KubeCon | CloudNativeCon

Europe 2023

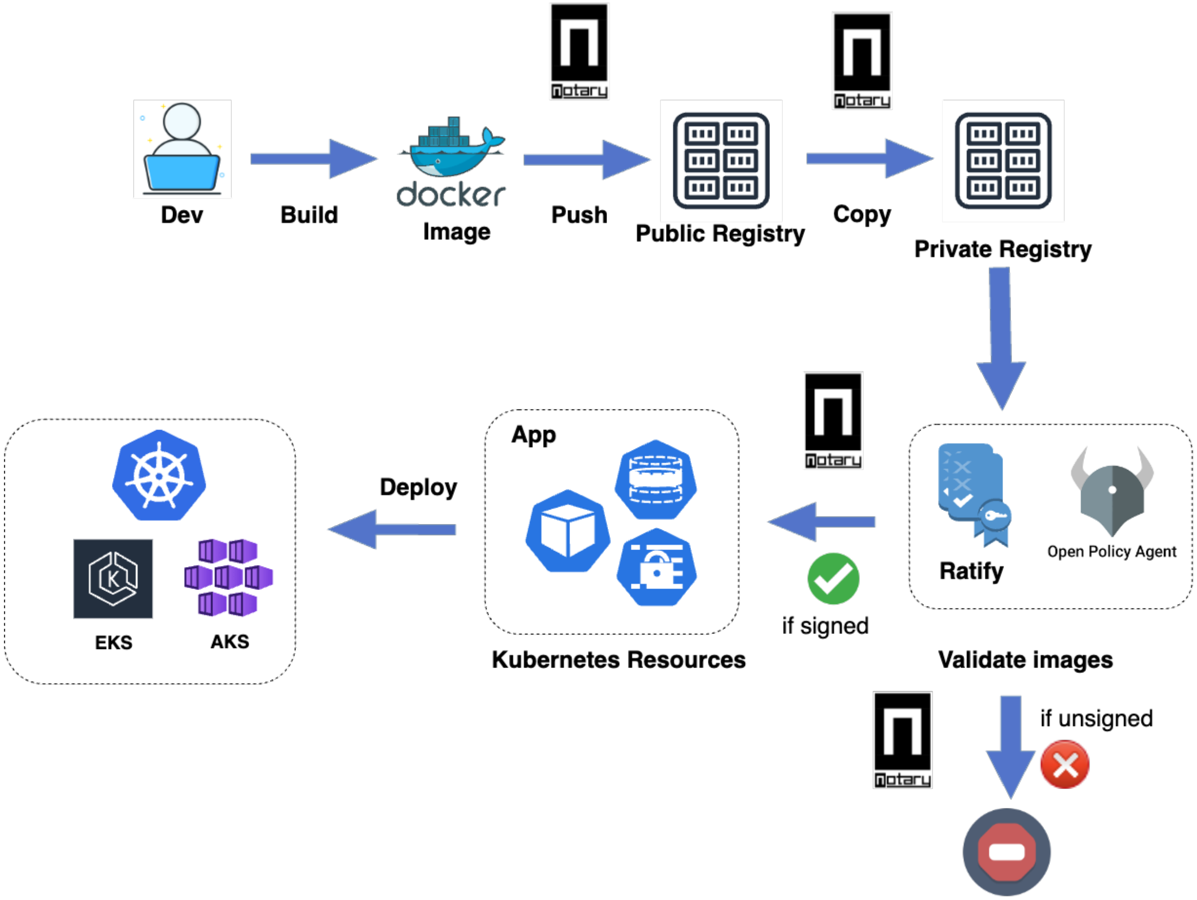
KubeCon | CloudNativeCon

Europe 2023

Securing the Container Supply Chain with Notary

Justin Cormack, CTO, Docker Inc.
Toddy Mladenov, Principal Product Manager, Microsoft

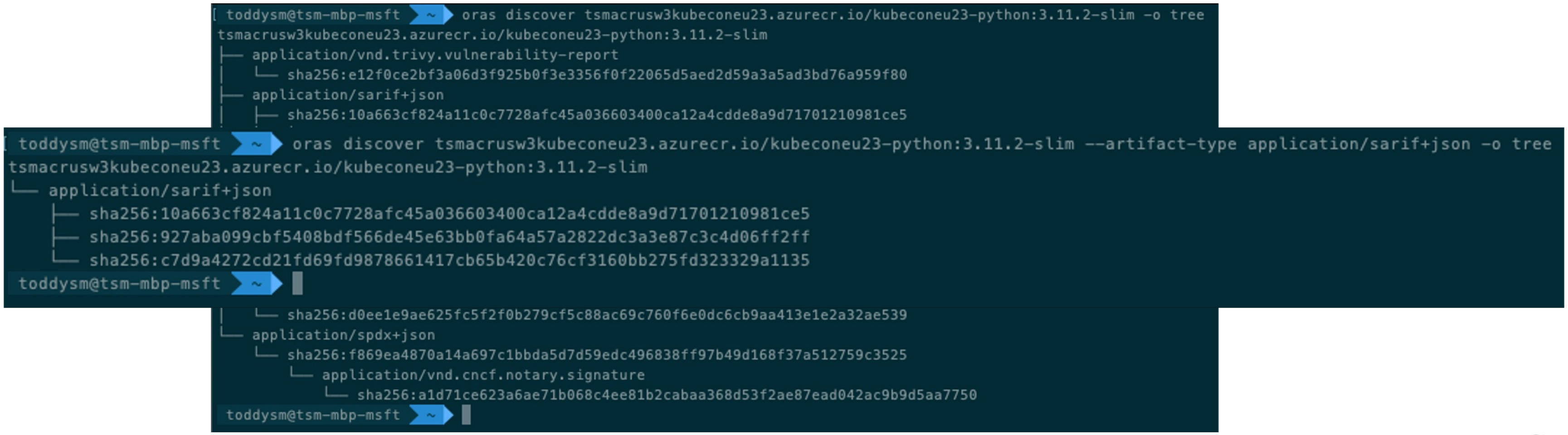
End-to-end Software Supply Chain



toddysm

Notary is Driving Innovation

notary
ORAS
OPEN CONTAINER INITIATIVE



```
[ toddysm@tsm-mbp-msft  ~  oras discover tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim -o tree
tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim
├── application/vnd.trivy.vulnerability-report
│   └── sha256:e12f0ce2bf3a06d3f925b0f3e3356f0f22065d5aed2d59a3a5ad3bd76a959f80
├── application/sarif+json
│   ├── sha256:10a663cf824a11c0c7728afc45a036603400ca12a4cdde8a9d71701210981ce5
│   └── sha256:d0ee1e9ae625fc5f2f0b279cf5c88ac69c760f6e0dc6cb9aa413e1e2a32ae539
└── application/spdx+json
    └── sha256:f869ea4870a14a697c1bbda5d7d59edc496838ff97b49d168f37a512759c3525
        └── application/vnd.cncf.notary.signature
            └── sha256:a1d71ce623a6ae71b068c4ee81b2cabaa368d53f2ae87ead042ac9b9d5aa7750
 toddysm@tsm-mbp-msft  ~ 
```

```
[ toddysm@tsm-mbp-msft  ~  oras discover tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim --artifact-type application/sarif+json -o tree
tsmacrusw3kubeconeu23.azurecr.io/kubeconeu23-python:3.11.2-slim
└── application/sarif+json
    ├── sha256:10a663cf824a11c0c7728afc45a036603400ca12a4cdde8a9d71701210981ce5
    ├── sha256:927aba099cbf5408bdf566de45e63bb0fa64a57a2822dc3a3e87c3c4d06ff2ff
    └── sha256:c7d9a4272cd21fd69fd9878661417cb65b420c76cf3160bb275fd323329a1135
 toddysm@tsm-mbp-msft  ~ 
```

toddysm

Notary is Based on Standards

IETF

JSON Web Signature (JWS)

CBOR

CBOR Object Signing and Encryption (COSE)

https://datatracker.ietf.org/doc/rfc9052/

Progress Since Last Kubecon

NEW RELEASE Candidate

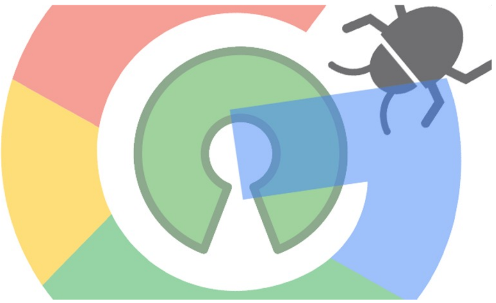
- Specifications Updates
  - RC.1 - Dec 6th 2022
    - Signature specification (support for both JWS and COSE)
    - Plugin specification
  - RC.2 - Feb 15th 2023
    - OCI image manifest support
- Notation
  - RC.1 - Dec 7th 2022
    - Remote signing
    - Trust store and trust policy
    - Troubleshooting improvements
  - RC.2 - Feb 16th 2023
    - Inspect signatures
    - Use of OCI image manifest
    - User defined metadata
  - RC.3 - Mar 7th 2023
    - Image manifest as default
    - Sign with on-demand keys
  - RC.4 - April 2023
    - Certificate revocation
    - Sign and verify local artifacts
    - Improved authentication experience
    - Security audit

Demos

- **Signing artifacts**
  recording, demo script
- **Verifying artifacts**
  recording, demo script
- **Troubleshooting**
  recording, demo script

DEMO

Notary Security



Google OSS-Fuzz

- Dec 26th 2022 - March 13th 2023
- 19 fuzz tests continuously running
  - Notation-go
  - Notation-core-go
  - Notary
- 2 issues
  - Security Advisory GHSA-87x9-7grx-m28v (CVE-2023-25656)
  - Dependency issue
- Fuzz report available
- CNCF blog announcement
- Thank you Ada Logics!

- Started Mar 20th 2023
- ETA for completion Apr 30th 2023
- Includes
  - Threat model
  - Comprehensive code review
- CVEs will be fixed in 90 days or before publishing the report
- Report is expected to be published in May 2023

Community Update

- 52 contributors
- 15 of those with 10+ PRs
- 9 releases for Notation CLI
- 8 releases for Notation-Go library
- 5 releases for Notation-Core-Go library
- 3 revisions of the signing specification
- Website update (notaryproject.dev)

What Is Next for Notation?

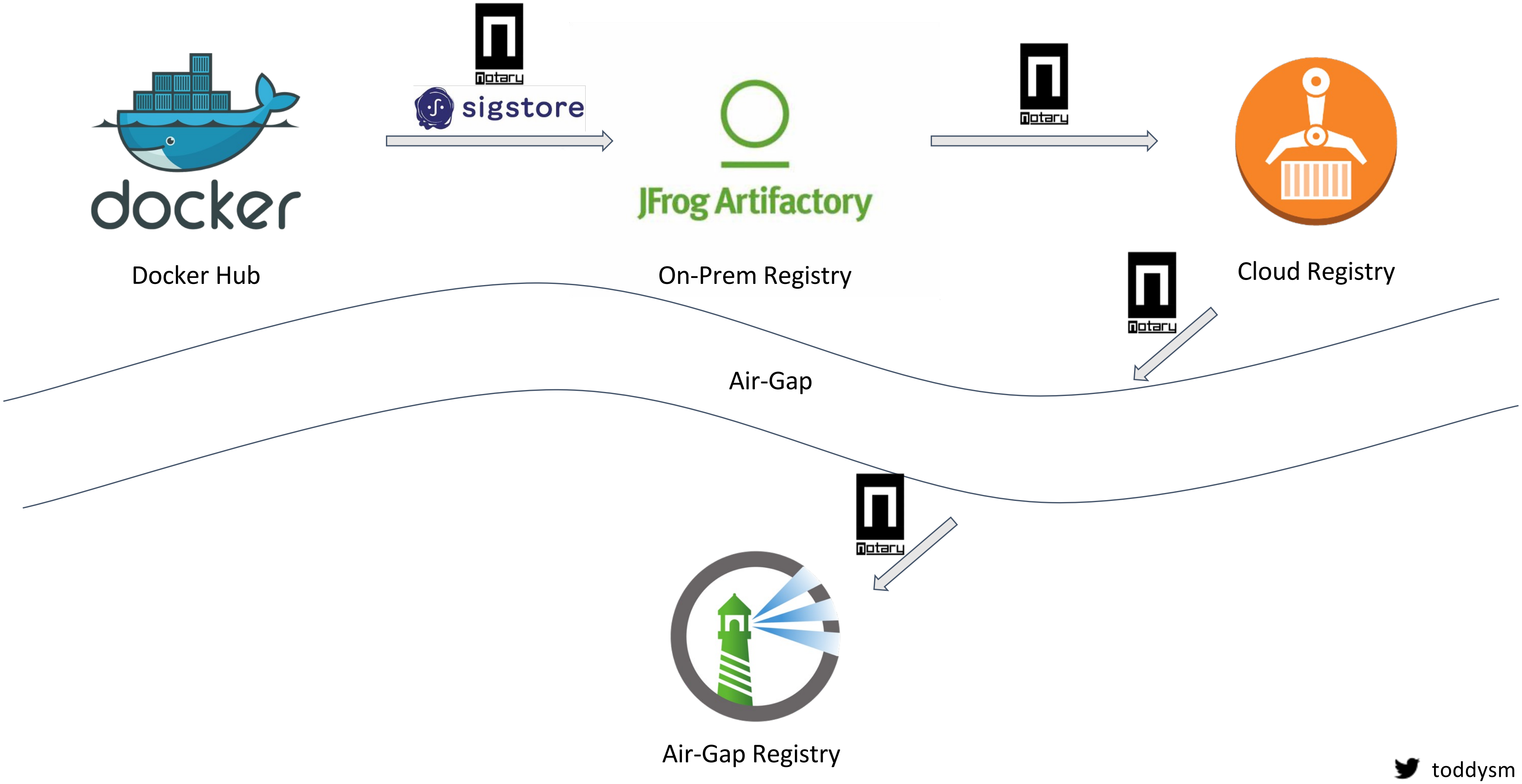
- New Capabilities
  - TSA
  - Certificate revocation
  - Multiple signature verification
- Usability Improvements
  - Structured inputs and outputs
  - Error message improvements
  - Scripting capabilities
- Troubleshooting
  - More debugging and verbose options

Demo

- **Signing local artifacts (experimental)**
  recording, demo script

DEMO

Portability



Docker Hub

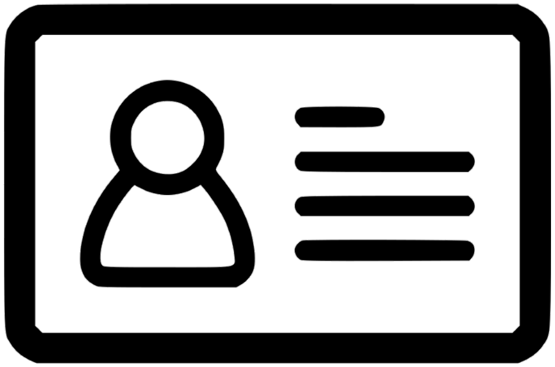
On-Prem Registry

Cloud Registry

Air-Gap

Air-Gap Registry

Strong Identity



Strong Identity

https://www.w3.org/TR/did-core/

Counter-Signatures and Transparency Log

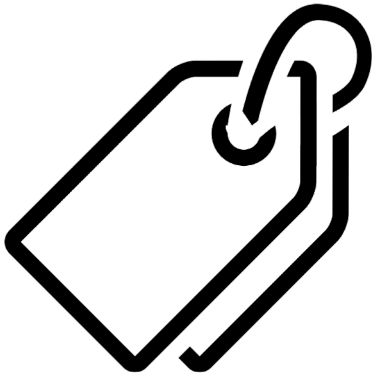
Counter Signatures

IETF

https://datatracker.ietf.org/group/scitt/about/

toddysm

Verifiable Metadata



Verifiable Metadata

VEX

SPDX

CycloneDX

SARIF

...

Learn More @ KubeCon EU 2023

KubeCon | CloudNativeCon Europe 2023

- Improve Vulnerability Management with OCI Artifacts - It Is That Easy!
  Itay Shakury, Aqua Security & Toddy Mladenov, Microsoft
- Checking the Chains at the Gate: Building Supply Chain Policies with Gatekeeper and Ratify
  Jeremy Rickard, Microsoft
- Kyverno Introduction and Deep Dive
  Charles-Edouard Brétéché, Nirmata & Jinhong Brejnholt, Saxo Bank

toddysm

Please scan the QR Code above
to leave feedback on this session