
KubeCon
CloudNativeCon
North America 2024

KubeCon

CloudNativeCon

North America 2024

Using Notary Project to Ensure Authenticity and Integrity of Artifacts within the Enterprise

Speakers

Tjark Rasche
Senior Cloud Software Engineer
Mercedes Benz Tech Innovation

Toddy Mladenov
Principal Product Manager
Microsoft

Agenda

1. Why authenticity and integrity matters?
2. So how do we get there?
    a. The dream scenario
    b. Challenges within enterprise environments
    c. What we need
    d. A step by step approach with Notary Project
3. What's new with the project?

Why authenticity and integrity matters?

Why integrity is needed

Zero Trust is King!

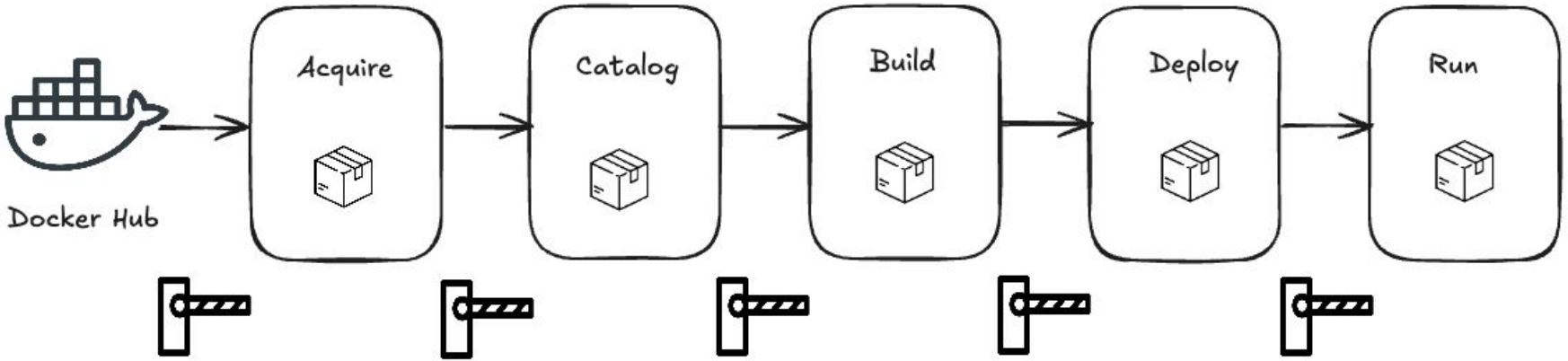
We don’t trust our applications

We don’t trust our users

We don’t trust our network

Why do we trust our artifacts?

Zero trust in the software supply chain

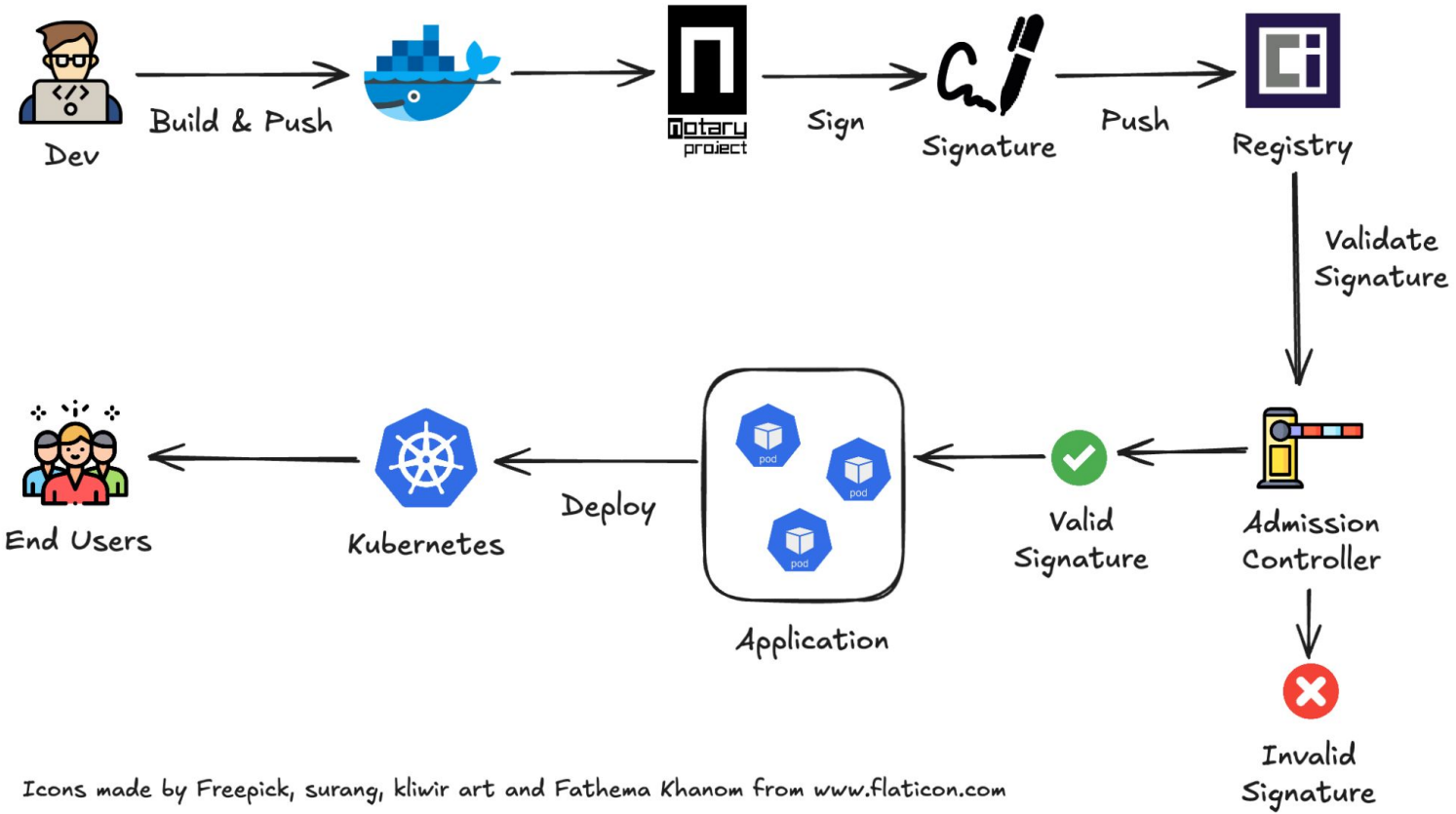


Do I trust the publisher?
Is the artifact tampered with?

Icons made by Freepik and pocike from www.flaticon.com

How do we get there?

The dream scenario



Icons made by Freepick, surang, kliwir art and Fathema Khanom from www.flaticon.com

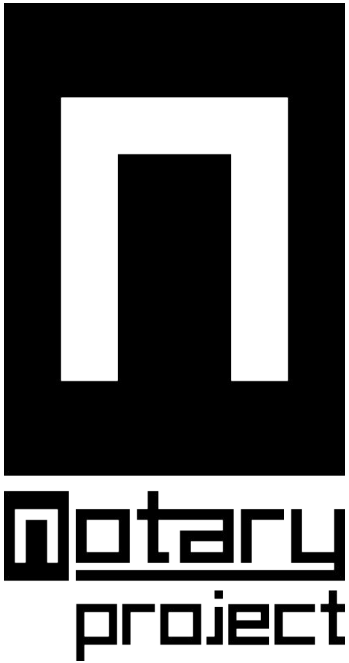
The Reality in Enterprise Environments

- “Grown”, heterogeneous infrastructure
- Existing trust infrastructure(s) (PKI, Secret Store)
- Multiple (maybe even an unknown number) stacks
- Lots of external suppliers
  - Additional unknown infrastructure
  - Maybe different artifact registries etc.
- A lot of legacy software and application runtimes

What do we need in a tool do cope with these challenges?

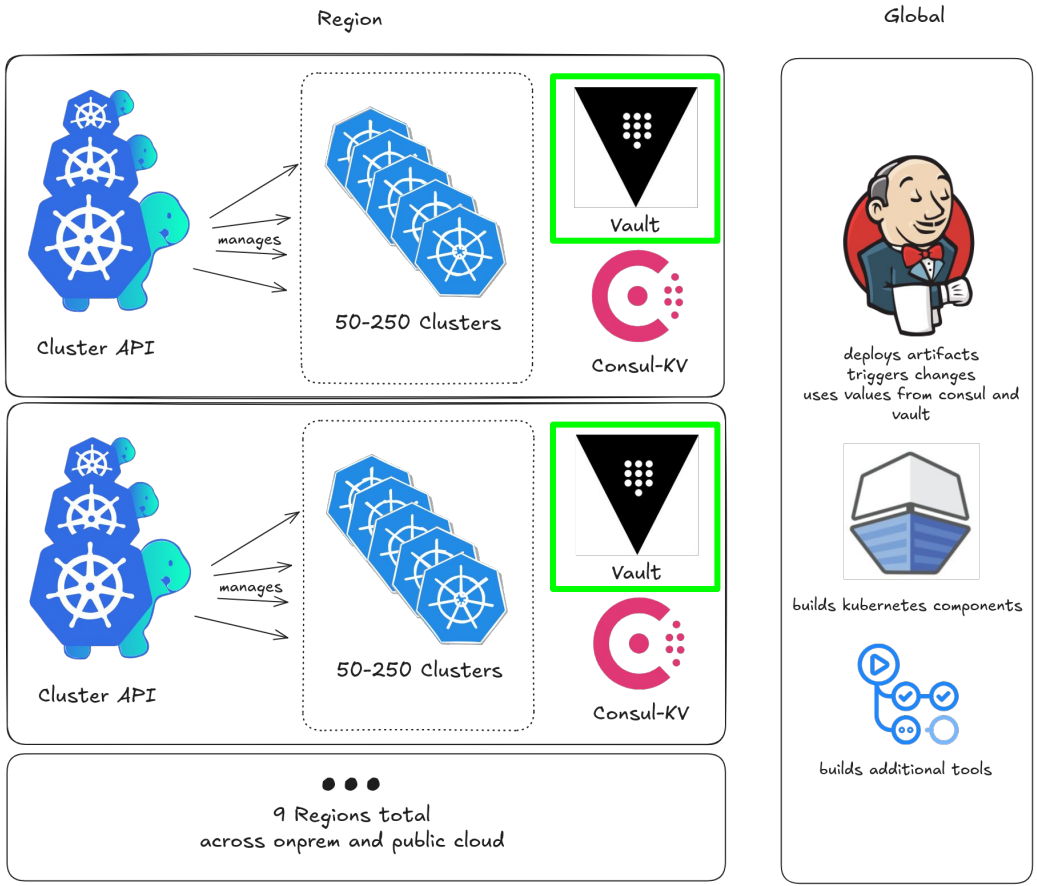
What we need

- Artifact Signing
  - OCI images
  - other artifacts
- With own Certificates
- Flexible support for keyvaults etc.

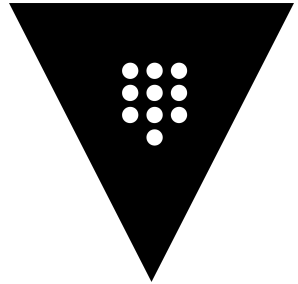


A practical example

Platform Overview



What’s the Vault doing



Global CA per region

CA for every cluster

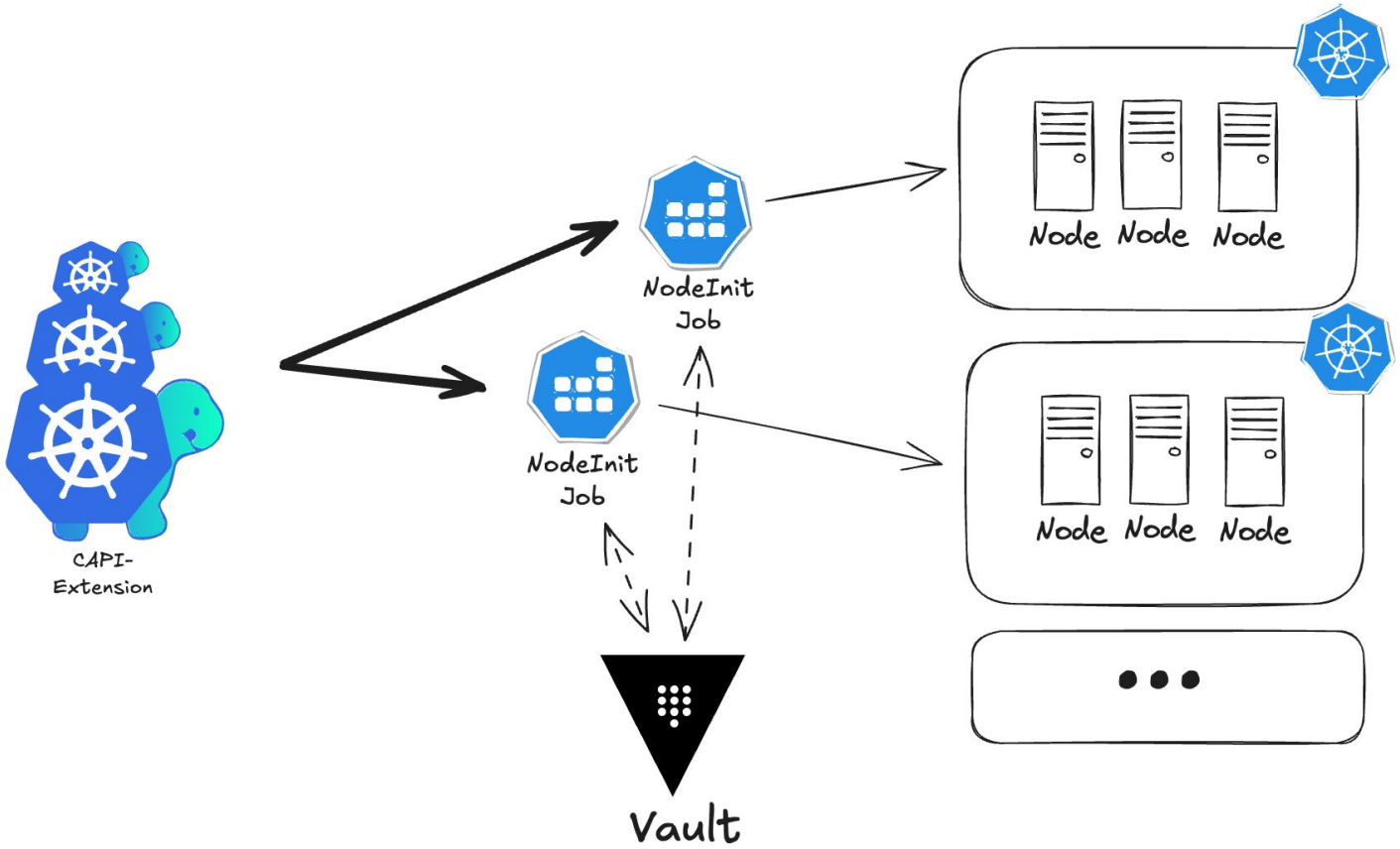
Used for signing user certs

Secrets store

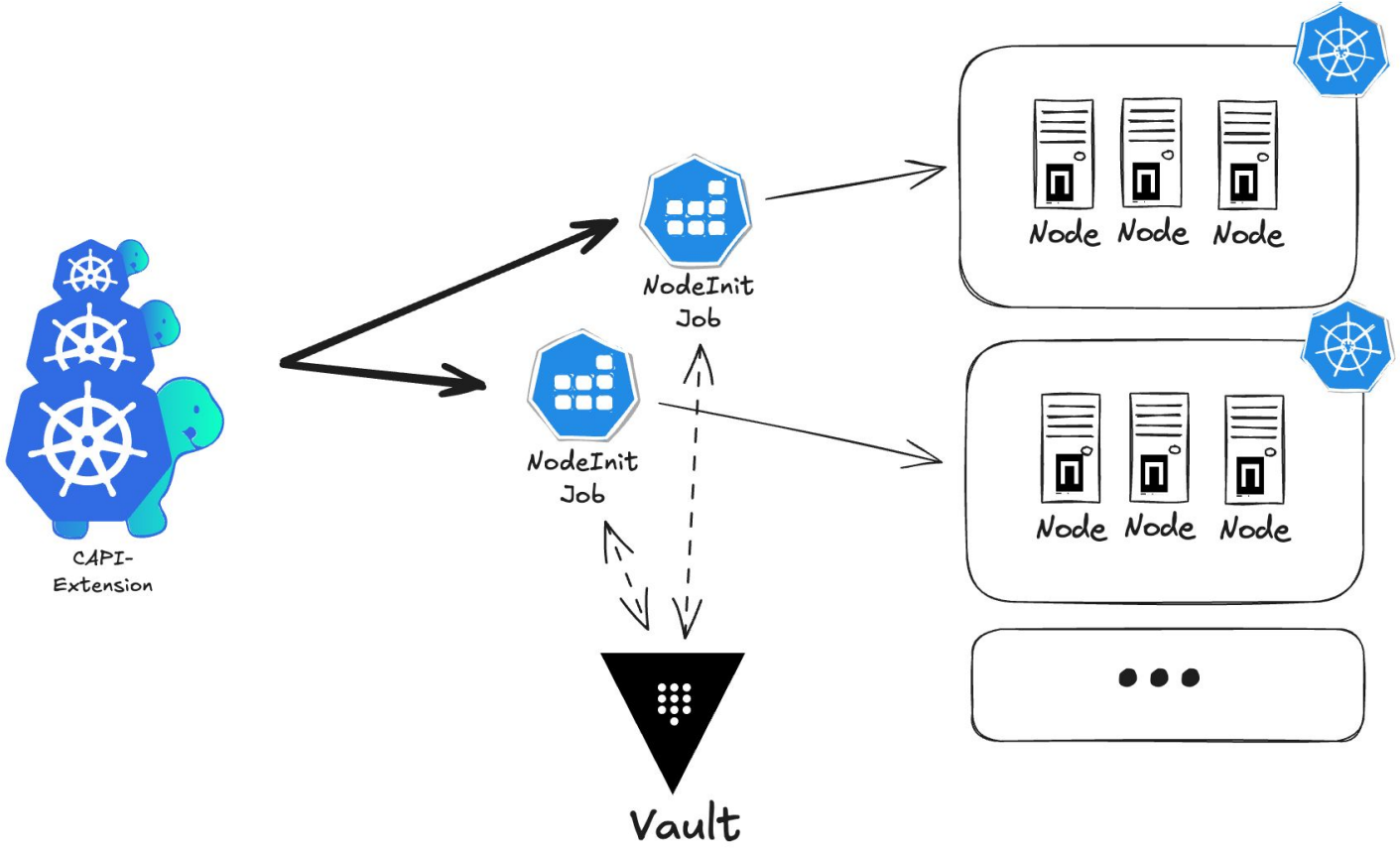
Build Side


```
./notation sign --id "myNotationTestKey" --plugin "hc-vault" example.com/kubelet@sha256:digest
```

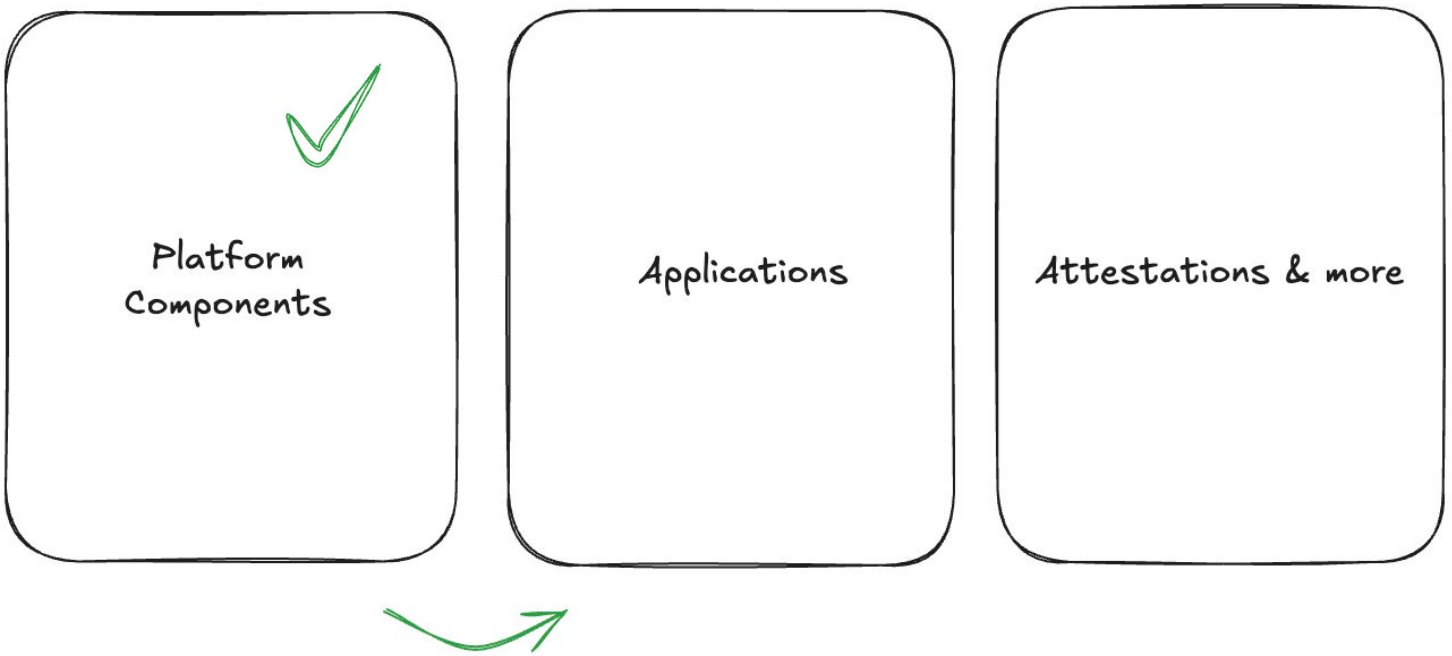
Existing PKI



Integrate Notation



Incremental Adoption



Learnings

Existing PKI can be used

Notation integrates well everywhere

Future proof thanks to pluggable architecture

Notary Project Update

Releases

- Notation CLI + libraries v.1.2.0 (Aug 29th, 2024)
  - Support for OCI v1.1.0 image and distribution specs
  - RFC 3161 compliant timestamping support
- Notation CLI GitHub Action v1.2.0 (Sep 27th, 2024)
- Notation CLI + libraries v1.3.0-rc1 (Oct 9th, 2024)
  - Revocation support using CRL
- Notation CLI + libraries v1.1.2 (Oct 15th, 2024)
- Security Audit covering Notation CLI, Notation Go libraries, and tcpclient-go library

Ecosystem

- Bitnami-packaged containers and Helm charts use Notary Project tooling for signing (Mar 2024)
- Flux 2.3 supports Notary Project signature verification (May 2024)
- Alibaba open-sourced Cloud Secret Manager plugin for Notation CLI (Aug 2024)

Roadmap

- Notation v2.0.0 (Mar 2025)
  - Blob signing
  - Using OCI 1.1 referrers API by default
- Notation v2.1.0 (Jun 2025)
  - Attestations support
  - Registry-wide trust policies

Q&A & Feedback