BUOYANT'S
SERVICE MESH
ACADEMY

The creators of
LINKERD

Linkerd with external CAs using Vault

Flynn, Technical Evangelist for Linkerd

@flynn (slack.linkerd.io)

@BuoyantIO

@kflynn



What's on the agenda?



Workshop with a bit of background first!

- (Quick) Intro to certificates and certificate hierarchies
- How identity and certificates work together for Linkerd
- (VERY quick) Intro to Vault and cert-manager
- Hands-on workshop!



LINKERD

Workshop Info

Follow along! **https://github.com/BuoyantIO/service-mesh-academy**
(in the **certificates-with-vault** directory)

Tools we'll use:

- Kubernetes cluster and the **kubectl** command
- **linkerd** – **https://linkerd.io/2/getting-started/**
- **step** – **https://smallstep.com/docs/step-cli/installation**
- **helm** – **https://helm.sh/docs/intro/quickstart/**
- **jq** – **https://jqlang.github.io/jq/**
- **bat** – **https://github.com/sharkdp/bat**

Also recommended: **demosh** from **https://github.com/BuoyantIO/demosh**



KUBE CRASH

Crash Courses on Cloud Native Tech

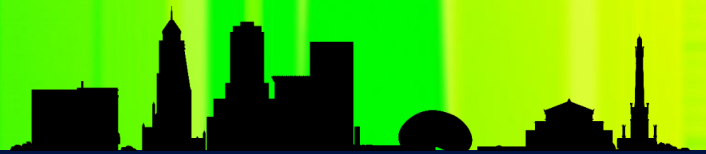
Multi-Cluster Deployments at Scale

Virtual. Free. 100% open source-focused conference.

October 18, 2023

Register at **kubecrash.io**

Follow us on Twitter for updates @KubeCrash





BUOYANT

Creators of LINKERD

Join Buoyant's Linkerd Forum!

Searchable, long-lived help threads and technical content.
(Slack is great, but messages die after 90 days.)
linkerd.buoyant.io



BUOYANT'S

SERVICE MESH ACADEMY

The creators of LINKERD



Fundamentals of the Service Mesh Online Course + Certification

With hands-on LINKERD labs at learn.buoyant.io









LINKERD

Enterprise early access

We're adding a few more **early access slots** for our enterprise Linkerd distro.

- SLAs around CVE remediation, SBOMs, continuously-scanned images
- **Cost-aware routing,** FIPS support
- Security policy generation and auditing
- Gitops-compatible lifecycle automation
- And lots more

Send William a DM on the Linkerd Slack

BUOYANT

Creators of LINKERD

BUOYANT | SERVICEMESH ACADEMY

Linkerd, Argo, and Gateway API



Regina Scott
Argo CD Maintainer



Flynn
Tech Evangelist

Sign up at
buoyant.io/sma

Thursday, October 26, 2023

9 am PT | 12 am CT | 6pm CET

Intro: Certificates



Much more information about all this stuff is available in the Buoyant mTLS guide:

`https://buoyant.io/mtls-guide`

LINKERD

Background: Public-key Cryptography

Public-key (asymmetric) cryptography forms the basis of trust in Linkerd

- Instead of "a key" use a keypair: a public key and a private key
  - What the public key encrypts, the private key decrypts
  - What the private key encrypts, the public key decrypts
  - Given just the public key, recovering the private key is "impossible"
- If Alice encrypts something with Bob's public key, only Bob can read it…
  - …because Bob is the only one with Bob's private key
- If Alice encrypts something with her own private key, only she could have written it…
  - …because Alice is the only one with Alice's private key
  - (This is very common in practice: encrypting a hash of some data with one's private key is called signing it.)



LINKERD

Background: Public-key Cryptography

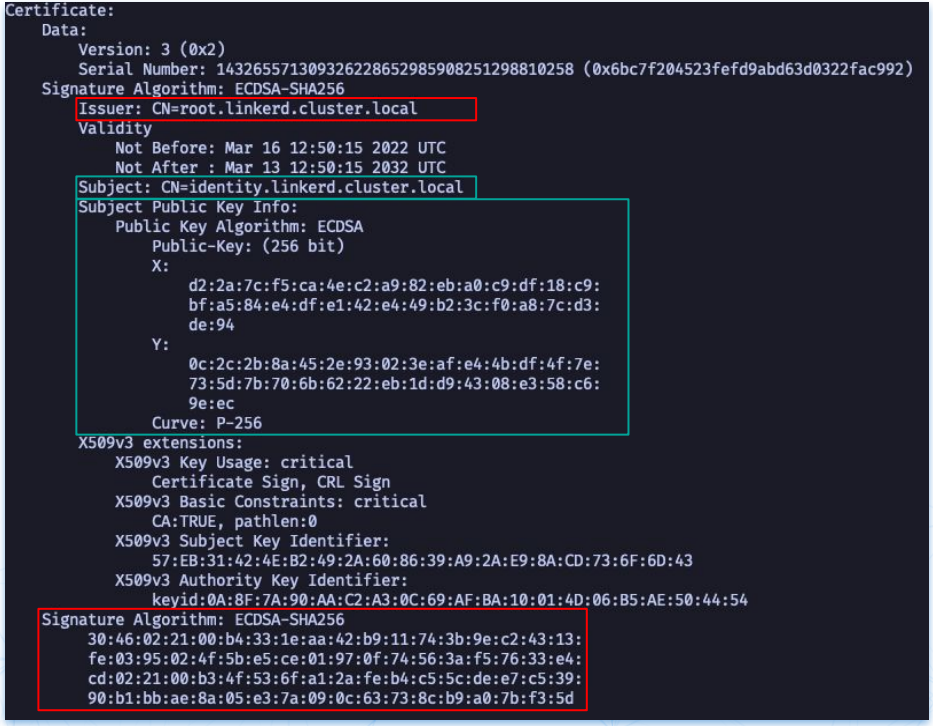
Public-key (asymmetric) cryptography forms the basis of trust in Linkerd

- ➔ Public-key cryptography allows safe communication and authentication, even without prior knowledge
  - mTLS relies on this
  - Linkerd authentication relies on mTLS
- ➔ To make this work:
  - Private keys must be kept private: they are the basis of identity
  - Public keys should be shared with the world to allow easy verification
- ➔ Problem: actually keeping track of public keys is a pain. Enter the certificate.



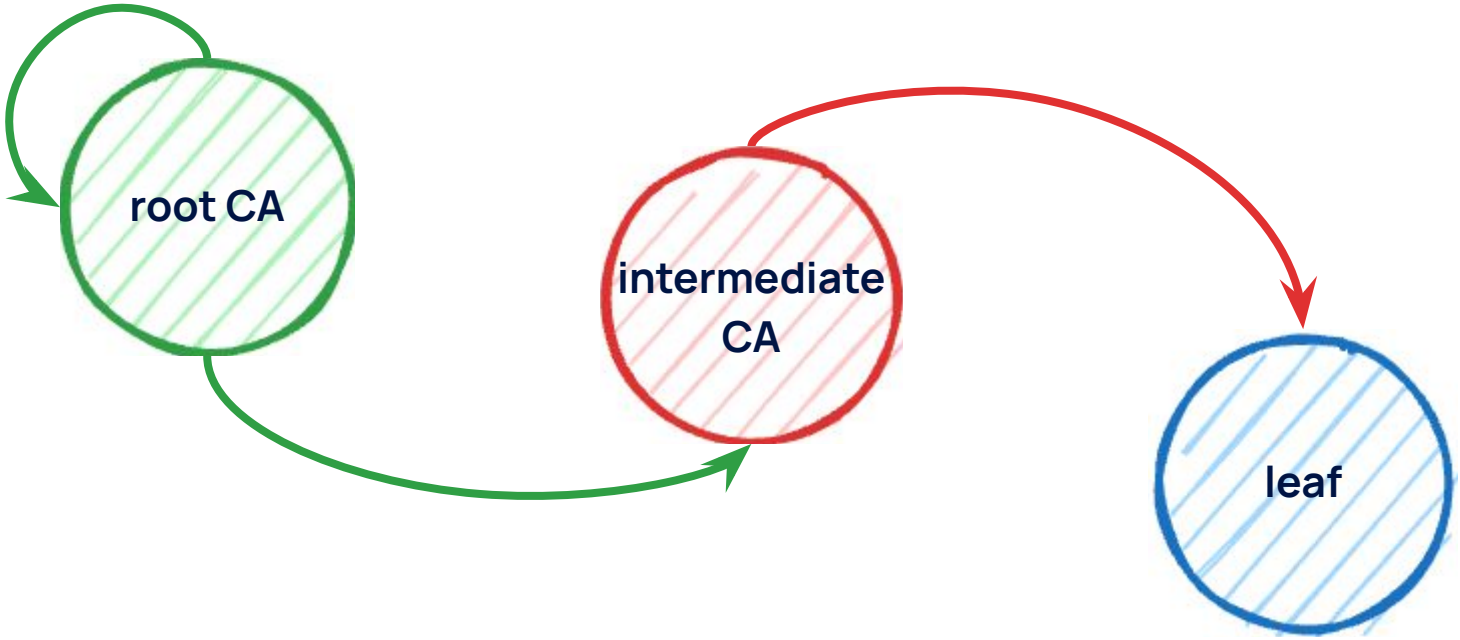
Background: Certificates

- X.509 certificates are data structures that bind a *subject* (really a name) to a keypair.
- Only public information is in a certificate – they're safe to share.
- Certificates are signed to prevent them from being spoofed, so they can be trusted.
- Rotation regenerates the keypair so that you're not relying on any one key for too long.



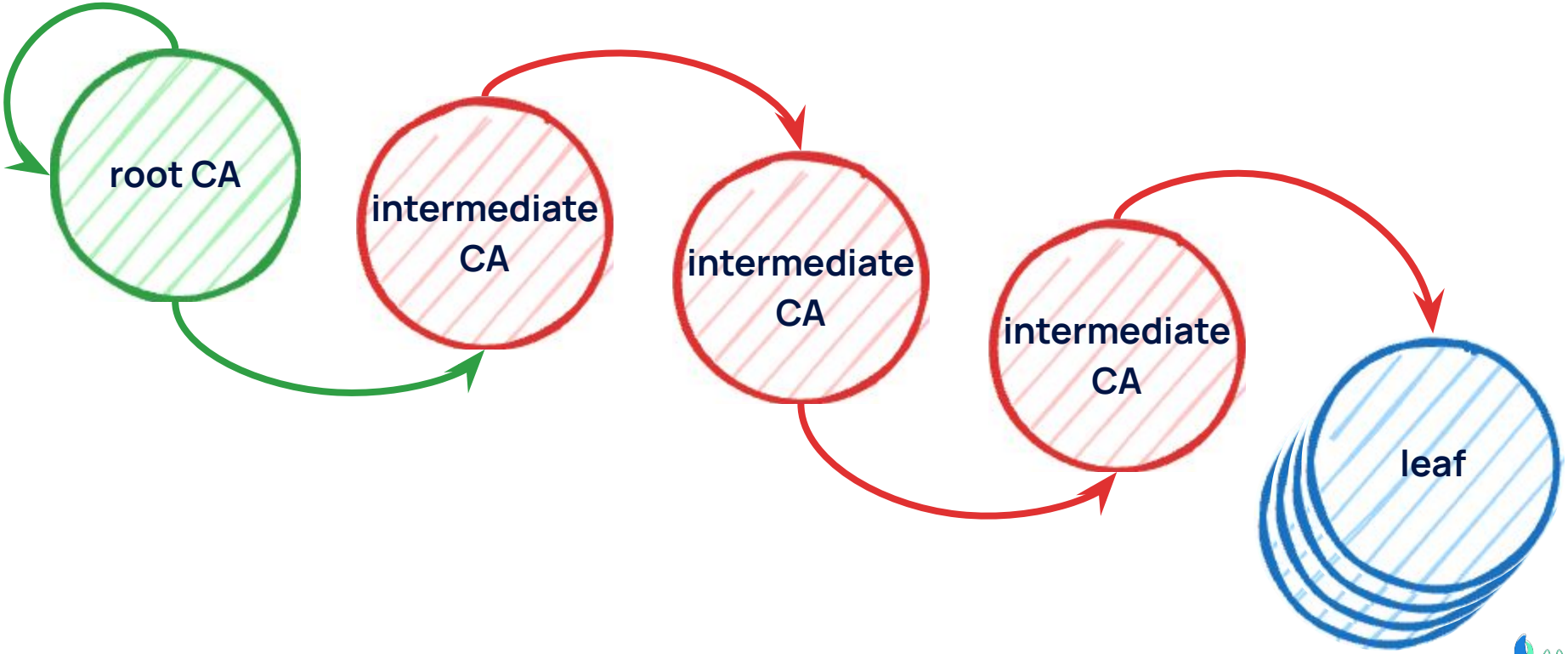
LINKERD

Certificate Hierarchy



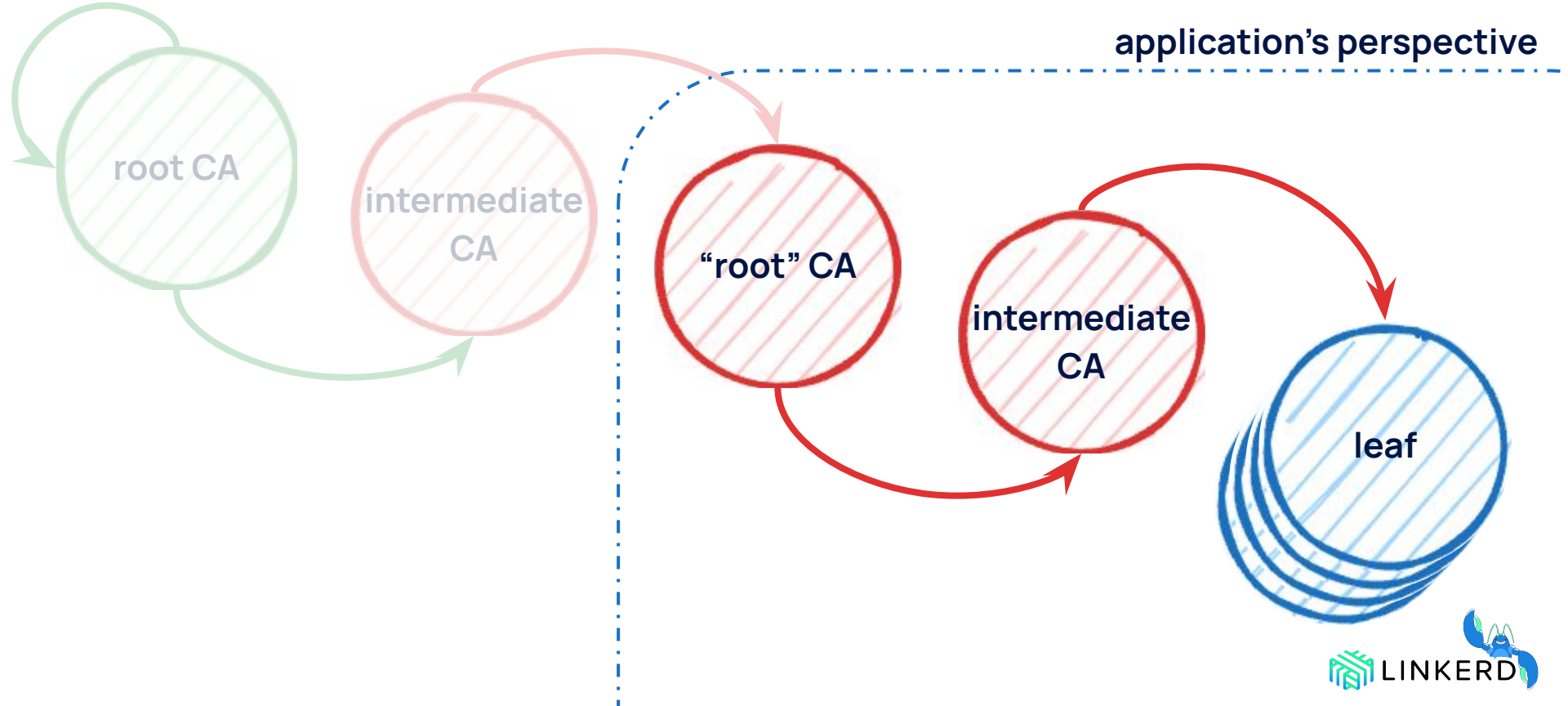
LINKERD

Certificate Hierarchy



LINKERD

Certificate Hierarchy: Delegation

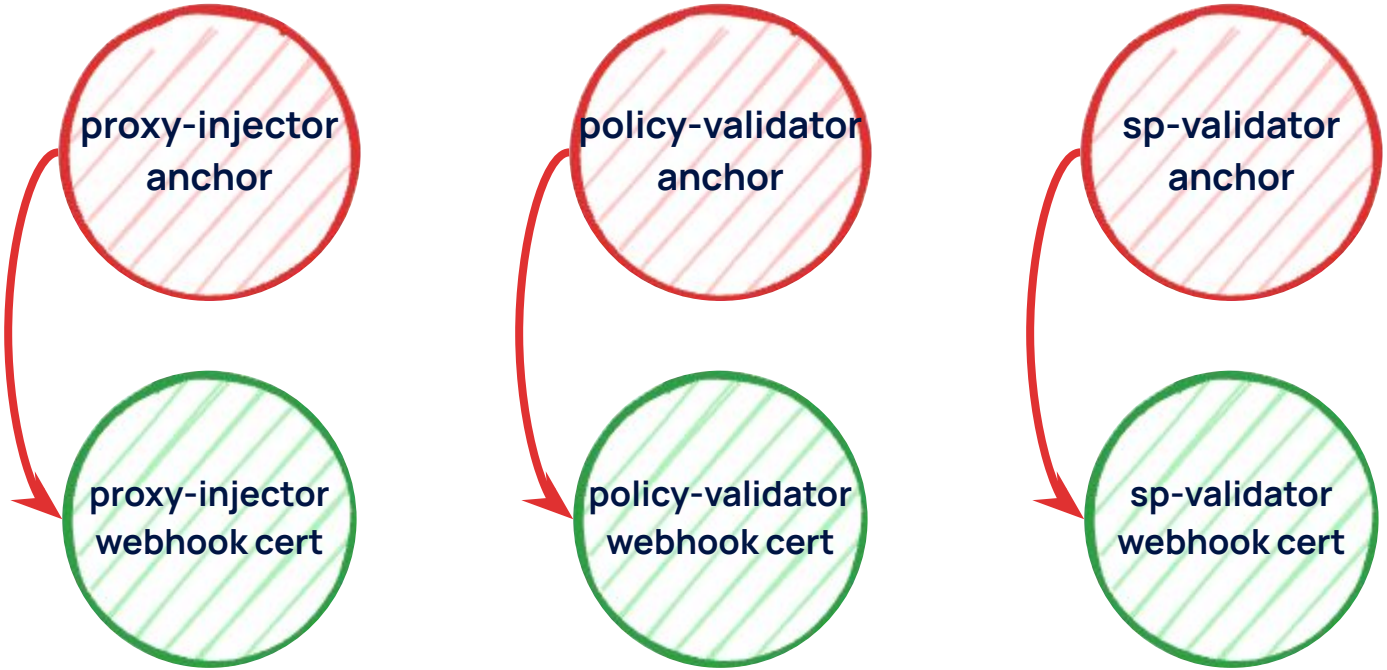


Certificate “Hierarchy”: Webhooks



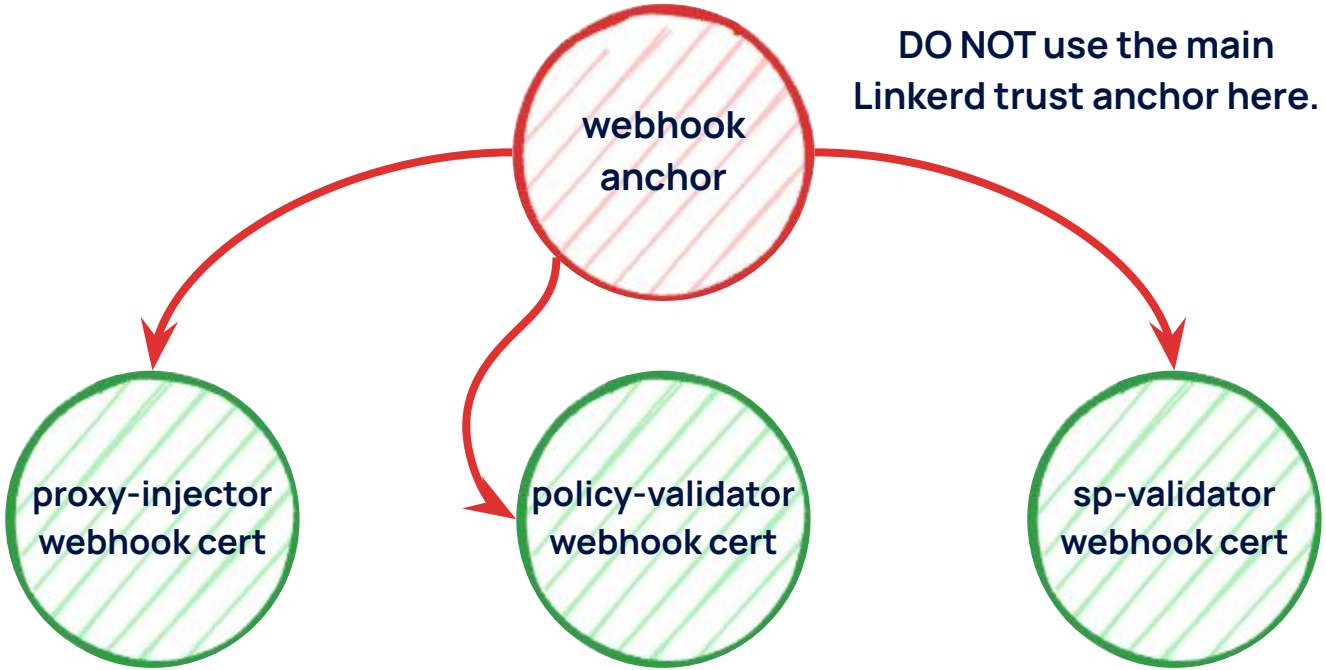
LINKERD

Certificate Hierarchy: Webhooks



LINKERD

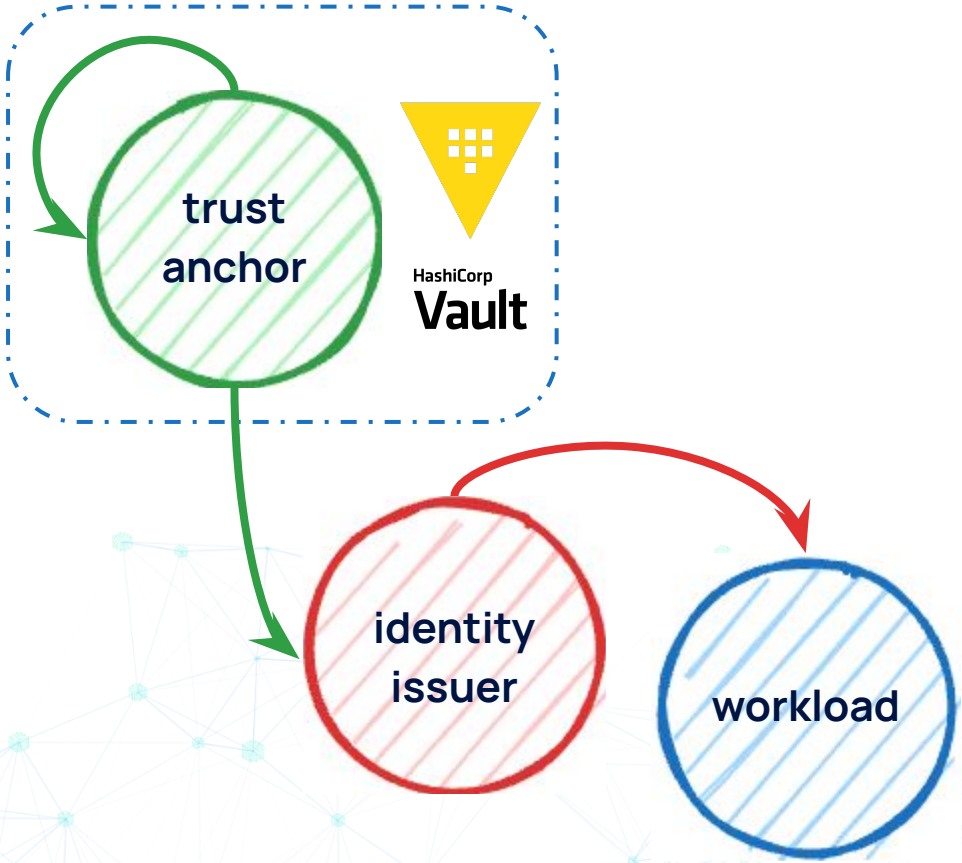
Certificate Hierarchy: Webhooks



LINKERD

Vault

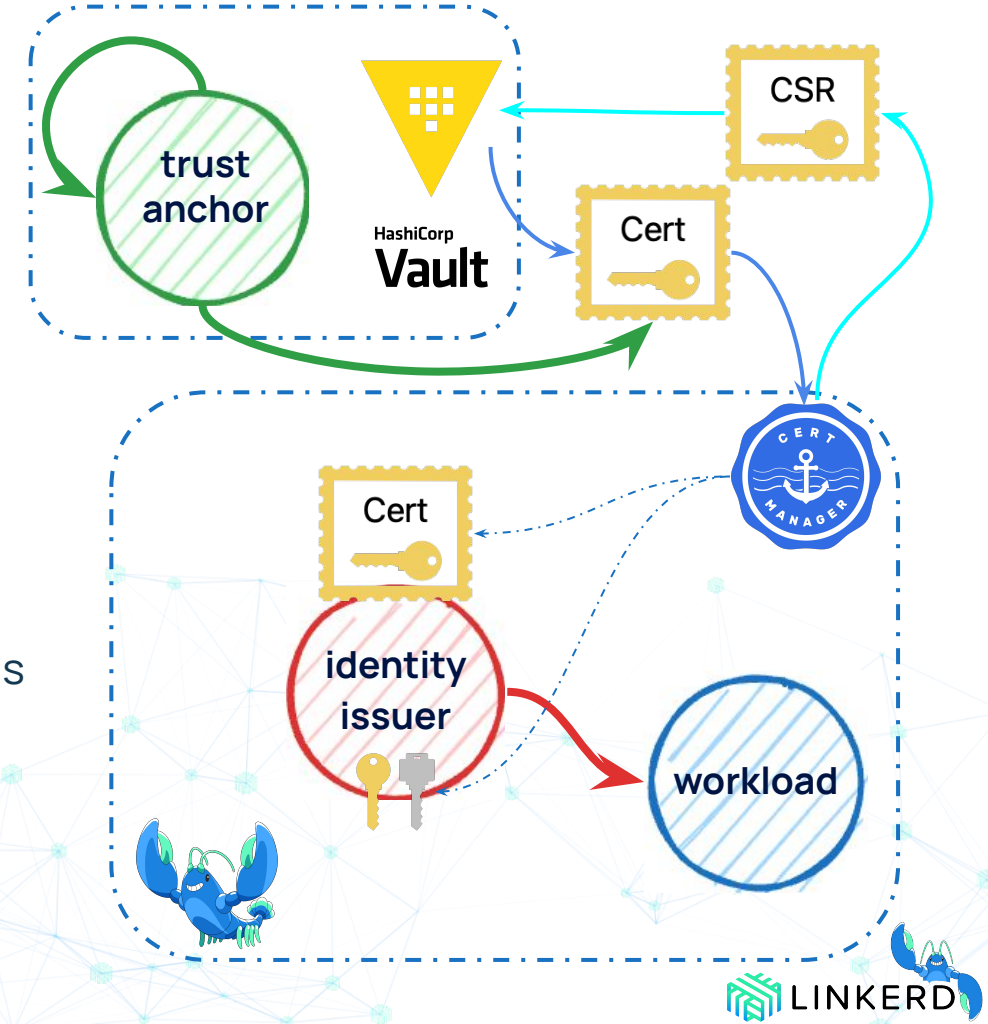
- Vault by HashiCorp, `https://vaultproject.io/`
  - "Manage secrets and protect sensitive data with Vault"
  - **NOT** a CNCF project 😢
- A basic function of Vault is being a safe place for private keys
- Vault can also act as a **CA**: it can use private keys it's storing to issue certificates, safely



LINKERD

cert-manager

- cert-manager by Venafi, **`https://cert-manager.io/`**
  - "X.509 certificate management for Kubernetes and OpenShift"
  - A CNCF project 🙂
- Distributing and rotating certificates is a pain
- cert-manager automates much of this away
- Most powerful when paired with external CAs (like Vault)



Workshop!

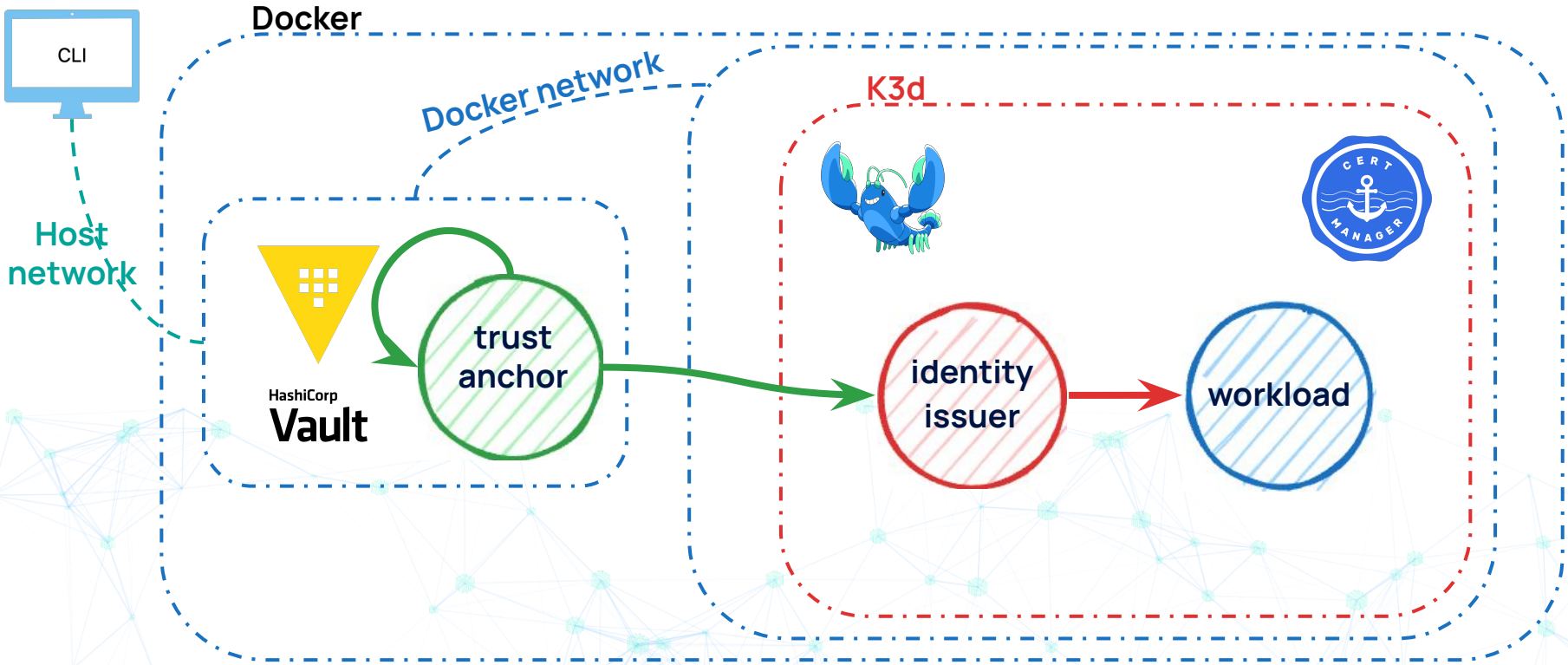
Follow along! **https://github.com/BuoyantIO/service-mesh-academy**
(in the **certificates-with-vault** directory)

Tools we'll use:

- Kubernetes cluster and the **kubectl** command
- **linkerd** – **https://linkerd.io/2/getting-started/**
- **step** – **https://smallstep.com/docs/step-cli/installation**
- **helm** – **https://helm.sh/docs/intro/quickstart/**
- **jq** – **https://jqlang.github.io/jq/**
- **bat** – **https://github.com/sharkdp/bat**

Also recommended: **demosh** from **https://github.com/BuoyantIO/demosh**




CLI
Docker
Docker network
K3d
Host network
HashiCorp
Vault
trust anchor
identity issuer
workload
CERT MANAGER
LINKERD

DEMO



BUOYANT | SERVICEMESH ACADEMY

Linkerd, Argo, and Gateway API



Regina Scott
Argo CD Maintainer



Flynn
Tech Evangelist

Sign up at
buoyant.io/sma

Thursday, October 26, 2023

9 am PT | 12 am CT | 6pm CET

BUOYANT'S
SERVICE MESH
ACADEMY

The creators of
LINKERD

Thanks so much!

Flynn
Tech Evangelist, Buoyant
flynn@buoyant.io

