KubeCon | CloudNativeCon

Europe 2020

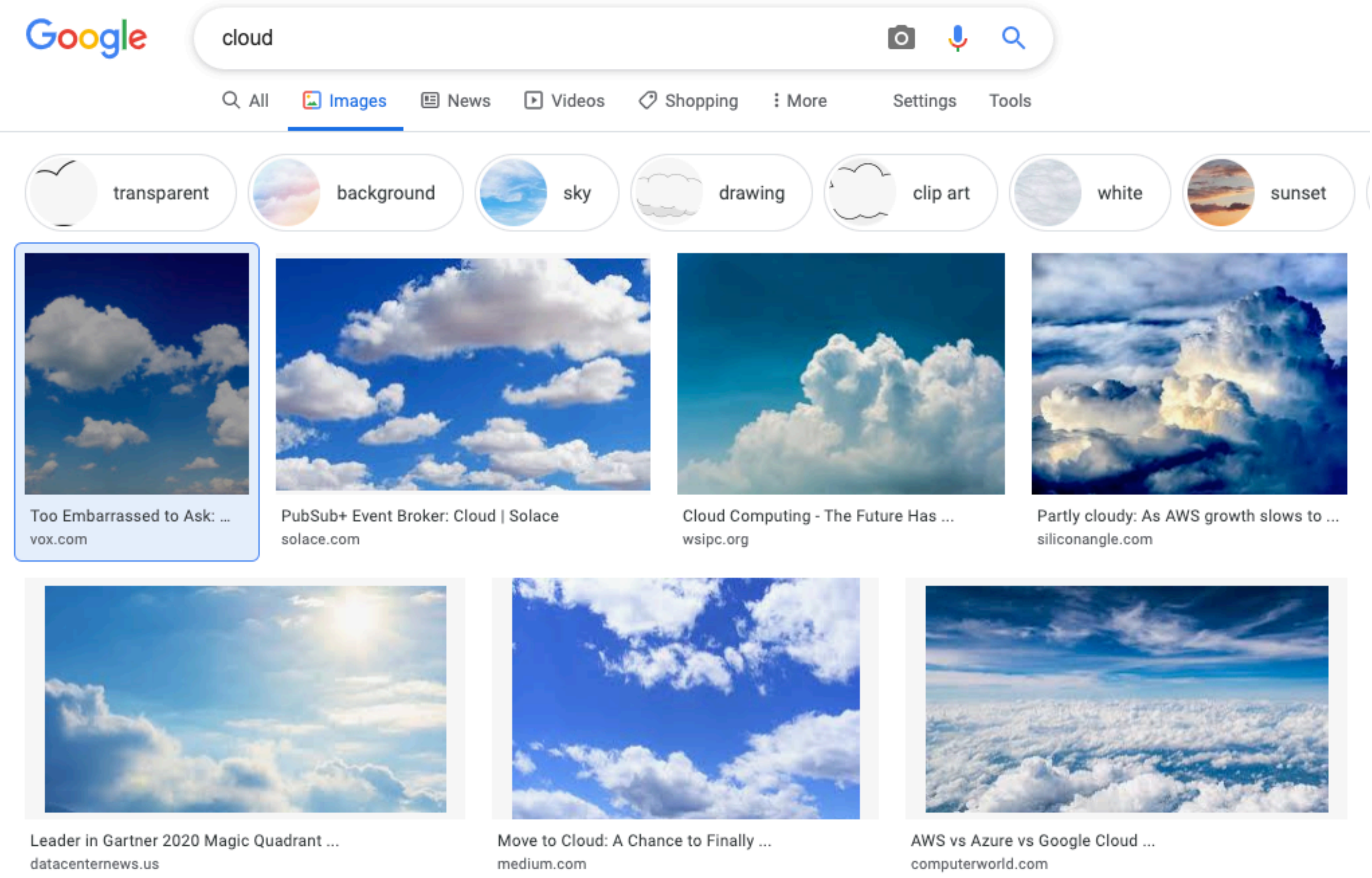
Virtual

Where are your images running? Stop worrying and start Encrypting!

Brandon Lum (@lumjjb), IBM
Harshal Patil, Red Hat

Contributions by: Stefan Berger

Where are my container workloads?



Google

cloud

All | Images | News | Videos | Shopping | More | Settings | Tools

transparent | background | sky | drawing | clip art | white | sunset

Too Embarrassed to Ask: ...
vox.com

PubSub+ Event Broker: Cloud | Solace
solace.com

Cloud Computing - The Future Has ...
wsipc.org

Partly cloudy: As AWS growth slows to ...
siliconangle.com

Leader in Gartner 2020 Magic Quadrant ...
datacenternews.us

Move to Cloud: A Chance to Finally ...
medium.com

AWS vs Azure vs Google Cloud ...
computerworld.com

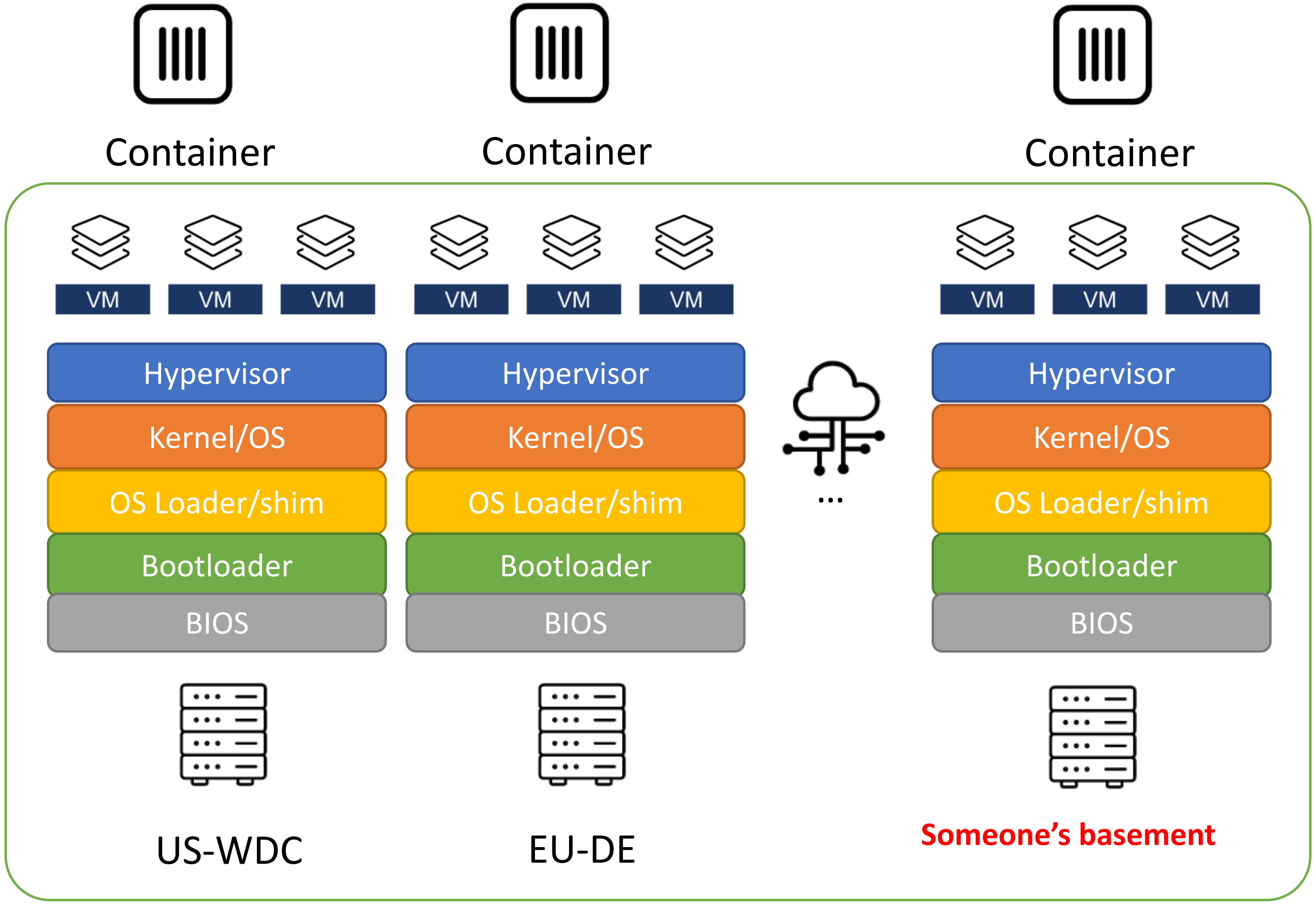
Where are my container workloads?

KubeCon | CloudNativeCon Europe 2020 Virtual

- Confidential code – i.e. Trade secret algorithms, should only be running on company datacenters

- Highly regulated industries → Compliance and security to know where certain container workloads are running.

- Export Control / Digital Rights Media



Geofencing Execution

Execution Geofencing

– Ability to tie compute execution to a specific compute location

Claim

Container Image Encryption + Key Management = Execution Geofencing

Geofencing Execution

Execution Geofencing

– Ability to tie compute execution to a specific compute location

Claim

Container Image Encryption + Key Management = Execution Geofencing

Encrypted Container Images

Build

- Build as normal
- **Encrypt**
- Push

Encrypt

- Encrypted image stored
- Cannot be read

Run

- Pull
- **Decrypt**
- Run

Encrypted Container Images

“Encrypt a container image so it is only decryptable by Key X”

- Image Confidentiality, Deprivileged Registry

Available today in:

- Buildah, skopeo, Containerd, Cri-o, DockerHub/Docker Distribution

Build

buildah

skopeo

Runtime

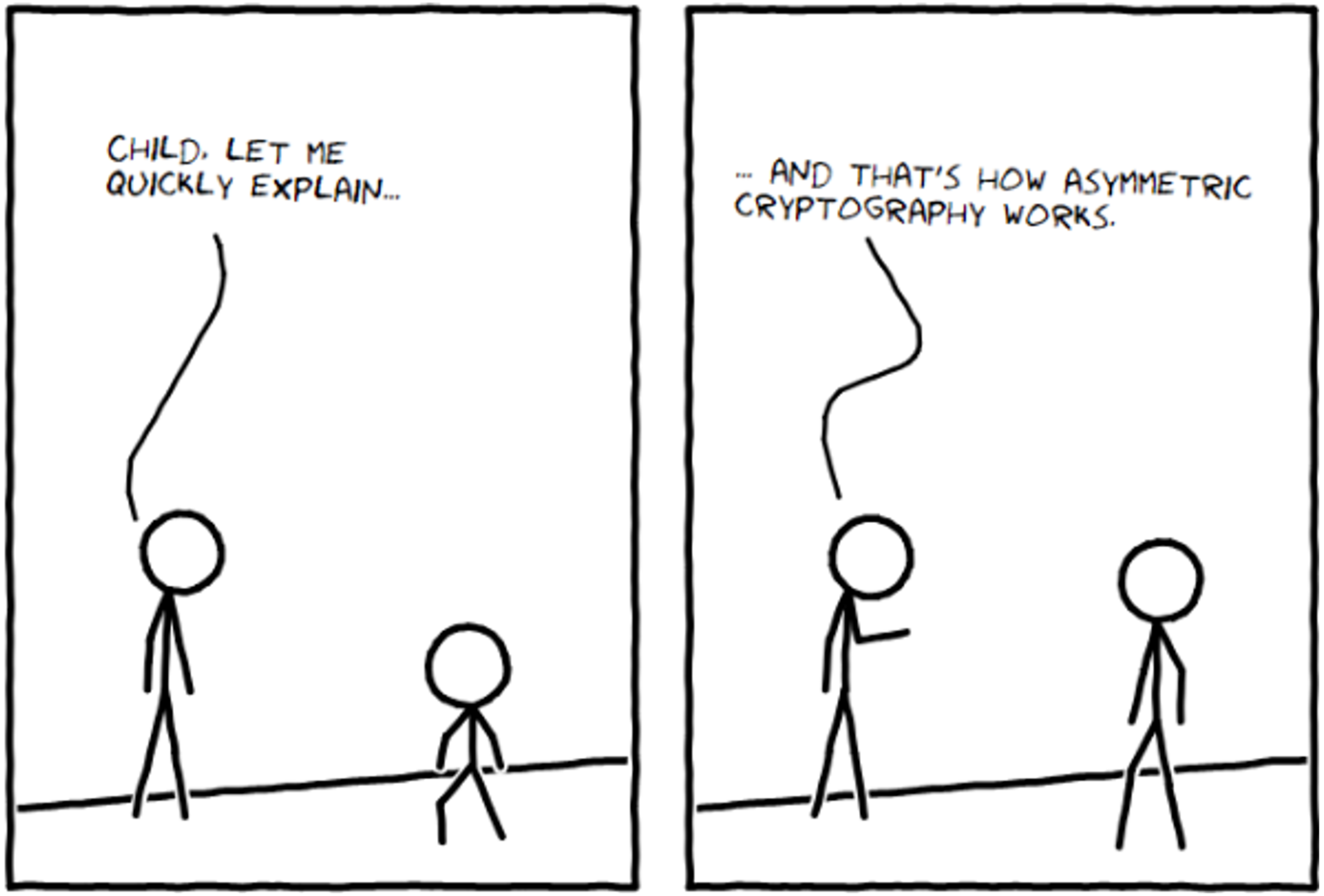
containerd

cri-o

Registry

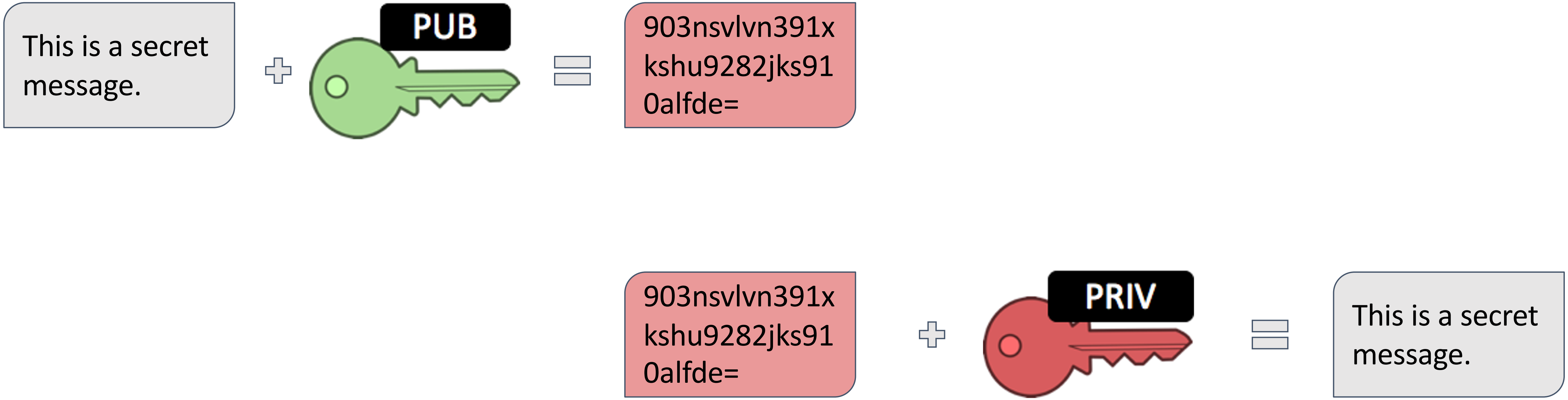
Docker Distribution

Encryption Primer


CHILD. LET ME QUICKLY EXPLAIN...
... AND THAT'S HOW ASYMMETRIC CRYPTOGRAPHY WORKS.

https://www.outsystems.com/blog/posts/how-to-teach-child-about-asymmetric-cryptography/

Encryption Primer – Asym. Enc.



This is a secret message. + PUB = 903nsvlvn391xkshu9282jks910alfde=

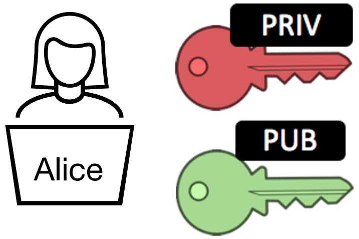
903nsvlvn391xkshu9282jks910alfde= + PRIV = This is a secret message.

Each user has a Public-Private key pair, where Public Key is not secret, can be published.

Send Encrypted Image to Alice

1 Alice Generates an RSA keypair on her workstation, and shares her **Public key**

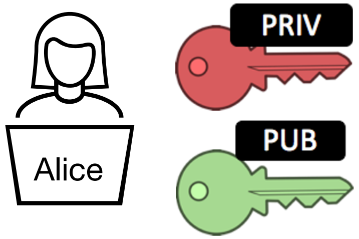
```
openssl genrsa -out alicePrivate.pem 2048
openssl rsa -in alicePrivate.pem -pubout ...
```



Send Encrypted Image to Alice

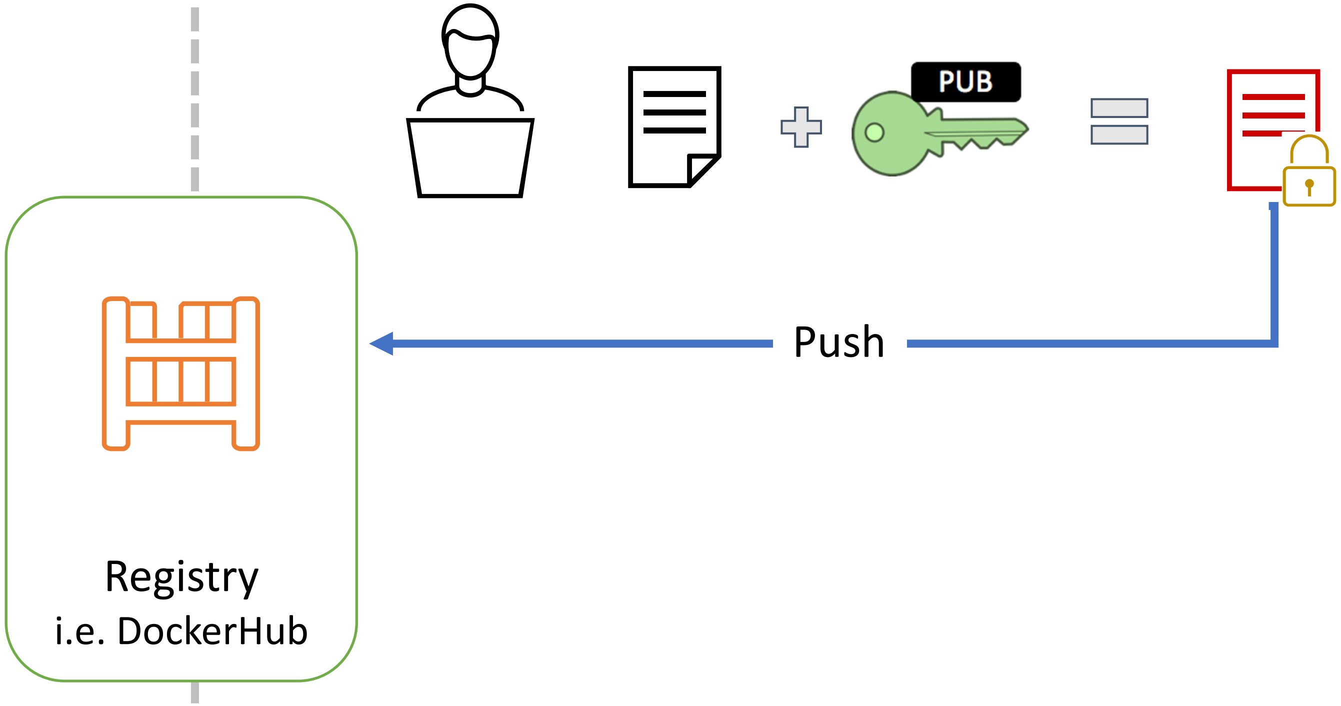
1 Alice Generates an RSA keypair on her workstation, and shares her **Public key**

```
openssl genrsa -out alicePrivate.pem 2048
openssl rsa -in alicePrivate.pem –pubout ...
```



2 **We encrypt a container image with Alice’ public key so that it is only decryptable by Alice’s Private Key.**

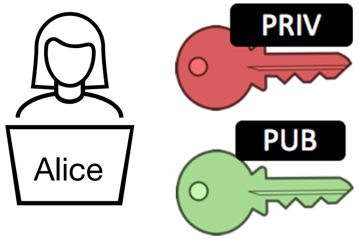
```
buildah push \
  –encryption-key jwe:alicePublic.pem
  my-cont-image
```



Send Encrypted Image to Alice

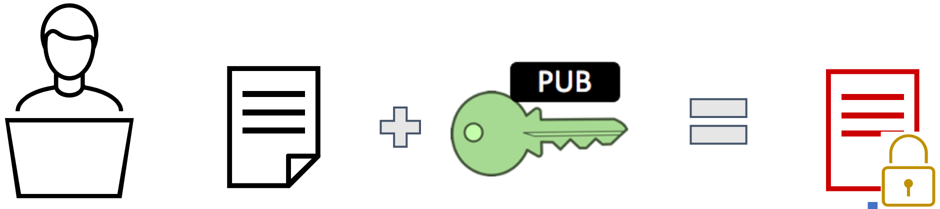
1 Alice Generates an RSA keypair on her workstation, and shares her **Public key**

```
openssl genrsa -out alicePrivate.pem 2048
openssl rsa -in alicePrivate.pem -pubout ...
```

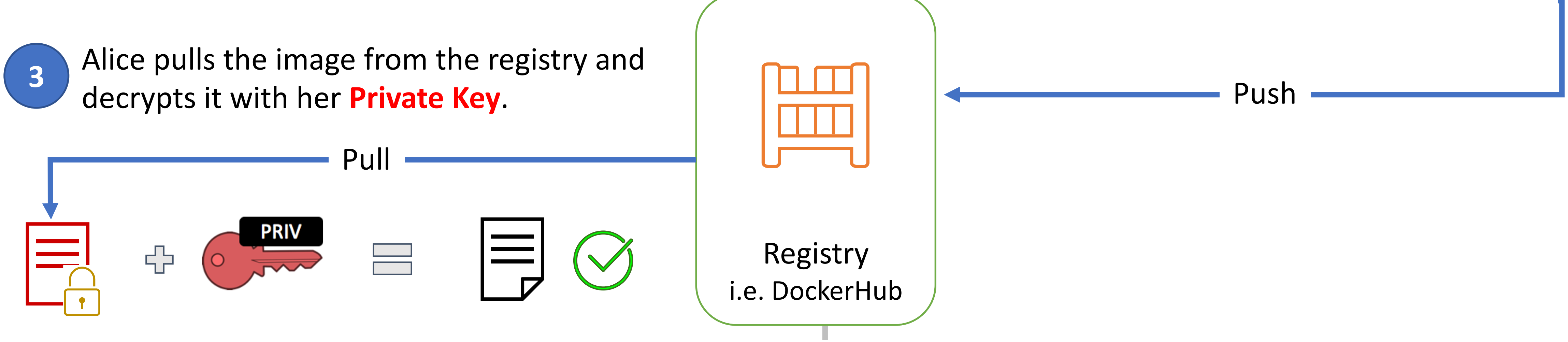


2 **We encrypt a container image with Alice’ public key so that it is only decryptable by Alice’s Private Key.**

```
buildah push \
  -encryption-key jwe:alicePublic.pem
  my-cont-image
```



3 Alice pulls the image from the registry and decrypts it with her **Private Key**.



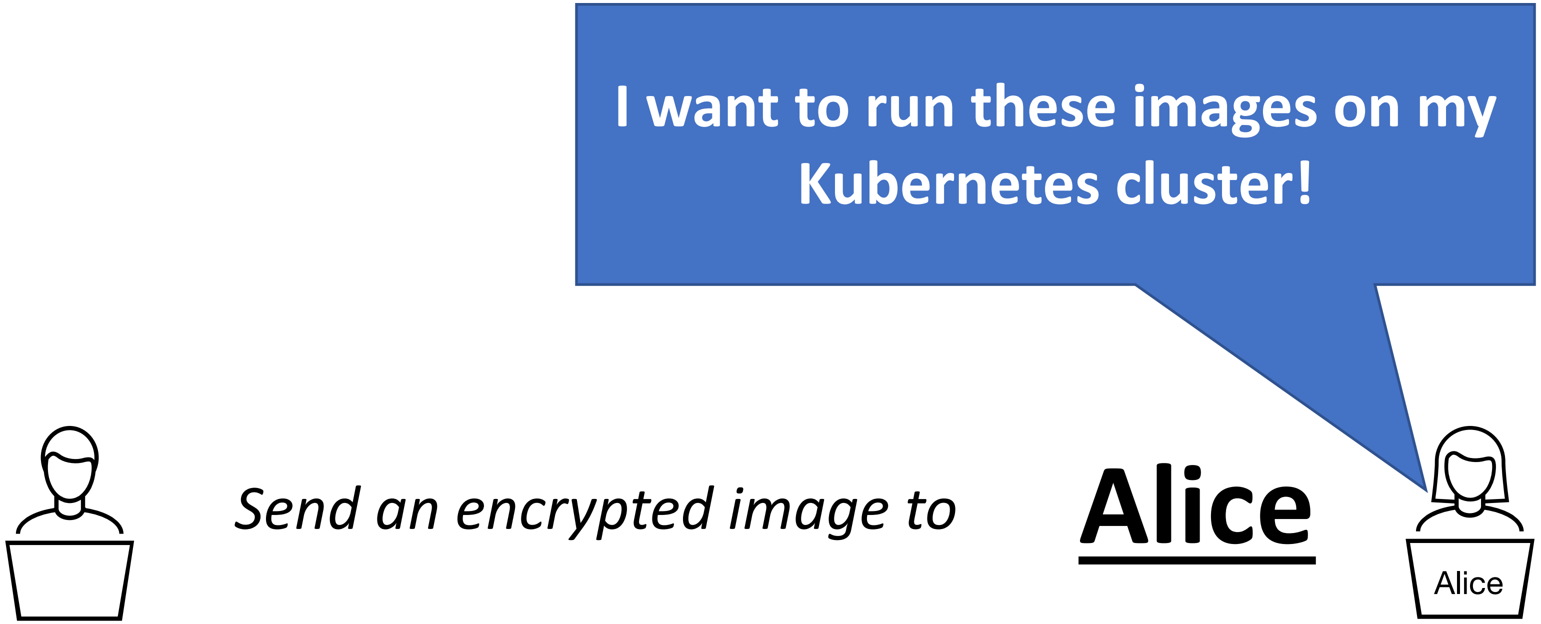
Simple Encryption Demo

Encrypted Container Images

Send an encrypted image to **<u>Alice</u>**

Alice

Encrypted Container Images



I want to run these images on my Kubernetes cluster!

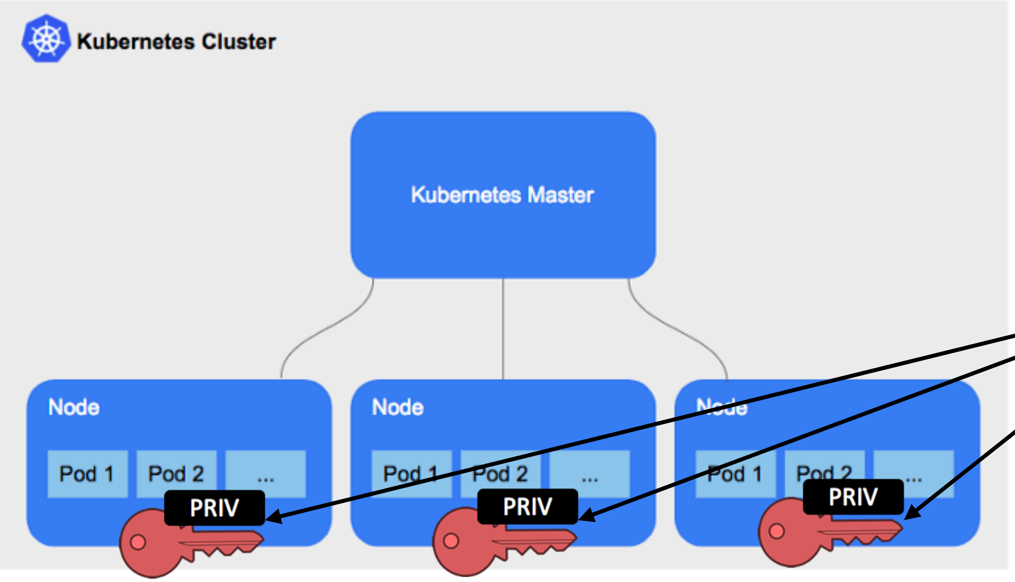
Send an encrypted image to **Alice**

Encrypted Container Images

- In Kubernetes, decryption is handled by the container runtime (i.e. cri-o, containerd)

cri-o containerd

- Keys are made available to the runtime, through the filesystem



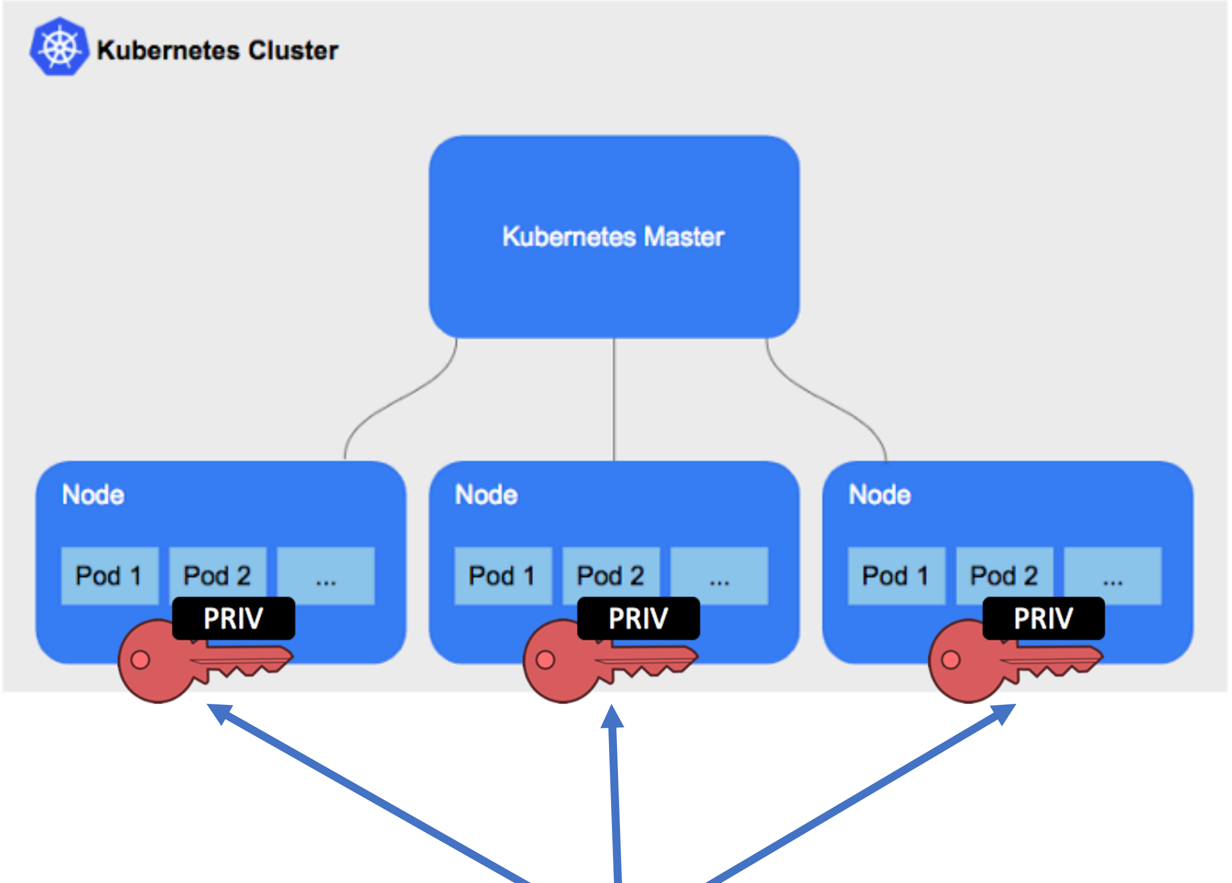
For example:
/etc/crio/keys
(default for cri-o)

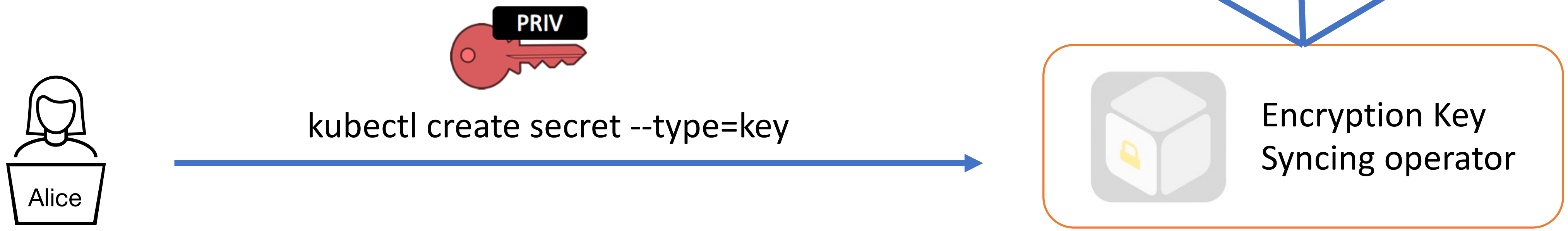
Encrypted Container Images

- To distribute keys to the container runtimes, we will use the help of an operator

Encryption Key Syncing operator

https://github.com/IBM/k8s-enc-image-operator





```
kubectl create secret --type=key
```

Kubernetes Demo

Encrypting for Alice

Let’s Recap

Encrypting for Alice

Container Image Encryption

“Encrypt a container workload so it is only decryptable by Alice Private Key”

Encrypting for Alice

Container Image Encryption

“Encrypt a container workload so it is only decryptable by Alice Private Key”

Alice

“Alice Private Key accessible on Alice’s workstation”

Encrypting for Alice

Container Image Encryption

"Encrypt a container workload so it is only decryptable by Alice Private Key"

Alice

"Alice Private Key accessible on Alice's workstation"

Container Exec

Container workload only decryptable on Alice's workstation

Encrypting for Alice's k8s Cluster

Container Image Encryption

"Encrypt a container workload so it is only decryptable by Alice Private Key"

Alice

"Alice Private Key accessible on {Alice's workstation, **Alice's k8s cluster**}"

Container Exec

Container workload only decryptable on {Alice's workstation, **Alice's k8s cluster**}

Encrypting for Alice’s k8s Cluster

Container Image Encryption

“Encrypt a container workload so it is only decryptable by Alice Private Key”

Alice (Key Management)

“Alice Private Key accessible on {Alice’s workstation, **Alice’s k8s cluster**}”

Container Exec

Container workload only decryptable on {Alice’s workstation, **Alice’s k8s cluster**}

Alice == Key Management

Container Image Encryption

"Encrypt a container workload so it is only decryptable by Alice Private Key"

Key Management

"Key X is only accessible by Entities E"

Key X = Alice Priv. Key

Entities E =
{ Alice's workstation, Alice K8s Cluster}

Container Exec

Container workload only decryptable on {Alice's workstation, Alice's k8s cluster}

QED

Container Image Encryption

"Encrypt a container workload so it is only decryptable by Key X"

Key Management

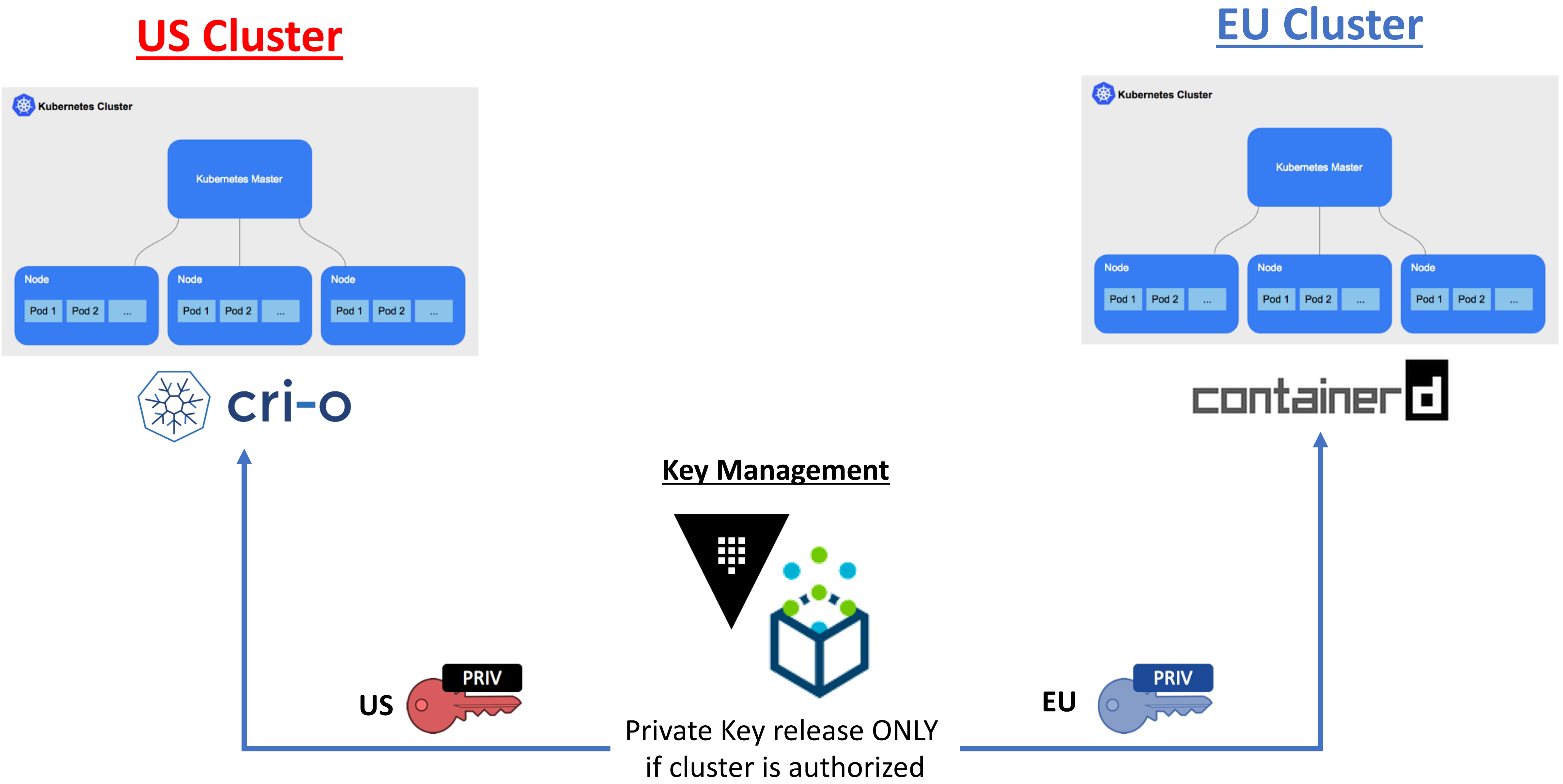
"Key X is only accessible by Entities E"

Execution Geofencing

"Container workload only decryptable on Entities E"

By Transitive property, it follows that Container Image Encryption + Key Management allows Execution Geofencing □

Enterprise Geo-fencing



US Cluster

EU Cluster

Key Management

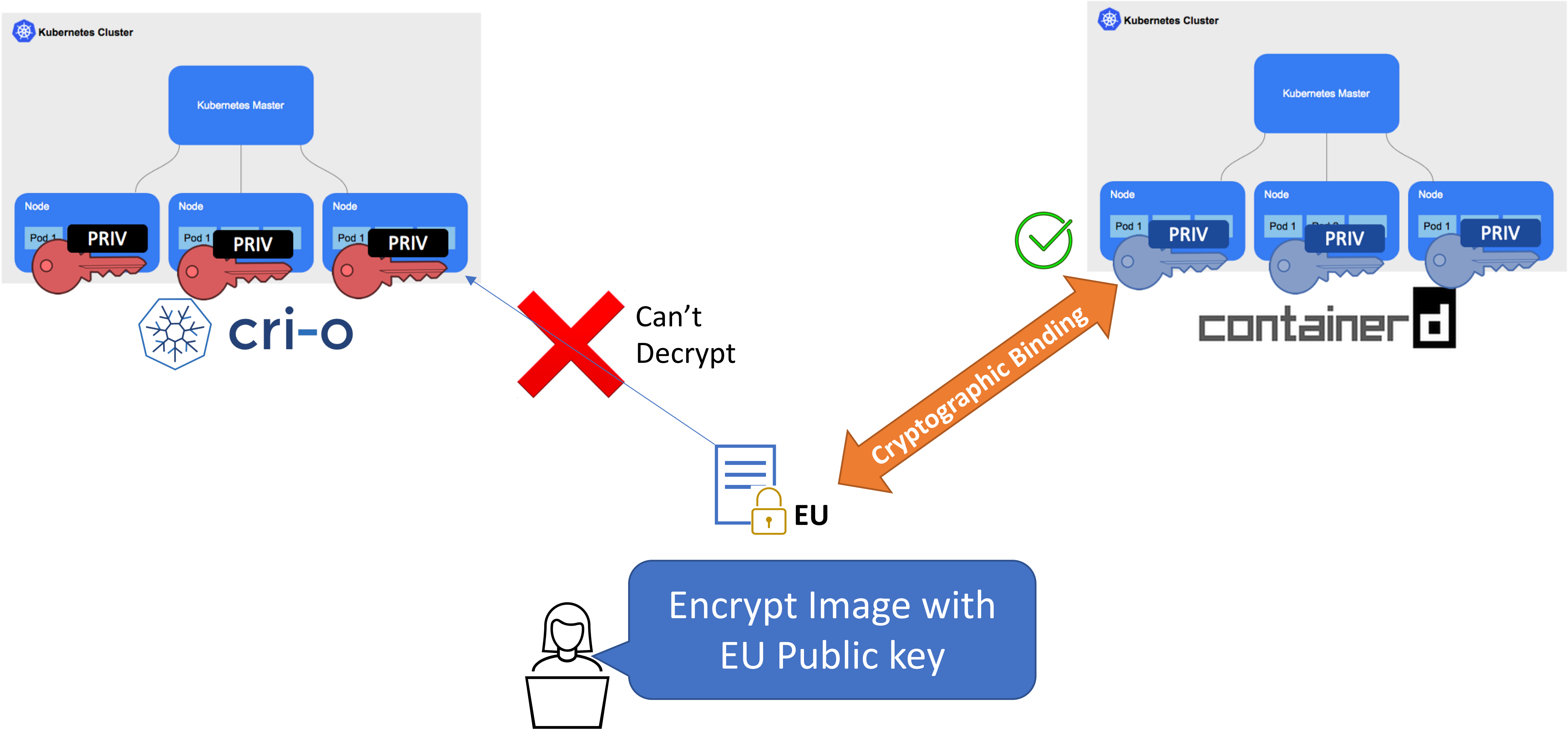
Private Key release ONLY if cluster is authorized

Enterprise Geo-fencing

KubeCon | CloudNativeCon
Europe 2020
Virtual

US Cluster

EU Cluster



Can’t
Decrypt

Encrypt Image with
EU Public key

Multi-cluster Geofencing Demo

Trust Bootstrapping/Attestation

Key Management - “Key X is only accessible by **Entities E**”

- How do we ensure that only those entities can access the keys?
- **Today:** Secure process or reliance on trusted administrator

Trust Bootstrapping/Attestation

Key Management - “Key X is only accessible by **Entities E**”

- Tie to HW Root of Trust (i.e. TPM) & asset tags
- Attests BIOS, firmware, OS, etc.
  - Keylime (RedHat)
  - Intel Datacenter Secure Libraries (ISecL)

- **NIST** Article on this topic of Trusted Container Platform: https://www.nccoe.nist.gov/news/policy-based-governance-trusted-container-platform

Summary

In some scenarios, it is critical to know where workloads are running, and we can achieve this by Encrypted Container Images + Key Management

Encrypted Container Image is supported today in the ecosystem: containerd, cri-o, buildah, skopeo, Docker Distribution, etc.

For High Assurance, Key management needs to be backed by strong Trust Bootstrapping and/or Attestation. Engage with us!
https://github.com/IBM/Trusted_Container

Thank You!

Speakers:
Brandon Lum (@lumjjb)
Harshal Patil (github.com/harche)

Shoutout to Stefan Berger, Phil Estes,
and other collaborators from OCI, Containerd, cri-o, github.com/containers

Links

Encrypted Container Images Links

- Encrypting container images with Skopeo https://medium.com/@lumjjb/encrypting-container-images-with-skopeo-f733afb1aed4
- How Encrypted Images brings about compliance in Kubernetes (via CRI-O) https://medium.com/@lumjjb/how-encrypted-images-brings-about-compliance-in-kubernetes-via-cri-o-6ab58fad6124
- Advancing container image security with encrypted container images https://developer.ibm.com/articles/advancing-image-security-encrypted-container-images/

Trusted Container Platform Links

- Policy Based Governance in Trusted Container Platform https://www.nccoe.nist.gov/news/policy-based-governance-trusted-container-platform
- Trusted Container Dicussion Repo: https://github.com/IBM/Trusted_Container

Tooling

- Buildah v1.15 release https://buildah.io/releases/2020/06/27/Buildah-version-v1.15.0.html
- Containerd (1.4+) https://github.com/containerd/cri/blob/master/docs/decryption.md
- Cri-o (1.17+) https://github.com/cri-o/cri-o/blob/master/tutorials/decryption.md
- Enc-key-sync Operator https://github.com/IBM/k8s-enc-image-operator/ https://operatorhub.io/operator/enc-key-sync
- Skopeo https://github.com/containers/skopeo
- Docker Distribution https://github.com/docker/distribution
- OCIcrypt https://github.com/containers/ocicrypt
- Containerd imgcrypt https://github.com/containerd/imgcrypt

KubeCon | CloudNativeCon

Europe 2020

Virtual

KEEP CLOUD NATIVE CONNECTED