
KubeCon
CloudNativeCon
Europe 2025
LONDON BUS

Signed, Sealed, Delivered

Sign and ***Verify*** All the Things

Jeremy Rickard

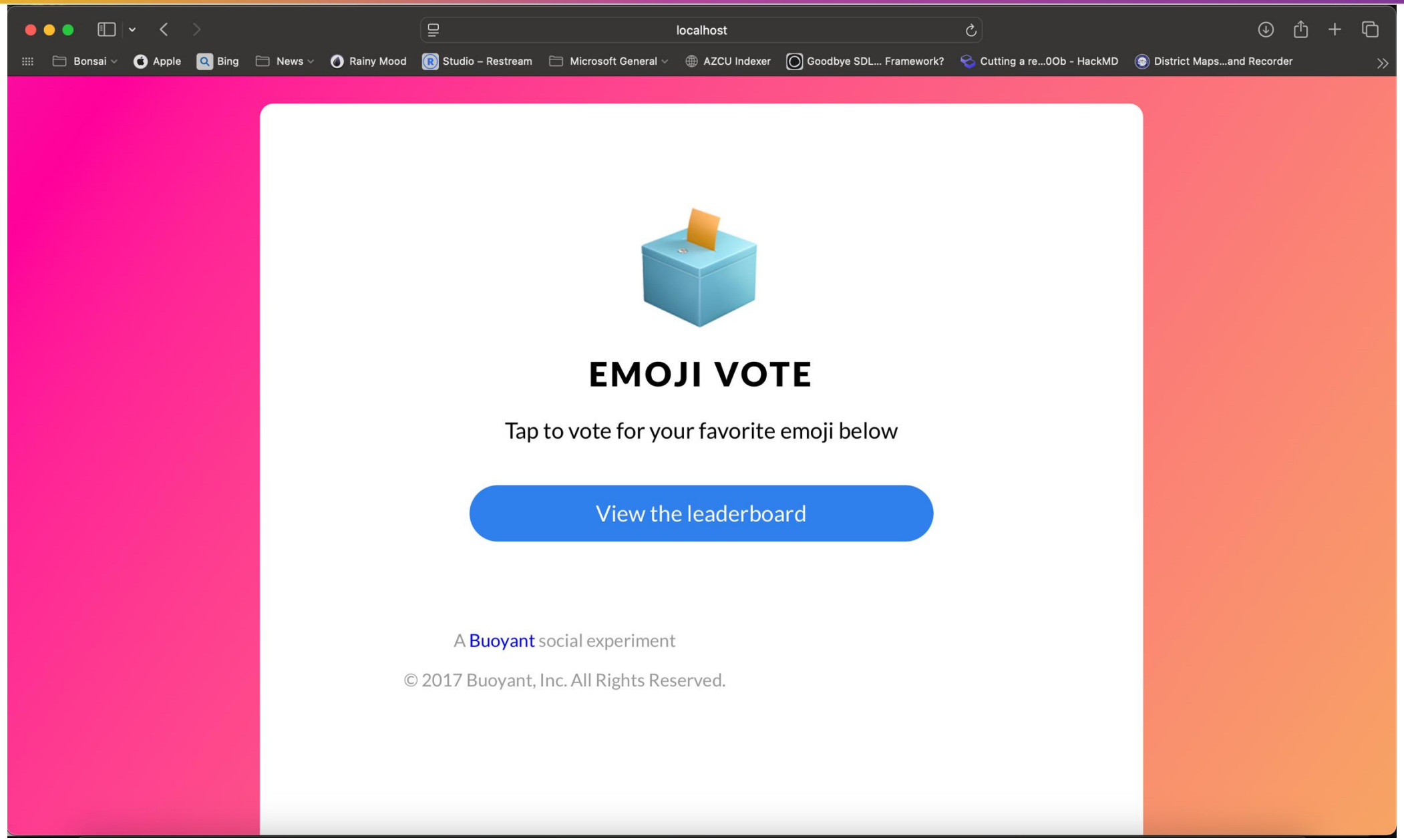
KubeCon | CloudNativeCon
Europe 2025

Hello!

@jeremyrickard.com on Bluesky

Using containers used to be so fun and carefree….

And with that in mind….



toomanyrequests: You have reached your pull rate limit. You may increase the limit by authenticating and upgrading: https://www.docker.com/increase-rate-limit

- a docker client somewhere

```
(⎈ |kind-kind:default) ~ trivy image --vuln-type os buoyantio/emojivoto-web:v11 | more
2025-04-01T10:47:47.620+0100    INFO    Vulnerability scanning is enabled
2025-04-01T10:47:47.620+0100    INFO    Secret scanning is enabled
2025-04-01T10:47:47.620+0100    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-04-01T10:47:47.620+0100    INFO    Please see also https://aquasecurity.github.io/trivy/v0.43/docs/scanner/secret/#recommendati
on for faster secret detection
2025-04-01T10:47:49.092+0100    INFO    Detected OS: debian
2025-04-01T10:47:49.092+0100    INFO    Detecting Debian vulnerabilities...
2025-04-01T10:47:49.192+0100    WARN    This OS version is no longer supported by the distribution: debian 10.4
2025-04-01T10:47:49.192+0100    WARN    The vulnerability detection may be insufficient because security updates are not provided

buoyantio/emojivoto-web:v11 (debian 10.4)
=========================================
Total: 942 (UNKNOWN: 9, LOW: 202, MEDIUM: 276, HIGH: 394, CRITICAL: 61)
```

SECURITY — KONG — IMAGES — SUPPLY CHAIN — NEWS

Kong urges action after Docker account compromised, malware uploaded

A cryptominer and trolling in logs? It could have been a LOT worse. Here's what builders should do...

Let’s ***start*** to take control of our container supply chain

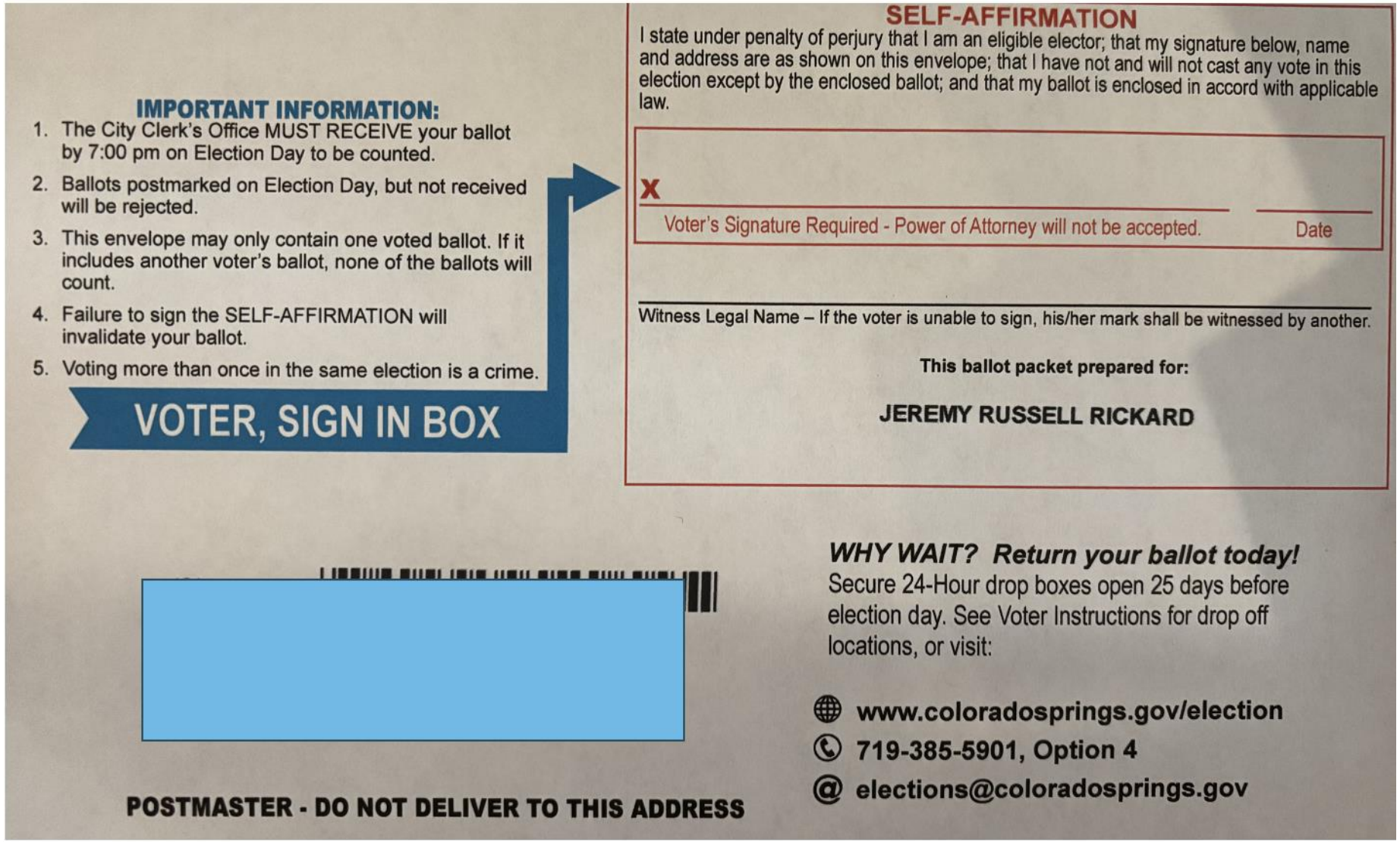
Guidance for Artifacts Authors

Content other than OCI container images MAY be packaged using the image manifest. When this is done, the `config.mediaType` value should not be a known OCI image config media type. Historically, due to registry limitations, some tools have created non-OCI conformant artifacts using the `application/vnd.oci.image.config.v1+json` value for `config.mediaType` and values specific to the artifact in `layer[*].mediaType`. Implementation details and examples are provided in the image manifest specification.

Things we could do….

1. Mirror images to an internal registry
2. Sign (and optionally patch) images
3. Enforce images only come from our registry
4. Verify container(s) before deployment
5. Verify deployment manifests

Ok so let's talk about verifying…



IMPORTANT INFORMATION:

1. The City Clerk's Office MUST RECEIVE your ballot by 7:00 pm on Election Day to be counted.
2. Ballots postmarked on Election Day, but not received will be rejected.
3. This envelope may only contain one voted ballot. If it includes another voter's ballot, none of the ballots will count.
4. Failure to sign the SELF-AFFIRMATION will invalidate your ballot.
5. Voting more than once in the same election is a crime.

VOTER, SIGN IN BOX

SELF-AFFIRMATION

I state under penalty of perjury that I am an eligible elector; that my signature below, name and address are as shown on this envelope; that I have not and will not cast any vote in this election except by the enclosed ballot; and that my ballot is enclosed in accord with applicable law.

X

Voter's Signature Required - Power of Attorney will not be accepted. Date

Witness Legal Name – If the voter is unable to sign, his/her mark shall be witnessed by another.

This ballot packet prepared for:

JEREMY RUSSELL RICKARD

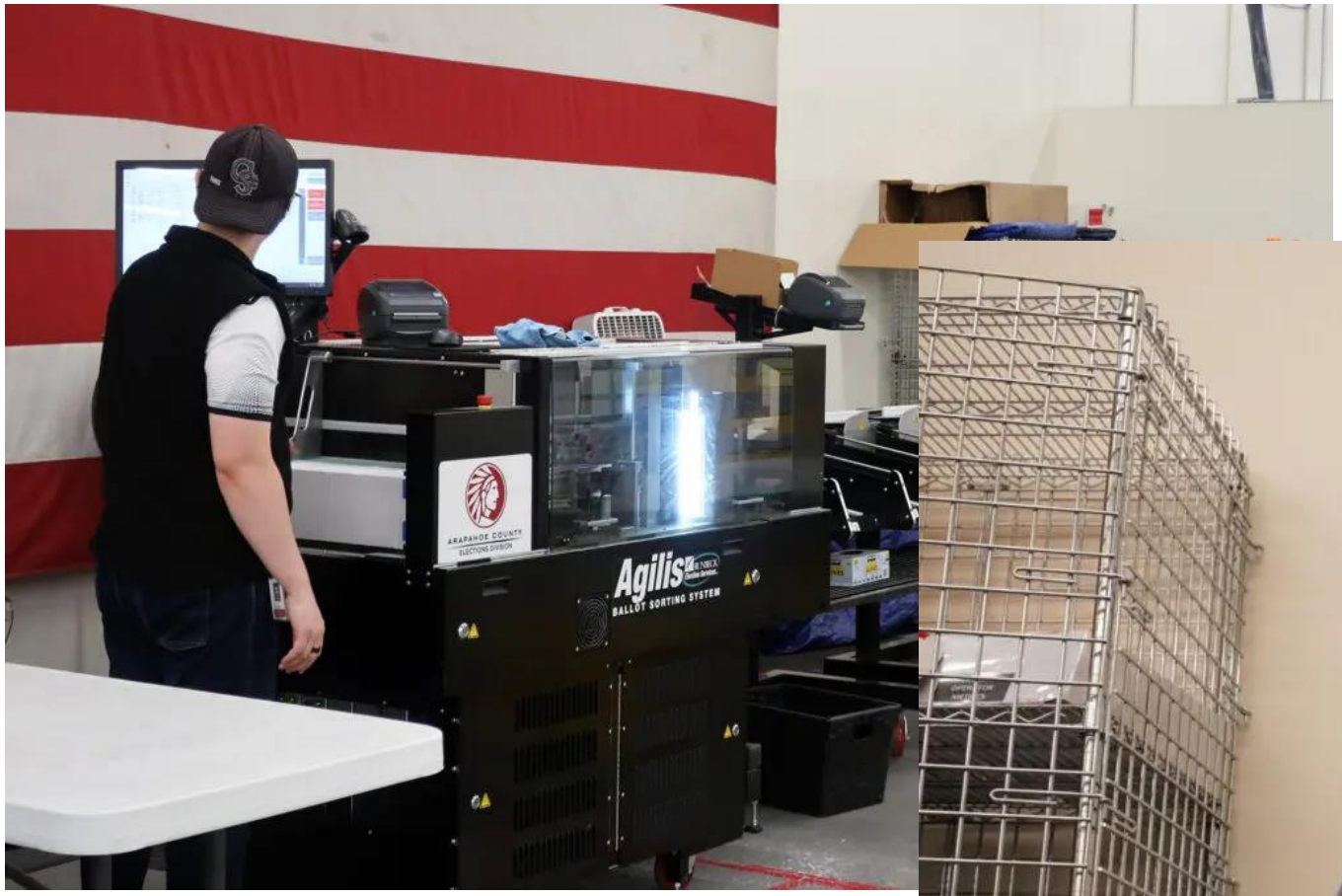
WHY WAIT? Return your ballot today!

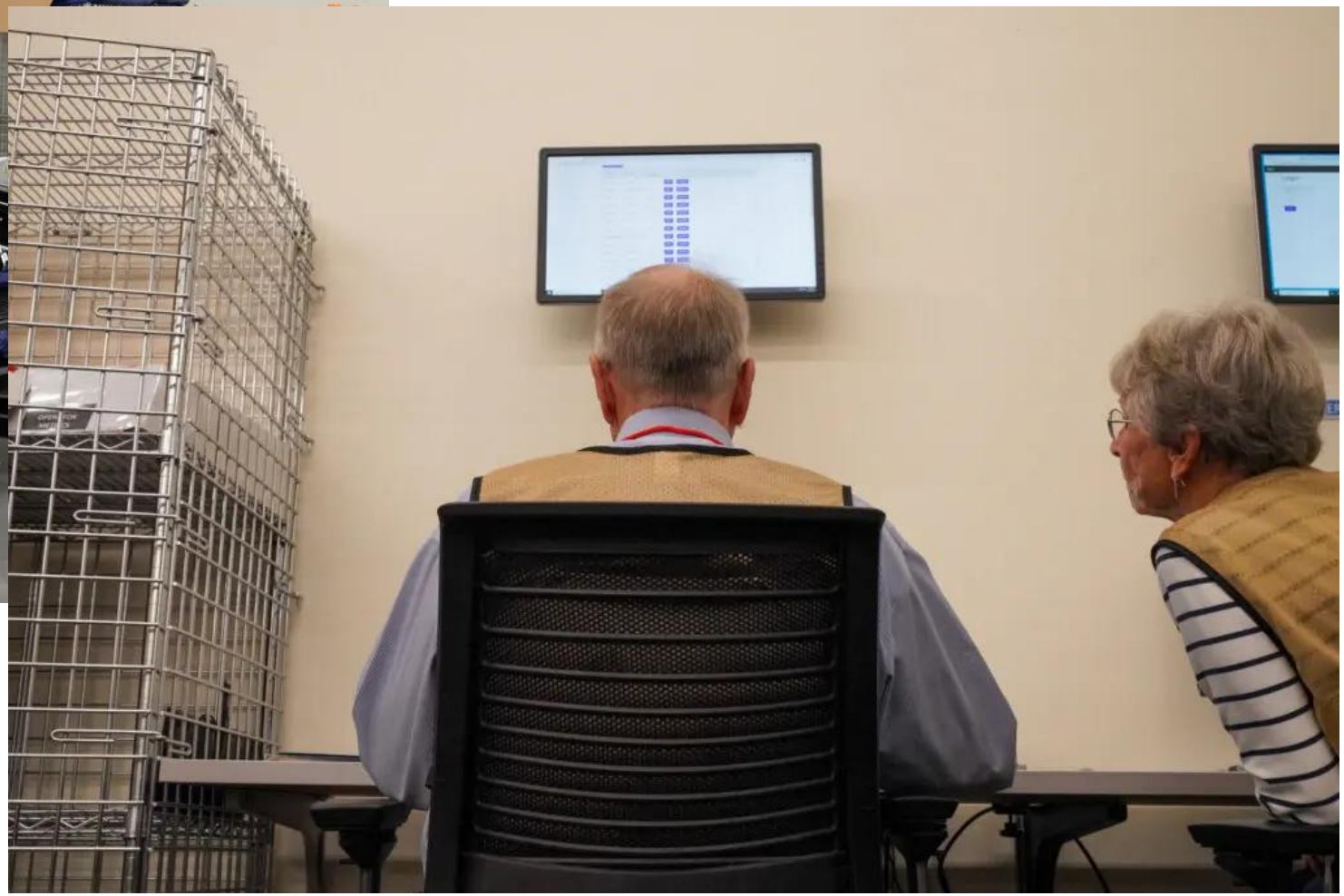
Secure 24-Hour drop boxes open 25 days before election day. See Voter Instructions for drop off locations, or visit:

www.coloradosprings.gov/election
719-385-5901, Option 4
elections@coloradosprings.gov

POSTMASTER - DO NOT DELIVER TO THIS ADDRESS

How do we verify who made the artifact?





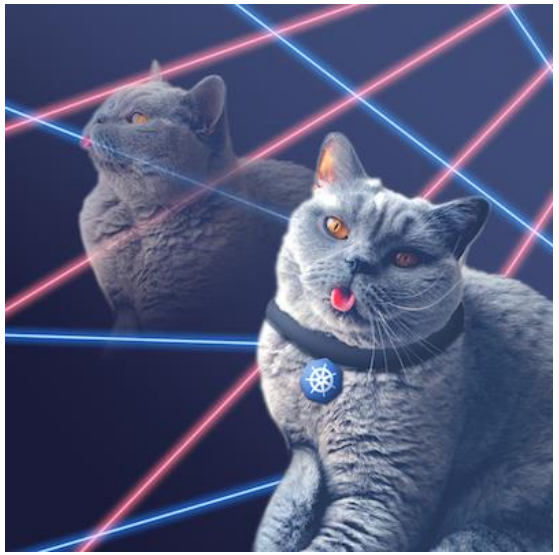
Ok, so how do we verify containers?

kubectl run signed-other --image=ghcr.io/test-verify-image:signed-by-someone-else

Error from server: admission webhook denied the request: resource Pod/default/signed-other was blocked due to the following policies check-image: check-image:

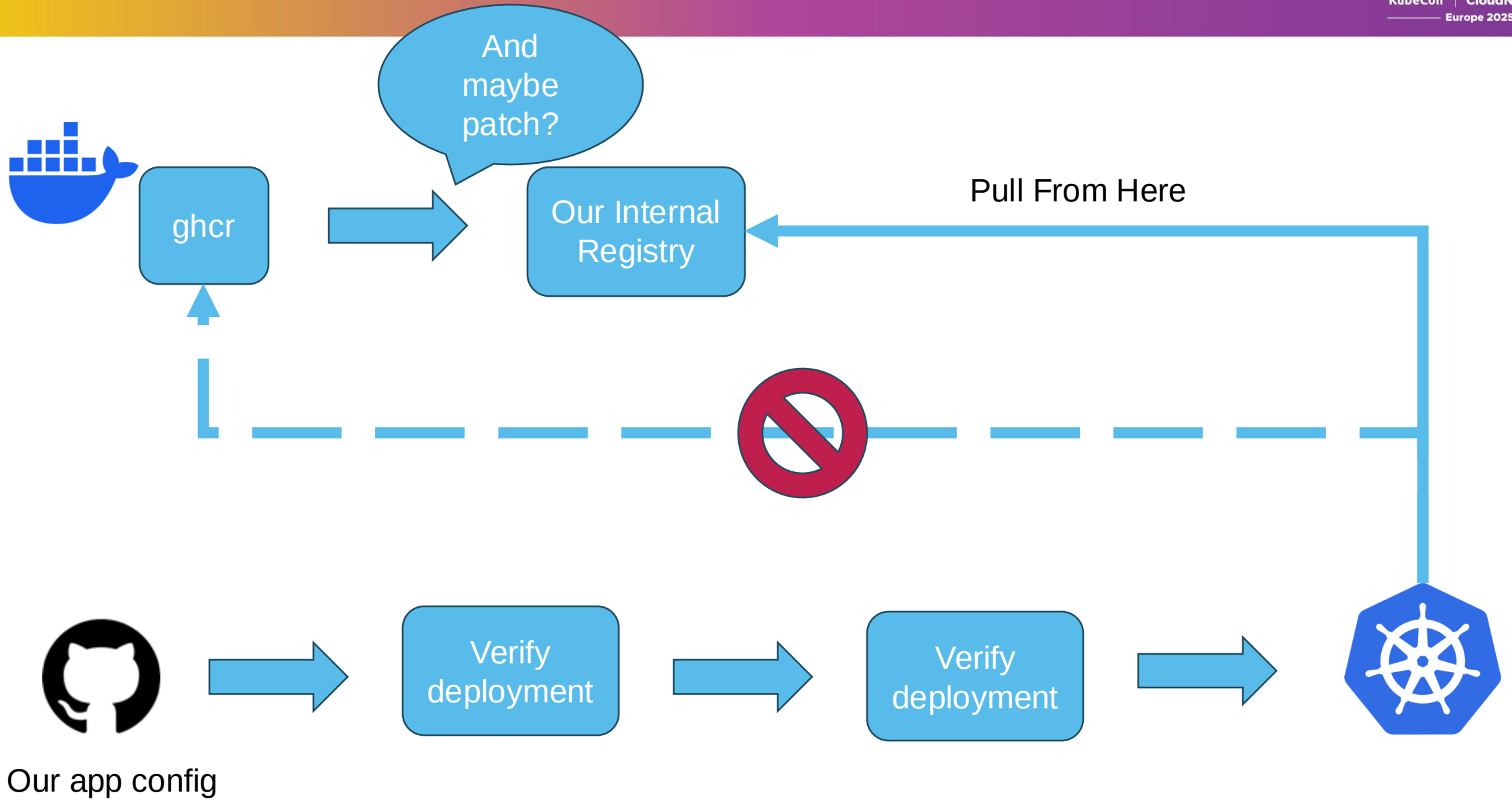
'image verification failed for ghcr.io/kyverno/test-verify-image:signed-by-someone-else: invalid signature'

$ oras pull docker.io/jrrickard/blepurrnetes:latest



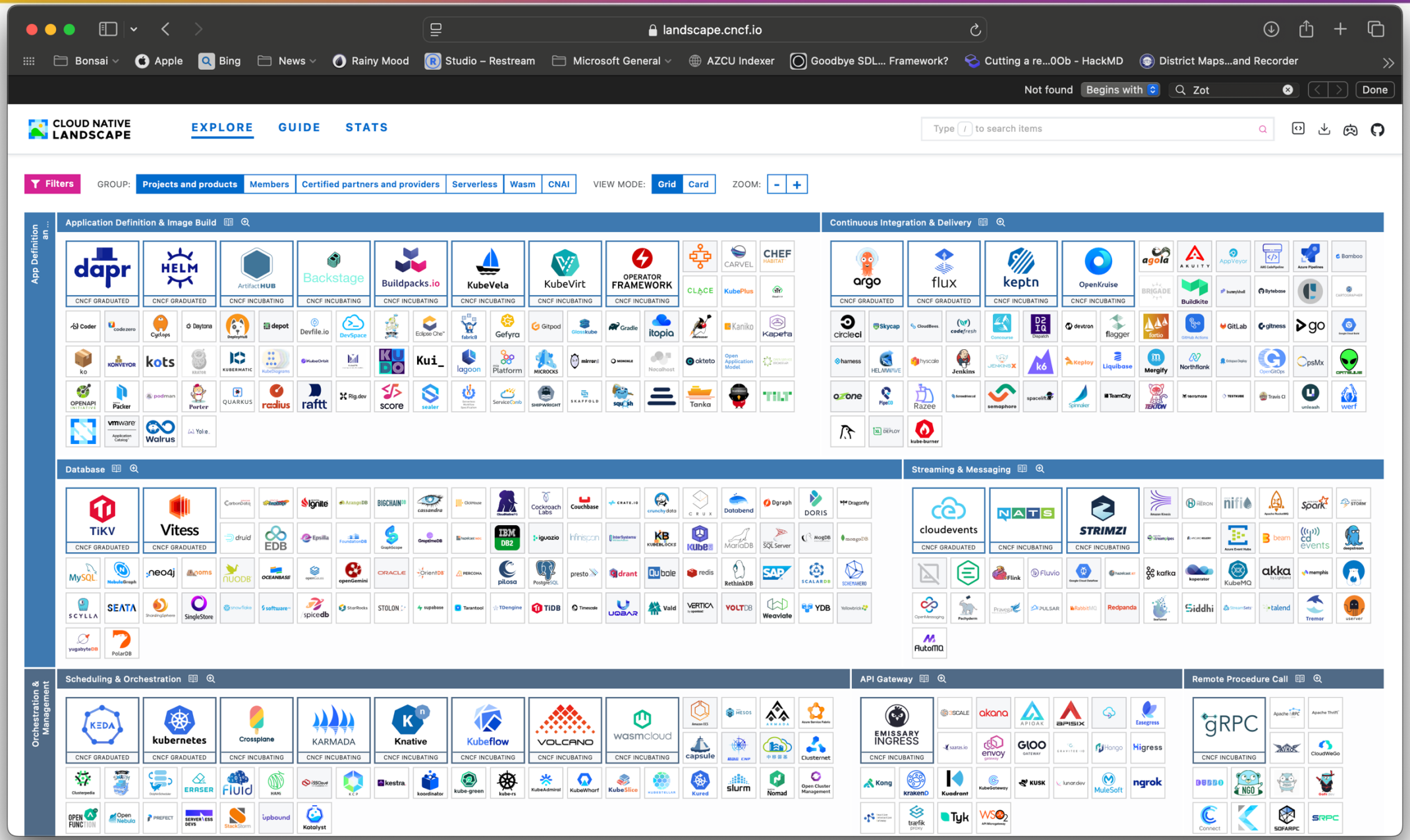
```
(⎈ |kind-kind:default) ~ notation verify docker.io/jrrickard/blepurrnetes@sha256:50b5df7575be1006a354a5a7064ff58df8b38f4c57a0ae195db2d7f33a4b460d
Successfully verified signature for docker.io/jrrickard/blepurrnetes@sha256:50b5df7575be1006a354a5a7064ff58df8b38f4c57a0ae195db2d7f33a4b460d
```

What we want to do



Can we do it with only CNCF projects?

KubeCon CloudNativeCon Europe 2025



How we will do this….

Registry: **Zot (Sandbox)**
Deployment: **Flux (Graduated)**
Artifact Signing**: Notation (Incubating)**
Image Patching: **Copa (Sandbox)**
Registry client: **ORAS (Sandbox)**
Policy Enforcement: **Kyverno (Incubating)**

Let’s put everything together…

Let’s try this out with a demo repo.

https://github.com/jeremyrickard/kubecon-signed-sealed

Some interesting upcoming sessions…

KubeCon CloudNativeCon Europe 2025

TUF-en Up Your Software Supply Chain
Marina Moore and Kairo De Araujo
Thursday April 3, 2025 11:45 - 12:15 BST
Platinum Suite | Level 3 | Room 1-2

Mind the gap: Bridging Supply Chain Policy With Git-less-Gitops and GUAC
Michael Lieberman and Andrew Martin
Thursday April 3, 2025 14:15 - 14:45 BST
Level 1 | Hall Entrance S10 | Room C

Notary Project: The Key To Secure Software Supply Chain
Yi Zha and Guillaume Gill
Friday April 4, 2025 13:45 - 14:15 BST
Level 3 | ICC Capital Suite 14-16

Don’t forget to check out the project booths!

Thank you!

Feedback welcome and appreciated!