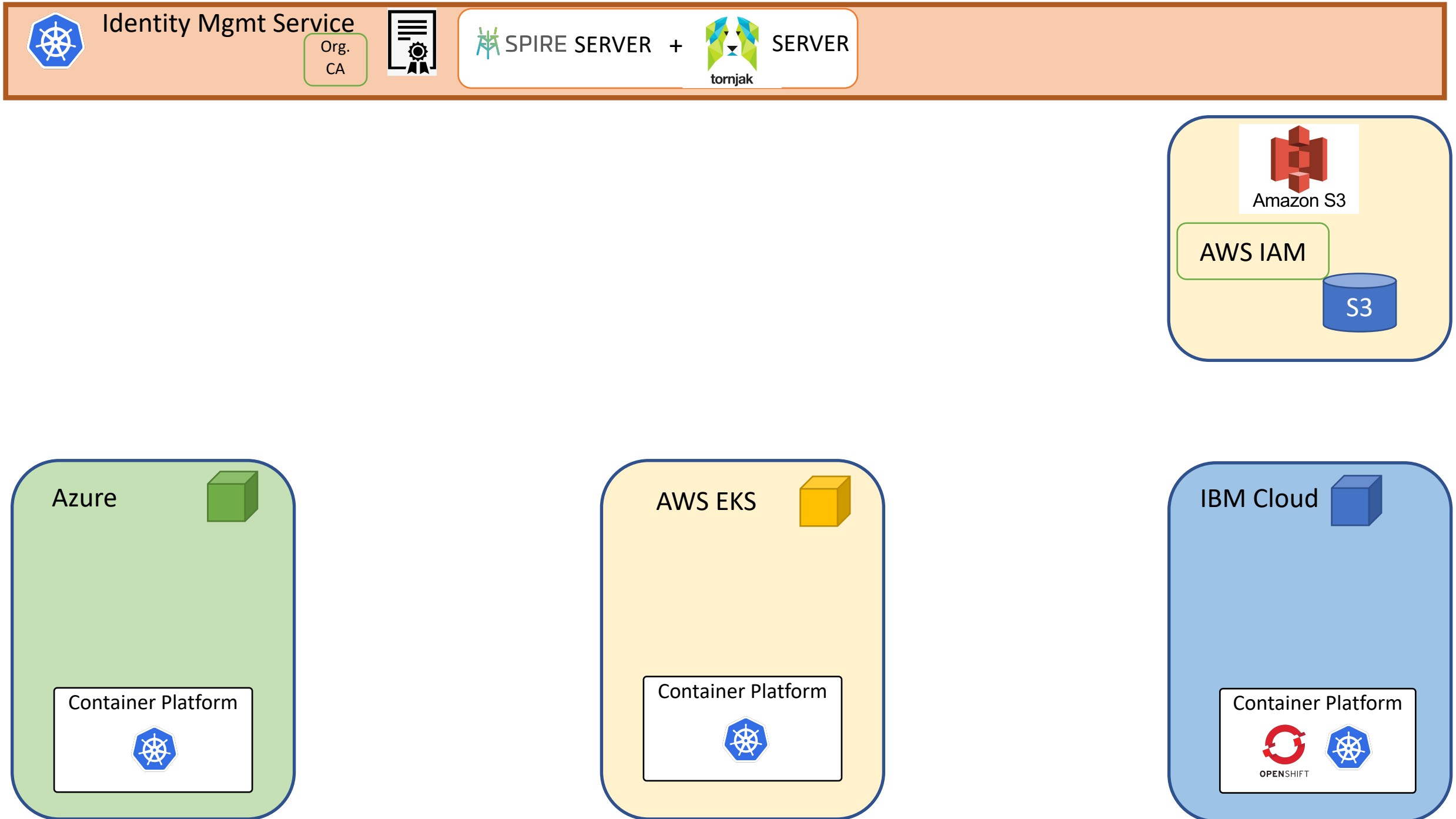
SPIRE

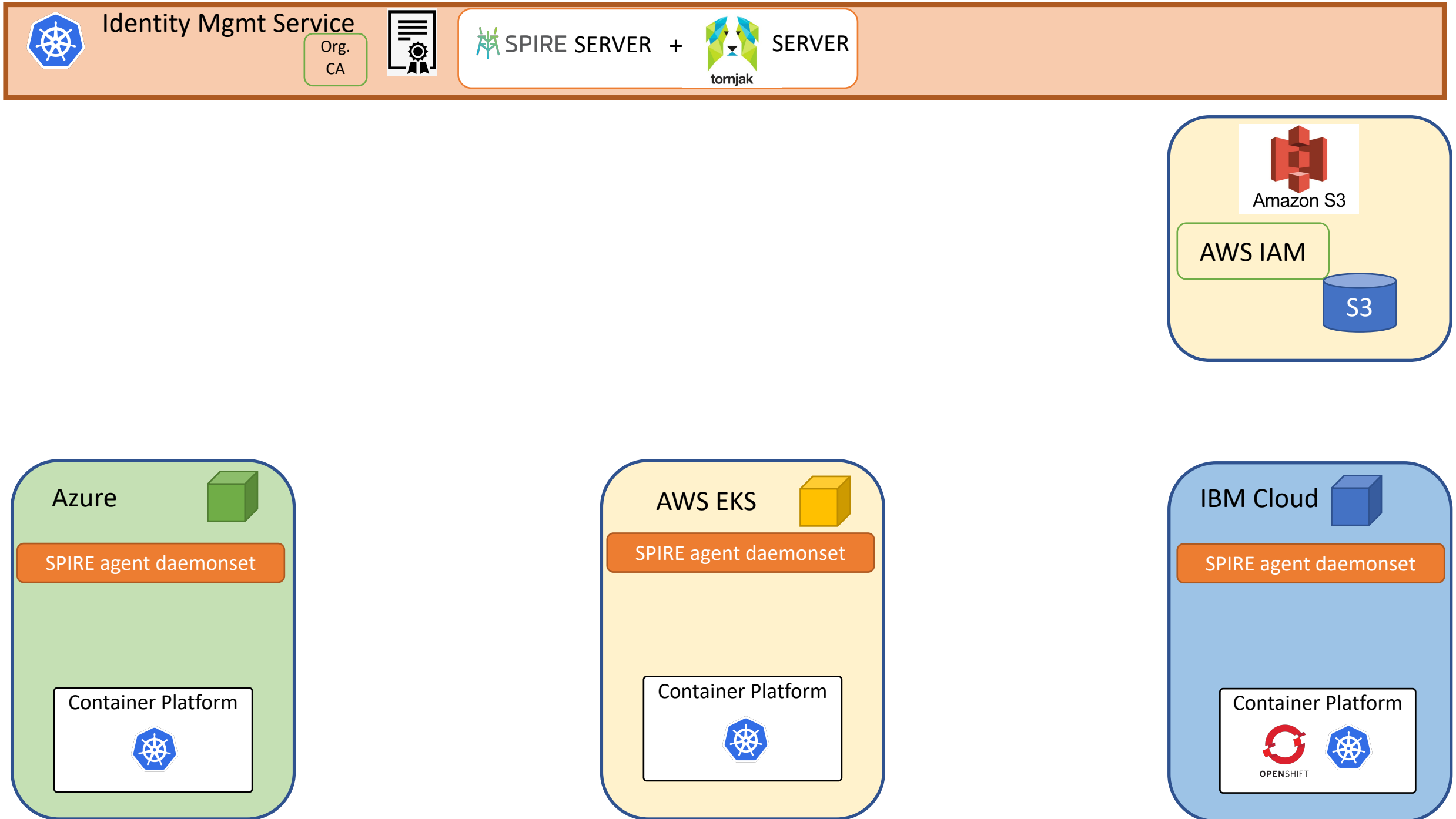
spiffe

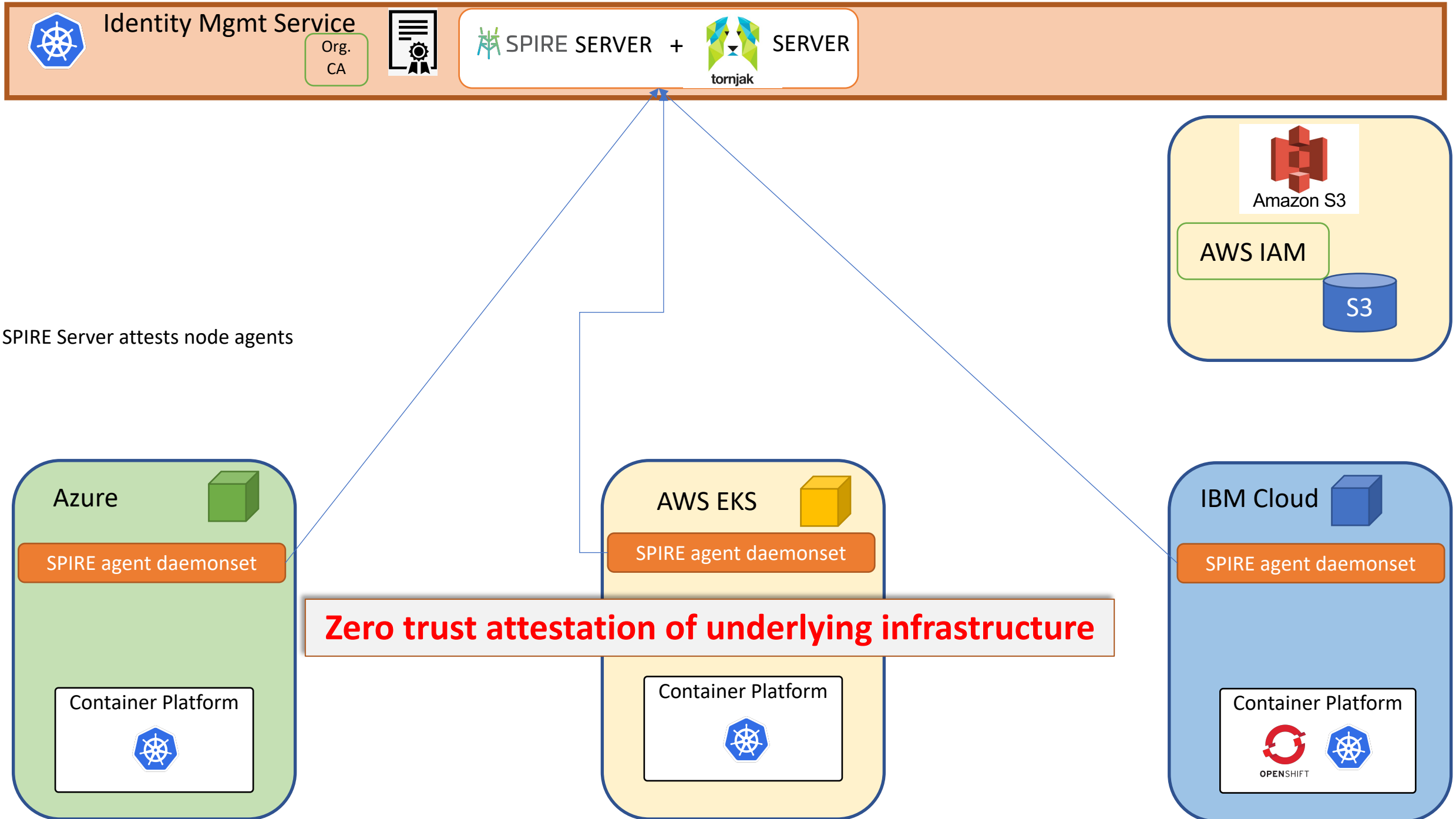
  - Define organizational workload identity scheme

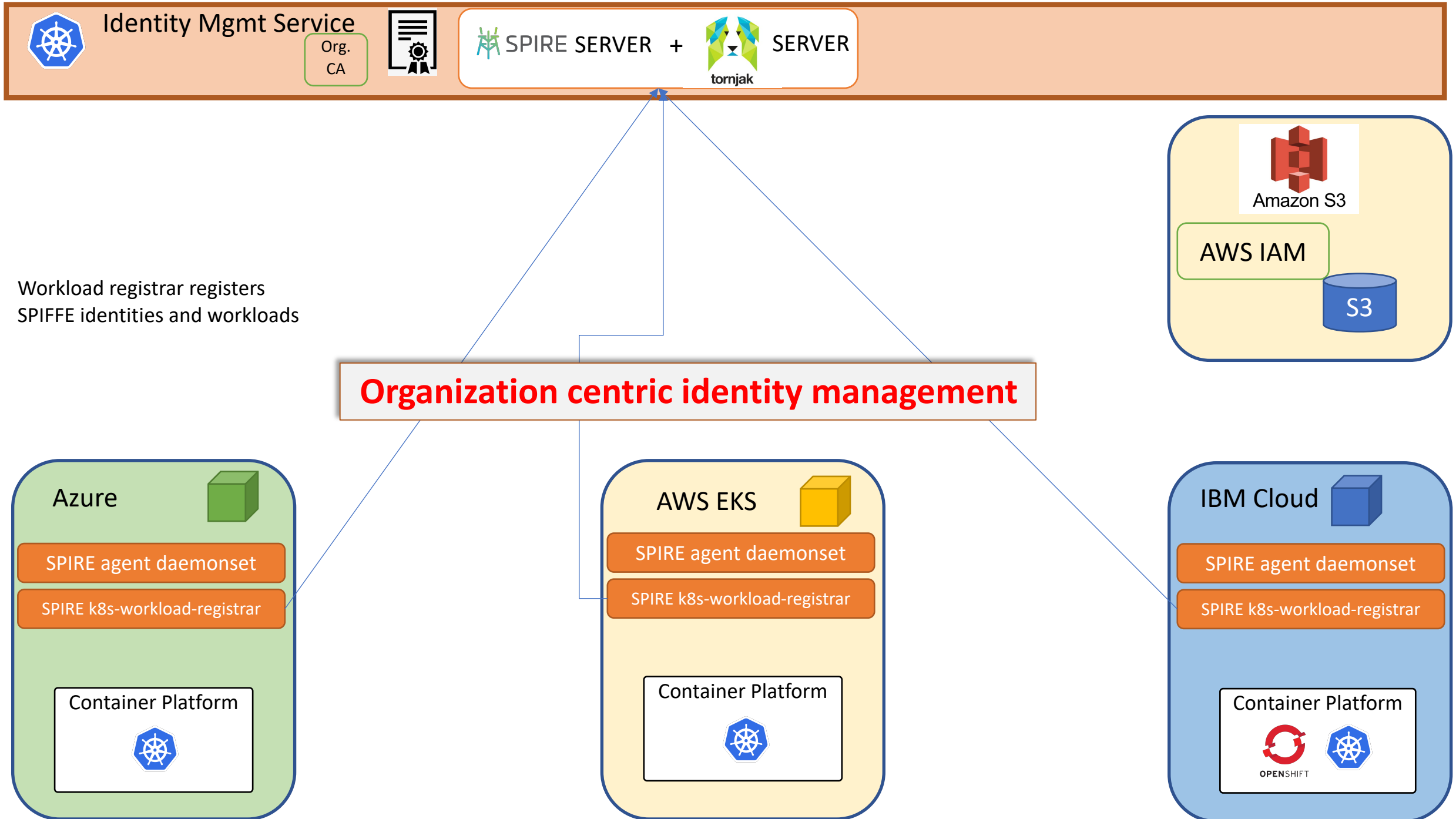
- **You receive:**
  - Zero Trust infrastructure attestation
  - Single configuration per cloud to federate all cloud access
  - **Centralized management of organization identities/policies to handle multi cloud complexity**
  - **Auditing of workload identities, attestation and policies**

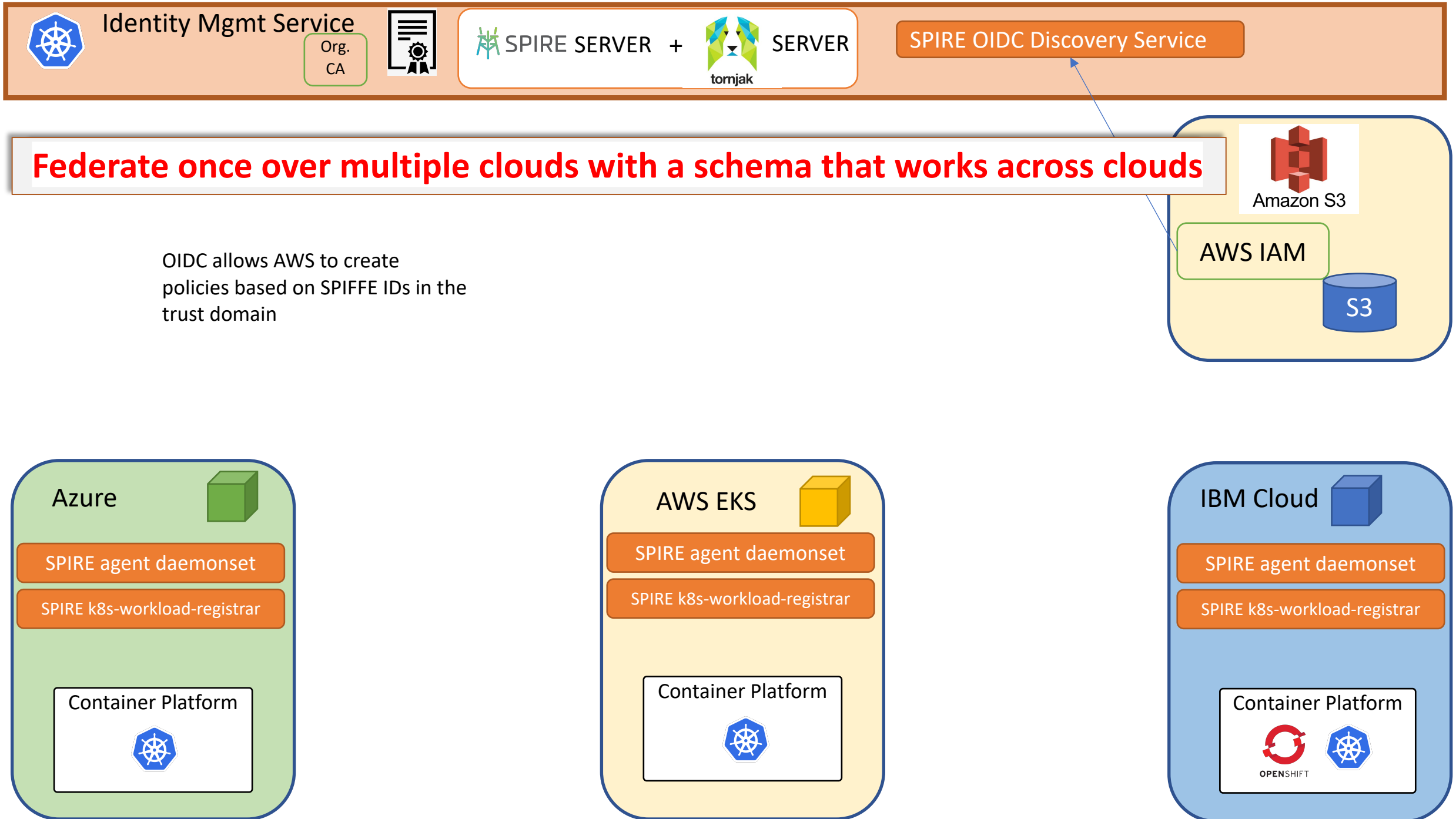

Amazon S3
AWS IAM
S3
Azure
Container Platform
AWS EKS
Container Platform
IBM Cloud
Container Platform
OPENSHIFT

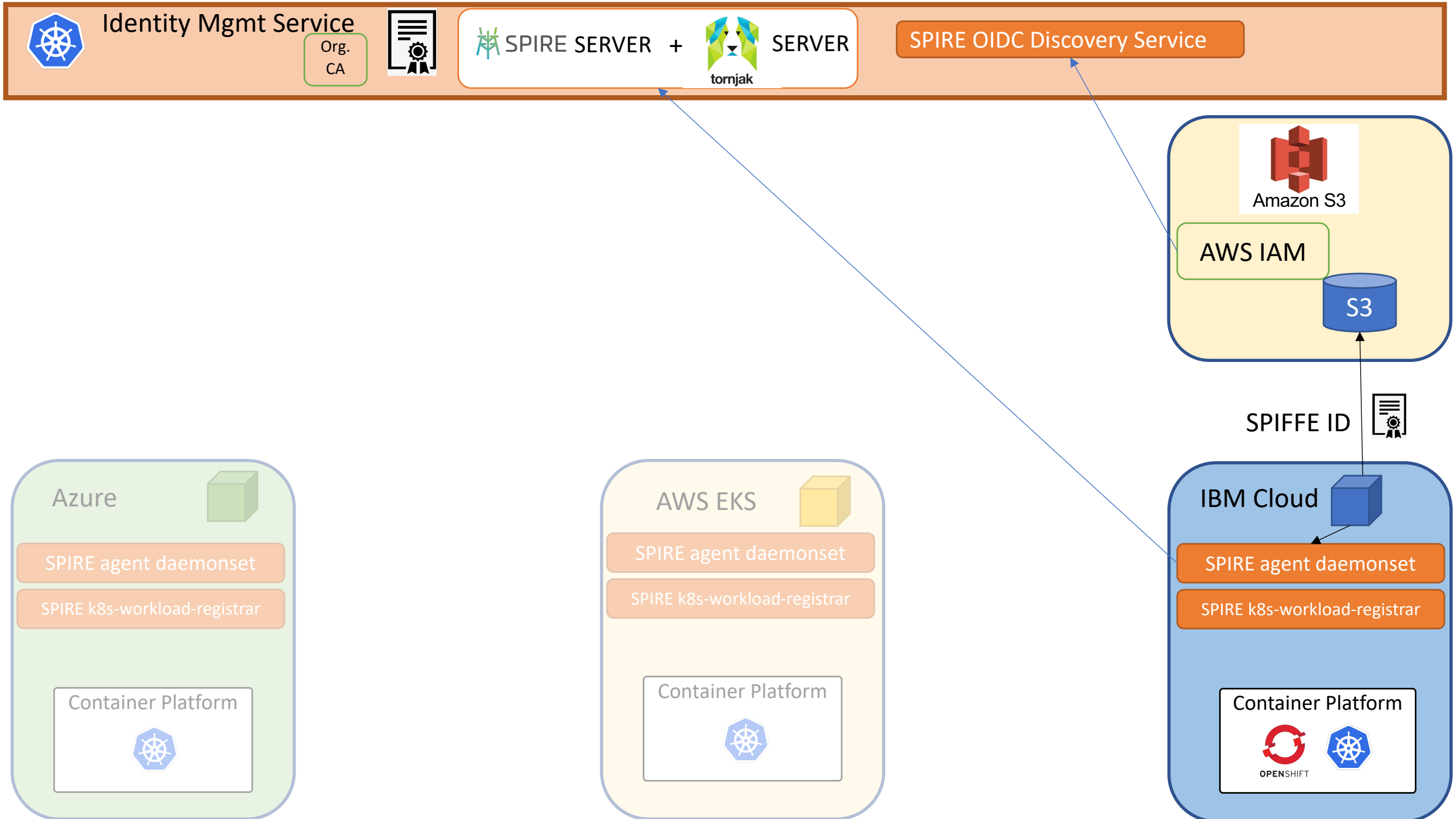

Identity Mgmt Service
Org.
CA
SPIRE SERVER +
tornjak
SERVER
Amazon S3
AWS IAM
S3
Azure
Container Platform
AWS EKS
Container Platform
IBM Cloud
Container Platform
OPENSHIFT


Identity Mgmt Service
Org. CA
SPIRE SERVER + tornjak SERVER
Amazon S3
AWS IAM
S3
Azure
SPIRE agent daemonset
Container Platform
AWS EKS
SPIRE agent daemonset
Container Platform
IBM Cloud
SPIRE agent daemonset
Container Platform
OPENSHIFT


Identity Mgmt Service
Org. CA
SPIRE SERVER + SERVER
tornjak
Amazon S3
AWS IAM
S3
SPIRE Server attests node agents
Azure
SPIRE agent daemonset
Container Platform
AWS EKS
SPIRE agent daemonset
Container Platform
IBM Cloud
SPIRE agent daemonset
Container Platform
OPENSHIFT
Zero trust attestation of underlying infrastructure


Identity Mgmt Service
Org. CA
SPIRE SERVER + tornjak SERVER
Amazon S3
AWS IAM
S3
Workload registrar registers
SPIFFE identities and workloads
Organization centric identity management
Azure
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
AWS EKS
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
IBM Cloud
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
OPENSHIFT


Identity Mgmt Service
Org. CA
SPIRE SERVER +
tornjak
SERVER
SPIRE OIDC Discovery Service
Federate once over multiple clouds with a schema that works across clouds
Amazon S3
AWS IAM
S3
OIDC allows AWS to create policies based on SPIFFE IDs in the trust domain
Azure
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
AWS EKS
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
IBM Cloud
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
OPENSHIFT


Identity Mgmt Service
Org. CA
SPIRE SERVER + SERVER
tornjak
SPIRE OIDC Discovery Service
Amazon S3
AWS IAM
S3
SPIFFE ID
Azure
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
AWS EKS
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
IBM Cloud
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
OPENSHIFT

Example of Universal Workload identity

spiffe://<TrustDomain>/region/<Region>/cluster_name/<ClusterName>/ns/<Namespace>/sa/<ServiceAccount>/pod_name/<PodName>

Access Policy for S3 bucket :

- Region must be in the US “us-*”
- Any cluster name
- Namespace is “mission”
- ServiceAccount is “elon-musk”
- PodName starts with “mars-mission”

"spiffe://openshift.space-x.com/region/us-east-1/cluster_name/tsi-kube01/ns/default/sa/elon-musk/pod_name/mars-mission-7874fd667c-72mtp"

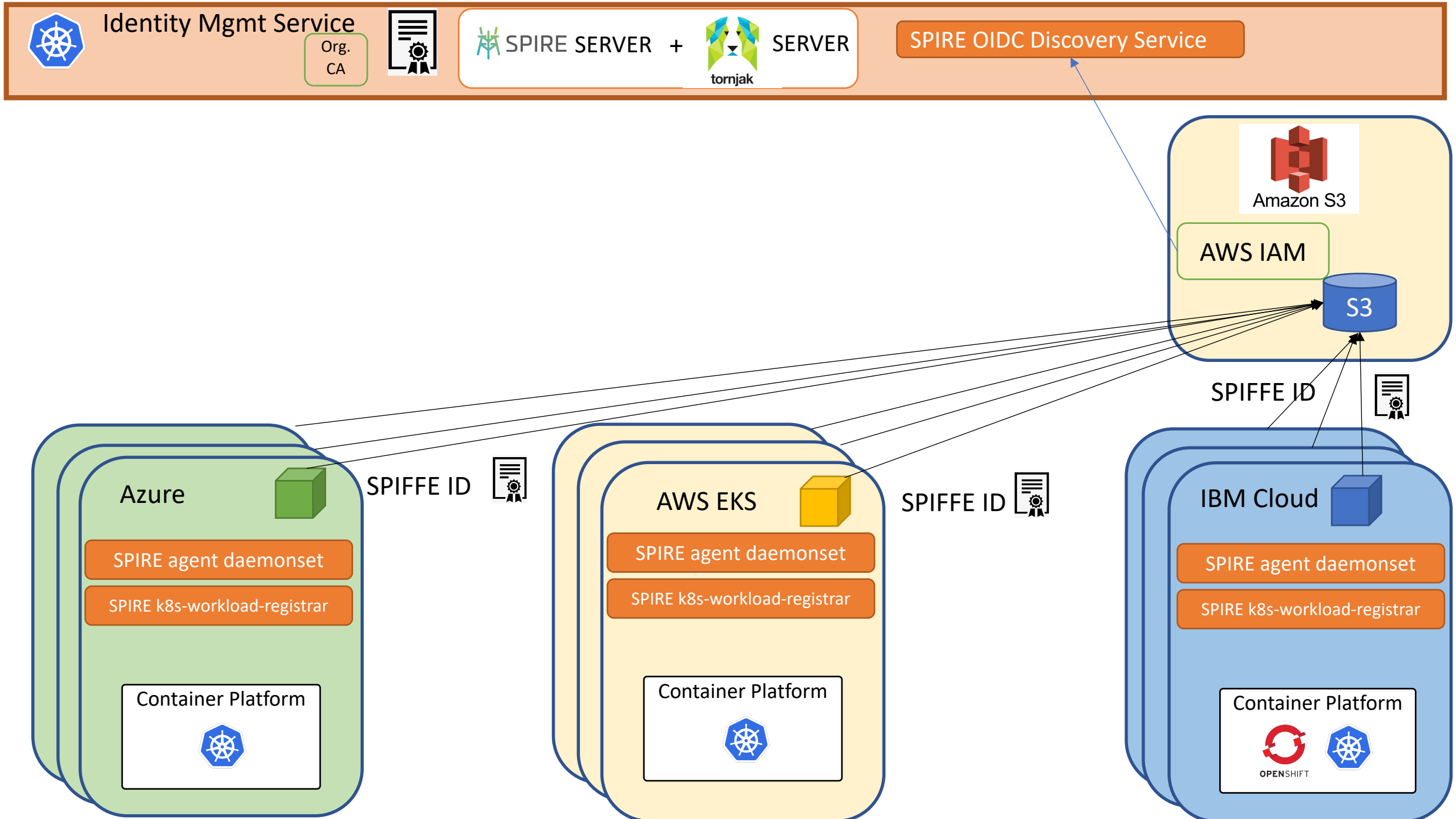

KubeCon | CloudNativeCon

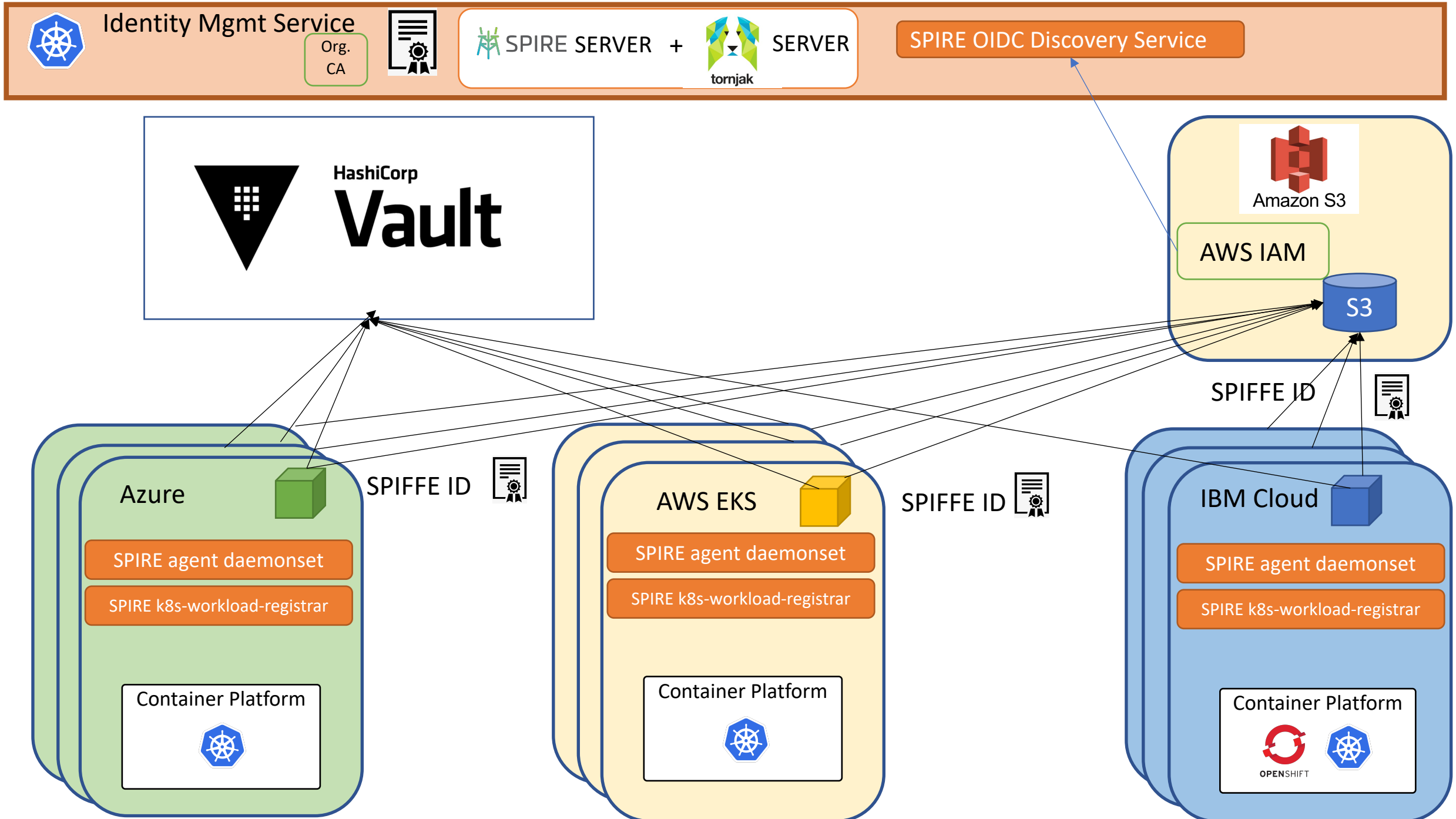
North America 2021

RESILIENCE

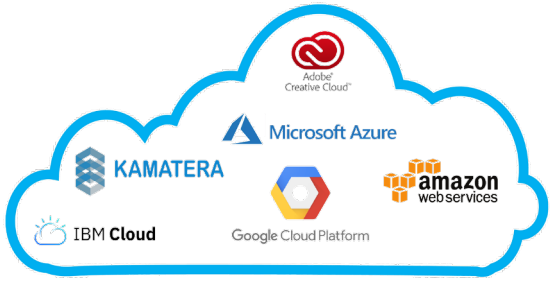
REALIZED

DEMO


Identity Mgmt Service
Org. CA
SPIRE SERVER + SERVER
tornjak
SPIRE OIDC Discovery Service
Amazon S3
AWS IAM
S3
SPIFFE ID
SPIFFE ID
SPIFFE ID
Azure
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
AWS EKS
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
IBM Cloud
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
OPENSHIFT


Identity Mgmt Service
Org. CA
SPIRE SERVER + tornjak SERVER
SPIRE OIDC Discovery Service
HashiCorp Vault
Amazon S3
AWS IAM
S3
SPIFFE ID
SPIFFE ID
SPIFFE ID
Azure
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
AWS EKS
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
IBM Cloud
SPIRE agent daemonset
SPIRE k8s-workload-registrar
Container Platform
OPENSHIFT

Interface to any IAM, SaaS, etc. via standard OIDC + policy framework



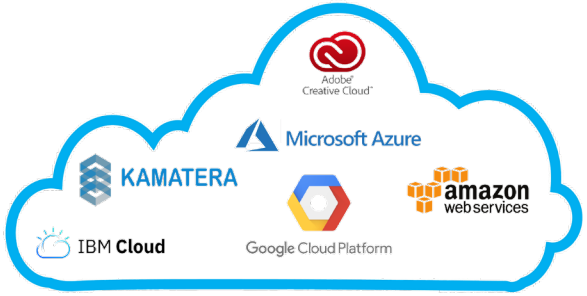
Zero Trust Workload Identity Management Platform

Container Platform

Container Platform

Container Platform

Interface to any cloud provider or attestation service



Call to Action

- Tornjak is now part of the CNCF / SPIFFE community (https://github.com/spiffe/tornjak)

- Tornjak is in active development! Come join us!
  (Looking for >=1 maintainer from another organization)

- Upcoming features in the roadmap
  - Registration RBAC OPA policy integration
  - Log integration – audit your SVID use/provisioning

- Give us feedback! https://github.com/spiffe/tornjak/issues/1
- Demo helm charts available at: https://github.com/IBM/trusted-service-identity
- Demo recordings: https://www.youtube.com/channel/UCmZKFwbge6WrUCP3OPss6mg

Questions?

tornjak

in SPIRE

Start herding your “cattle”

Brandon Lum

IBM Research

@lumjjb

Mariusz Sabath

IBM Research

@mrsabath

“Your shepherd, Louie, has retired. I’m Mr. Smathers. I will be your grazing-resource coördinator and flock welfare-and-security manager.”