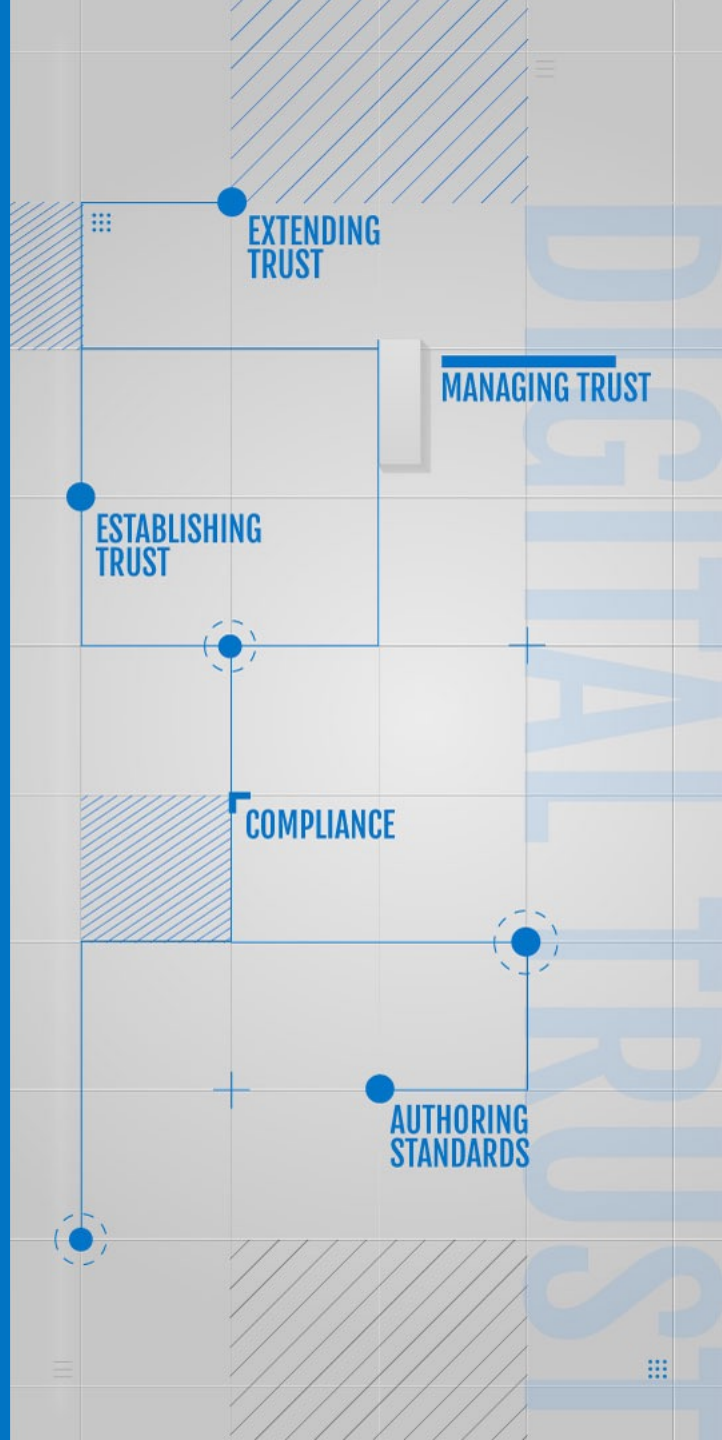
CLOUD NATIVE IDENTITY

Convergence of Public/Private PKI

digicert®



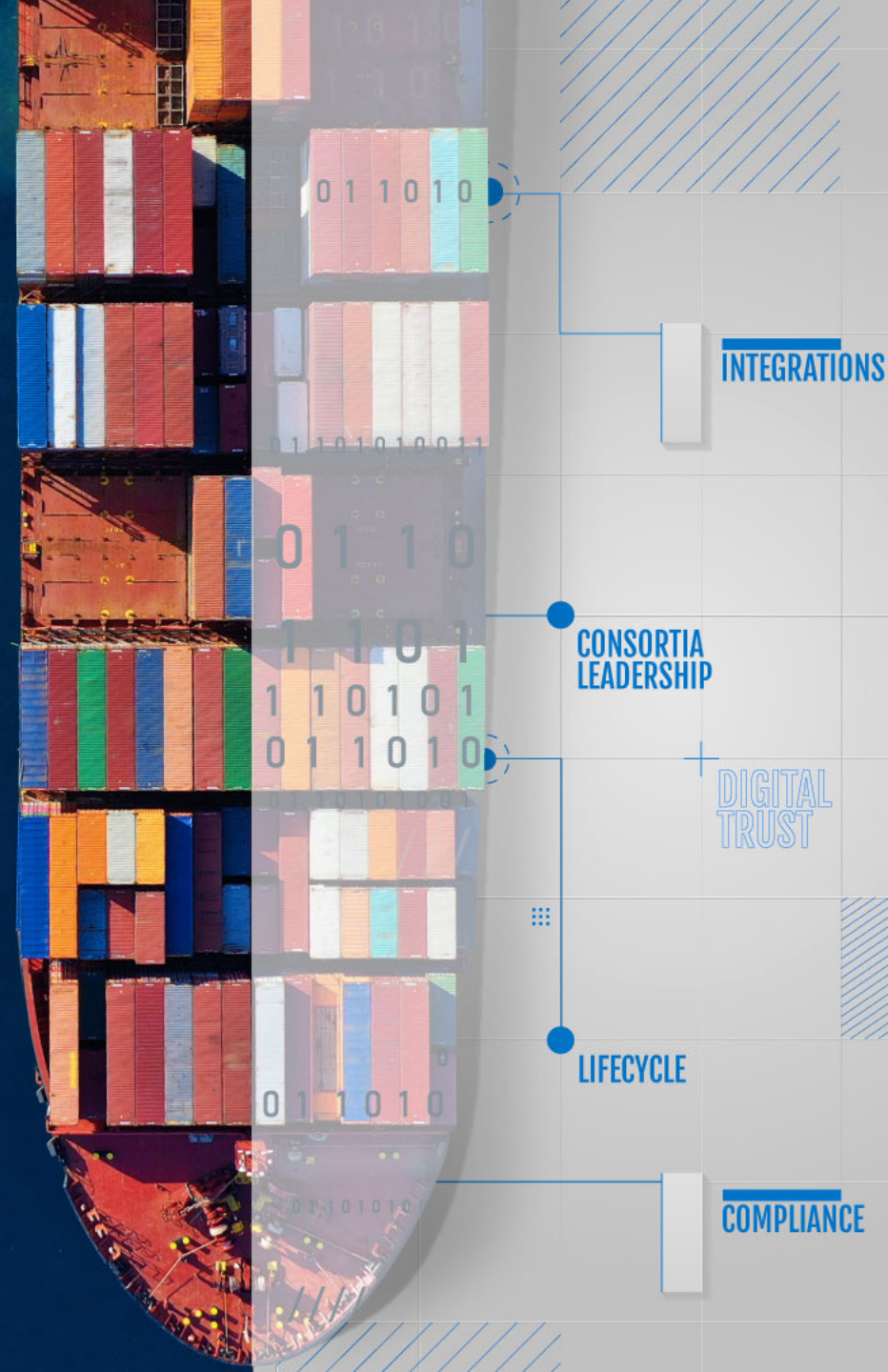
MEET YOUR PRESENTER

David Croston

Strategic Accounts Director
david.croston@digicert.com

CERTIFICATE MANAGEMENT IS REALLY IMPORTANT

- Everyone

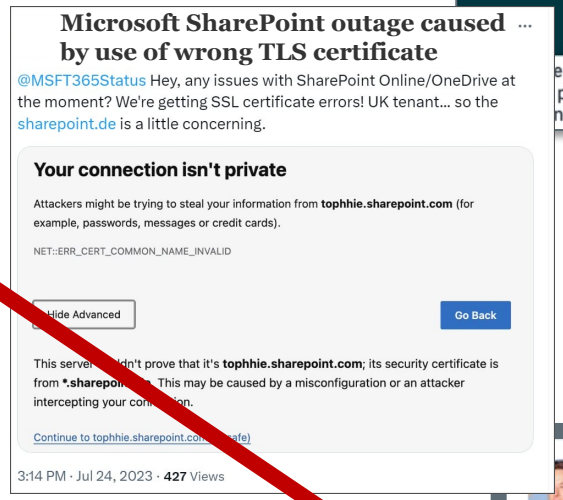


REALITY

58% suffered a certificate-management related **data breach***

57% said they have incurred costs upwards of **$100,000** USD per **outage***

According to respondents,
the top two **change drivers*** were:
1. Desire to **reduce the risk of data breaches**
2. **Gain visibility over certificates** and keys



* 2023 Forrester study

PKI MANAGEMENT IS A BUSINESS DRIVER

CONVERGED PKI

Managed PKI

SPEED & AGILITY

EFFICIENCY

RETURN ON INVESTMENT

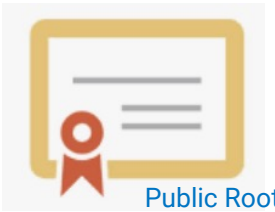
OUR UNIVERSE

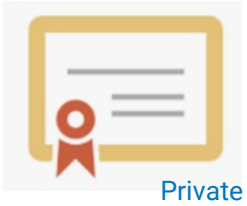
Your leadership is key to our collective success.

Credit: Space.com

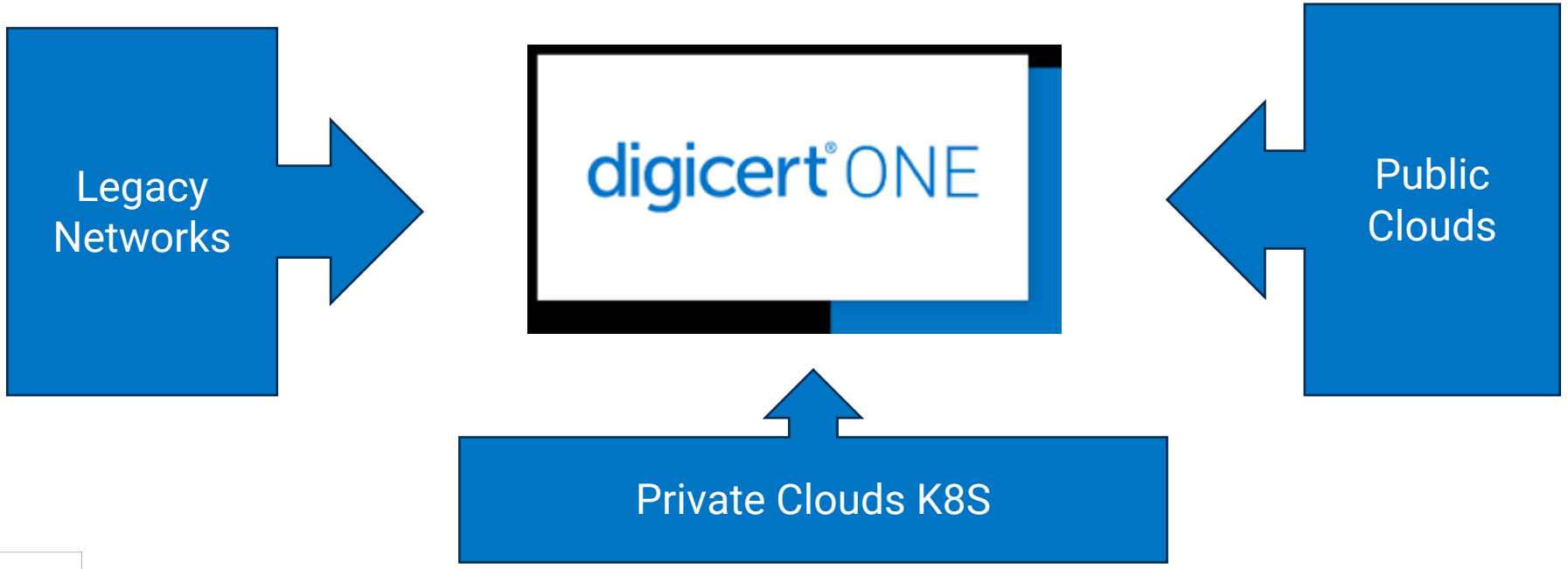
WHAT IS THE PKI 3.0 MOMENT

Disparate Certificate Roots


Public Root


Private Root


MSCA



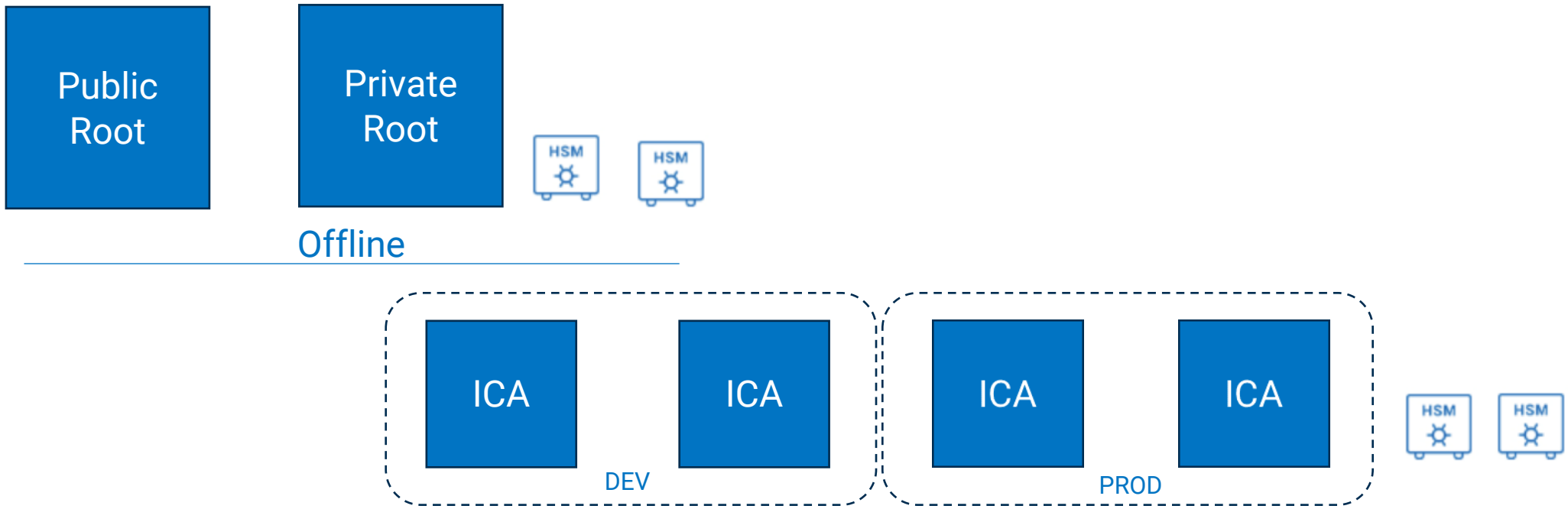
PROLIFERATION OF DYNAMIC SERVICES

Private & Public K8S

1 Million Containers and 100x Pods with key rotation every day/week/month

IMPORTANCE OF BEING A CA

It’s really important…



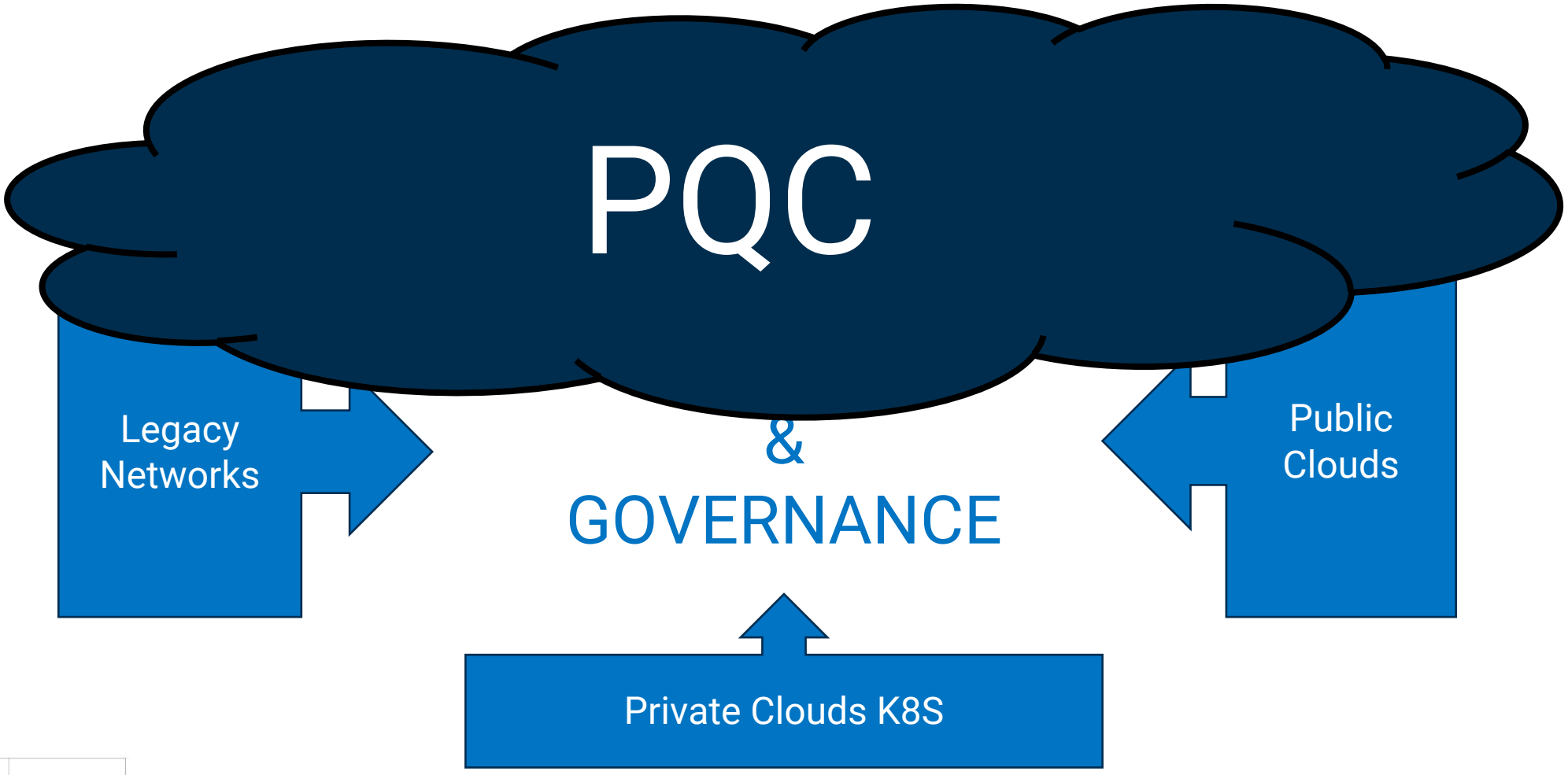
CAPEX/OPEX Savings, Extensibility, Control, Visibility, Flexibility, Speed, Crypto Agility…

MY COMPASS

and your sextant

QUANTUM SAFE

Do you have a defined timetable?



MAKE A PLAN

We are here to help

TAKING STEPS TO BECOME MORE CRYPTO AGILE

- **Discovery:** The first step to gain visibility & control of certificate environment
- **Automation**: Save time & reduce risks by eliminating manual renewal & installation process
- **Managed PKI**: Transition from legacy PKI for centralized management & control
- **Key Management:** Follow secure key management practices; perform key ceremony
- **Policy & Compliance:** Define and embed policies & practices in your PKI environment

CNCF GRADUATE PROJECTS

spiffe

Secure Production Identity Framework for Everyone

SPIRE

SPIFFE ID:

... a URI

... with a spiffe scheme

... where the authority component identifies the trust domain

... and the path component is an entity within the trust domain

spiffe://trust-domain/entity

SPIFFE and SPIRE provide a uniform identity control plane across modern and heterogeneous infrastructure.

SVID

SPIFFE Verifiable Identity Document (SVID)

SVID:

... a document

... containing a SPIFFE ID

... signed by an authority in the trust domain

... defined for both X.509 certificates and JWT

SPIFFE Bundle:

... a collection of authorities

... scoped to a trust domain

... used to validate SVIDs belonging to the trust domain

... also called the "trust domain bundle" or just "trust bundle"

TRUST DOMAIN

spiffe://trust-domain/entity — namespace

spiffe://prod.trust-domain/entity — security boundary

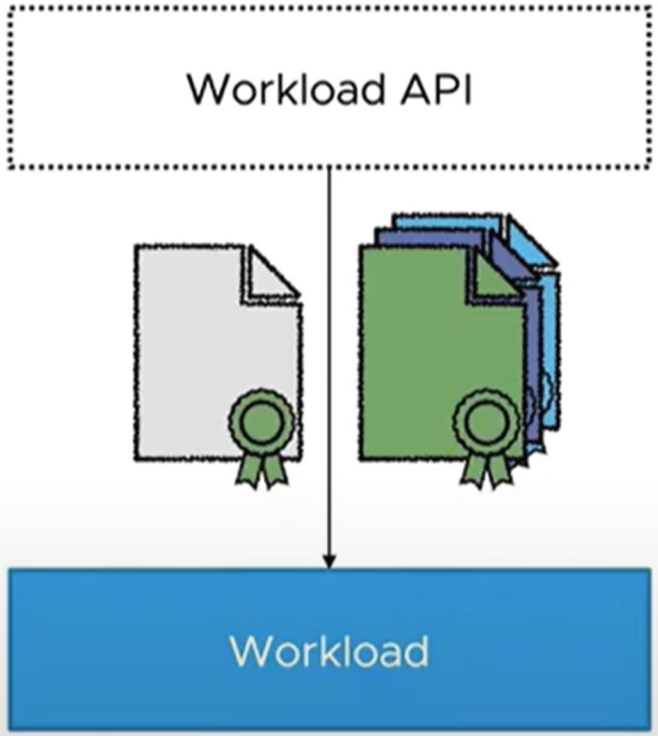
spiffe://sales.trust-domain/entity — **administrative domain**

spiffe://accounts.trust-domain/entity — different administrative domain

anchored by one or more CAs

SPIFFE WORKLOAD API

Defining Secure Workflow

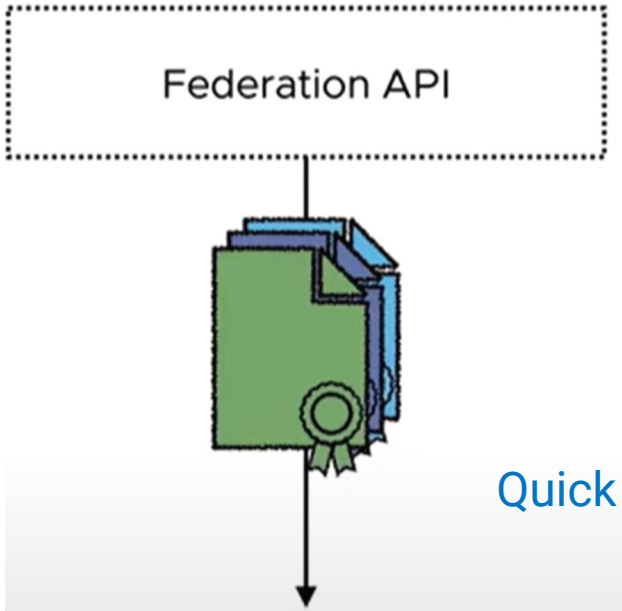


Workload API:

- … services (unauthenticated) workloads
- … provides X.509 and JWT SVIDs
- … provides bundles for authenticating SVIDs
- … streams updates
- … solves the secret-zero problem for workloads

SPIFFE FEDERATION API

One-way Requests for Trust

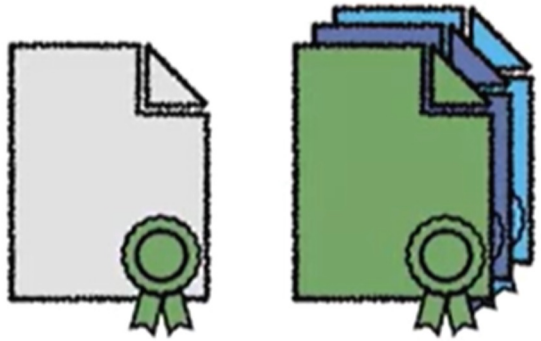


Federation API:

- … interoperable way to obtain SPIFFE bundles
- … facilitates authenticating SVIDs from foreign trust domains
- … one-way

Quick method for Trust Domains to exchange key material

SPIFFE FRAMEWORK FOR DYNAMIC TRUST



Workload API

Federation API

SPIFFE:

... cryptographic

... verifiable

... secret-zero

... frequently rotated

... federate-able

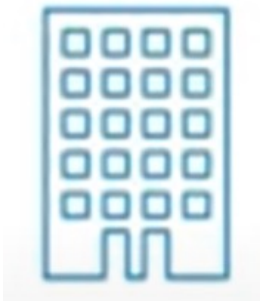
... namespaced

... uniform identity

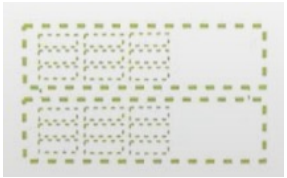
SPANNING ALL ENVIRONMENTS

Cloud

Organization



Bare Metal



VMs

Containers

SPIFFE implementation to manage workload identity

digicert®

TRUST SUMMIT ROAD SHOW