KubeCon CloudNativeCon

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

AI_dev

Open Source GenAI & ML Summit

China 2024

KubeCon

CloudNativeCon

China 2024

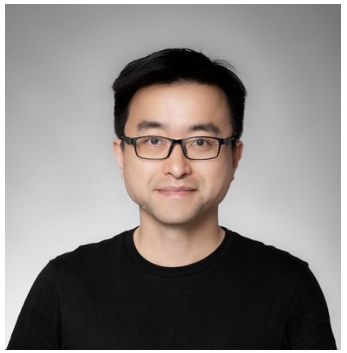
Safeguarding Cloud Native Supply Chain

Notary Project Intro & What's Next

Yi Zha, Senior Product Manager, Microsoft

Mostafa Radwan, Principal Consultant, CloudRoads

About us



Yi Zha
Sr Product Manager at Microsoft
Maintainer at CNCF project Notary Project
Cloud Native Supply Chain Security and Ecosystem

Mostafa Radwan
Principal Consultant at CloudRoads
CNCF Chicago Community Group Organizer

Agenda

- Background
- Notary Project Overview
- Features & Milestones
- User Stories
- Demo
- Q&A

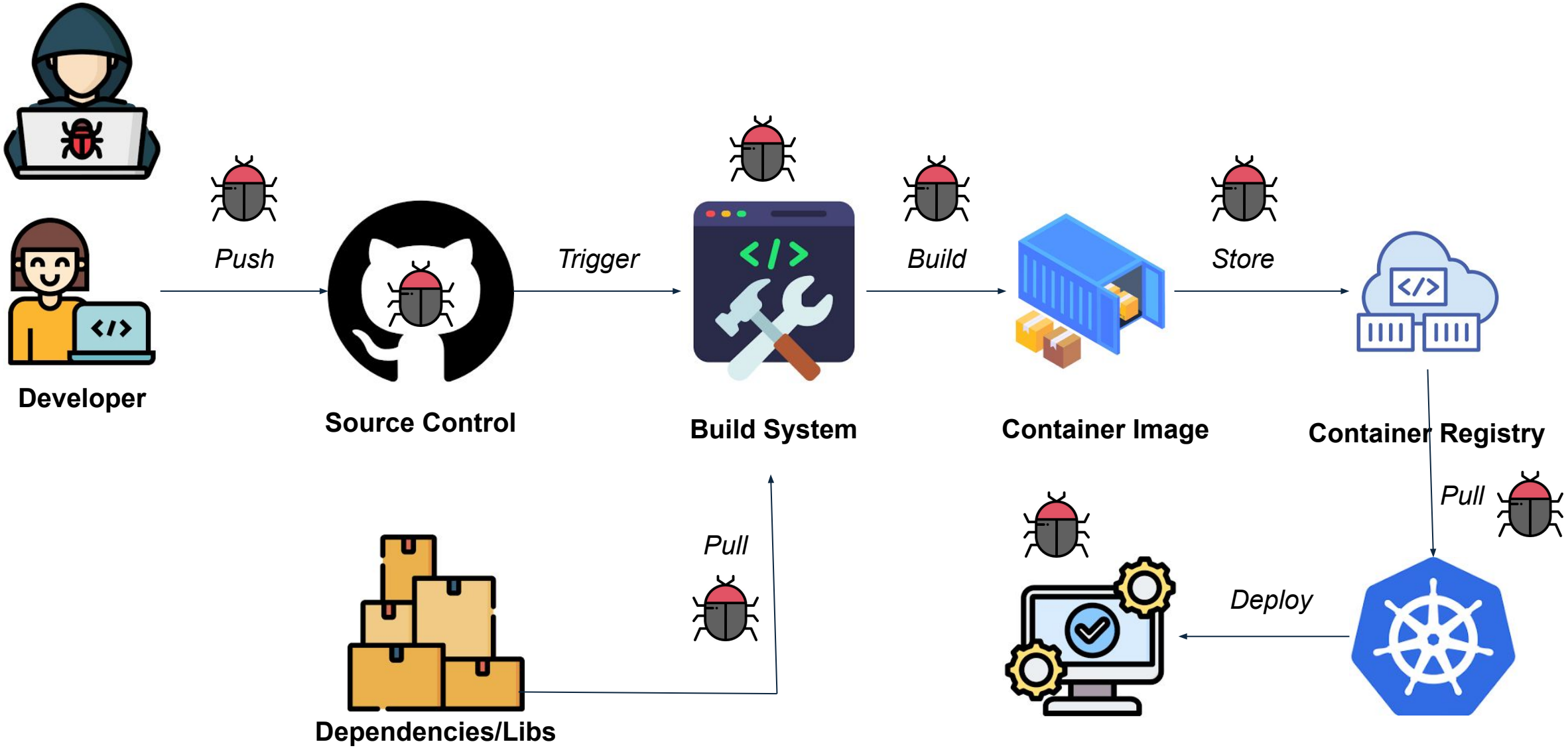
Background

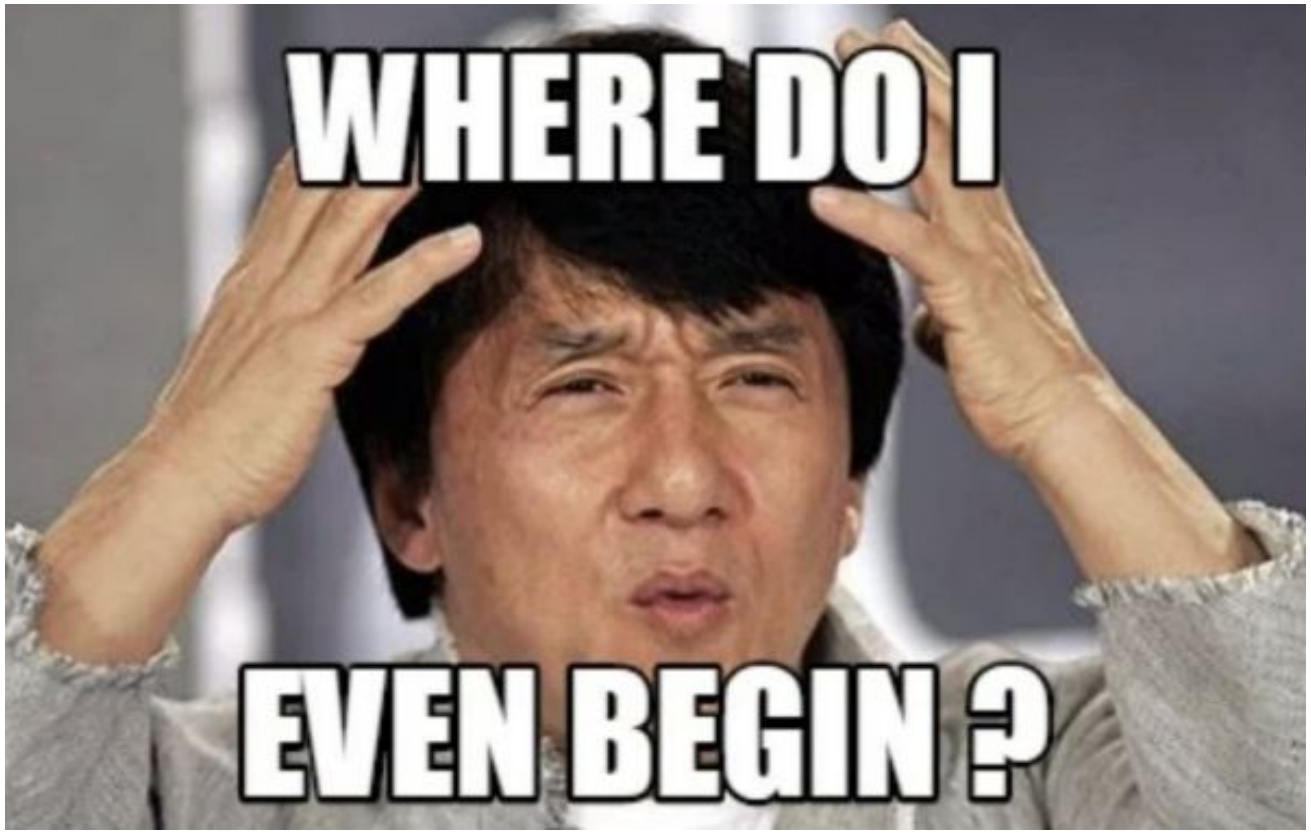
“ 91% of Organizations experienced software supply chain attacks last year ”
– The Security Magazine, February 2024 🔗

“ There has been a 742% average annual increase in software supply chain attacks over the past 3 years ”
– The State of Software Supply Chain Report 2023 🔗

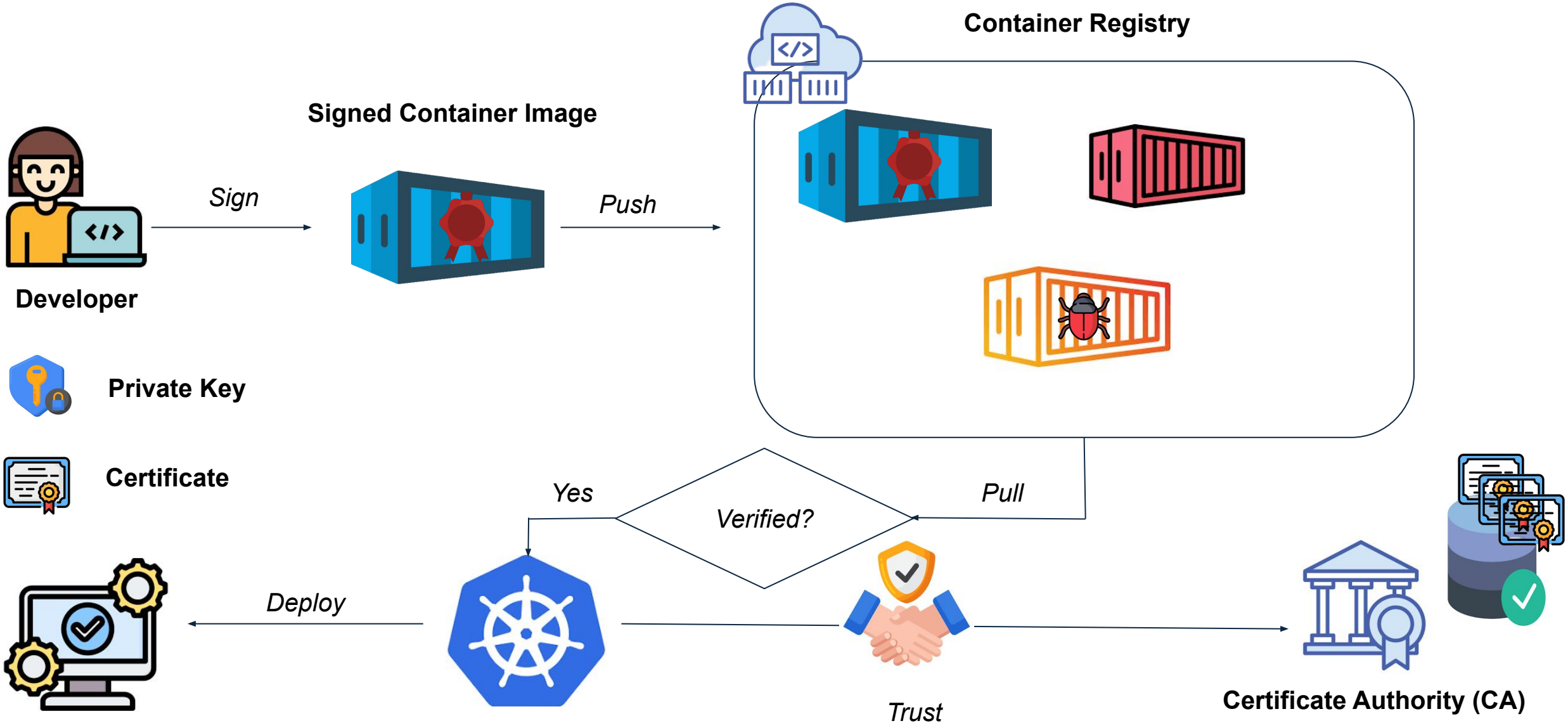
“ Software supply chain attacks have impacted 62% of organizations surveyed ”
– The Software Supply Chain Security Report 2022 🔗

Understand The Problem




WHERE DO I
EVEN BEGIN ?

Signing Container Images



Notary Project - Our Mission

Securing software supply chains by using authentic container images and artifacts.

https://notaryproject.dev

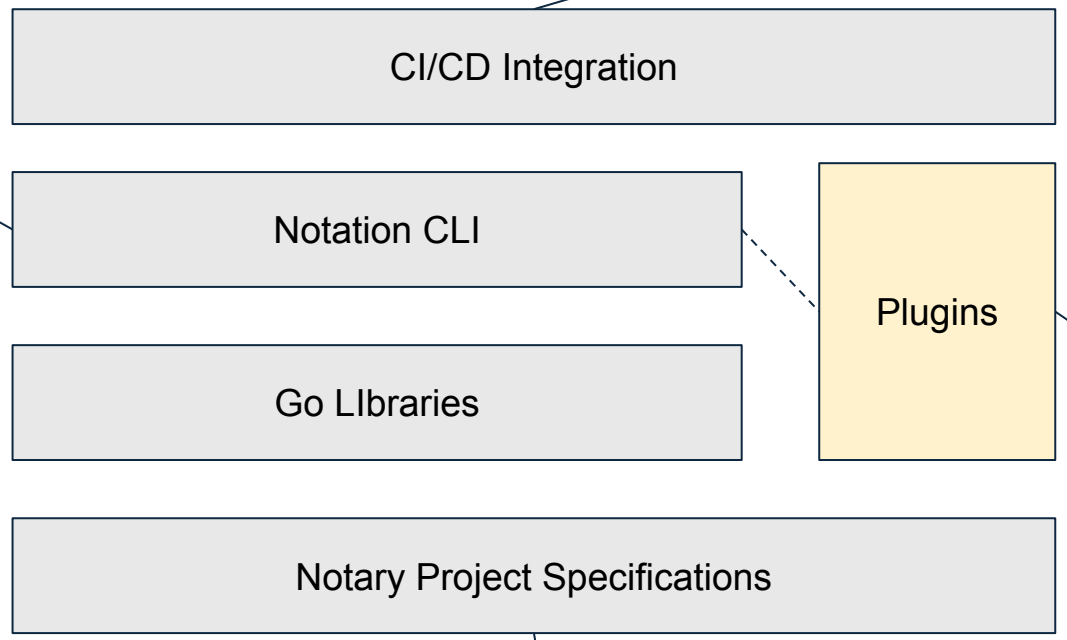
The Benefits of Notary Project

- ★ **Smooth PKI Integration**: Ensures security, privacy, and data compliance.
- ★ **Extensibility**:
  - KMS Support: Azure Key Vault, AWS Signer, Alibaba Cloud Secret Manager plugin, and Hashicorp Vault.
  - Custom Plugins: Allows for the integration of custom plugins for signing and verification workflow
- ★ **Signature Portability**: Compatible with OCI v1.1
- ★ **Signature Formats**: JWS and COSE.
- ★ **Fine-tuned Trust Policies**: Operates on a zero-trust model, ensuring no implicit trust by default.
- ★ **Security Audit**: Undergoes third-party audits to ensure the highest security standards and code quality.

Notary Project: sub-projects

https://github.com/notaryproject

- GitHub Actions
- Azure DevOps Tasks



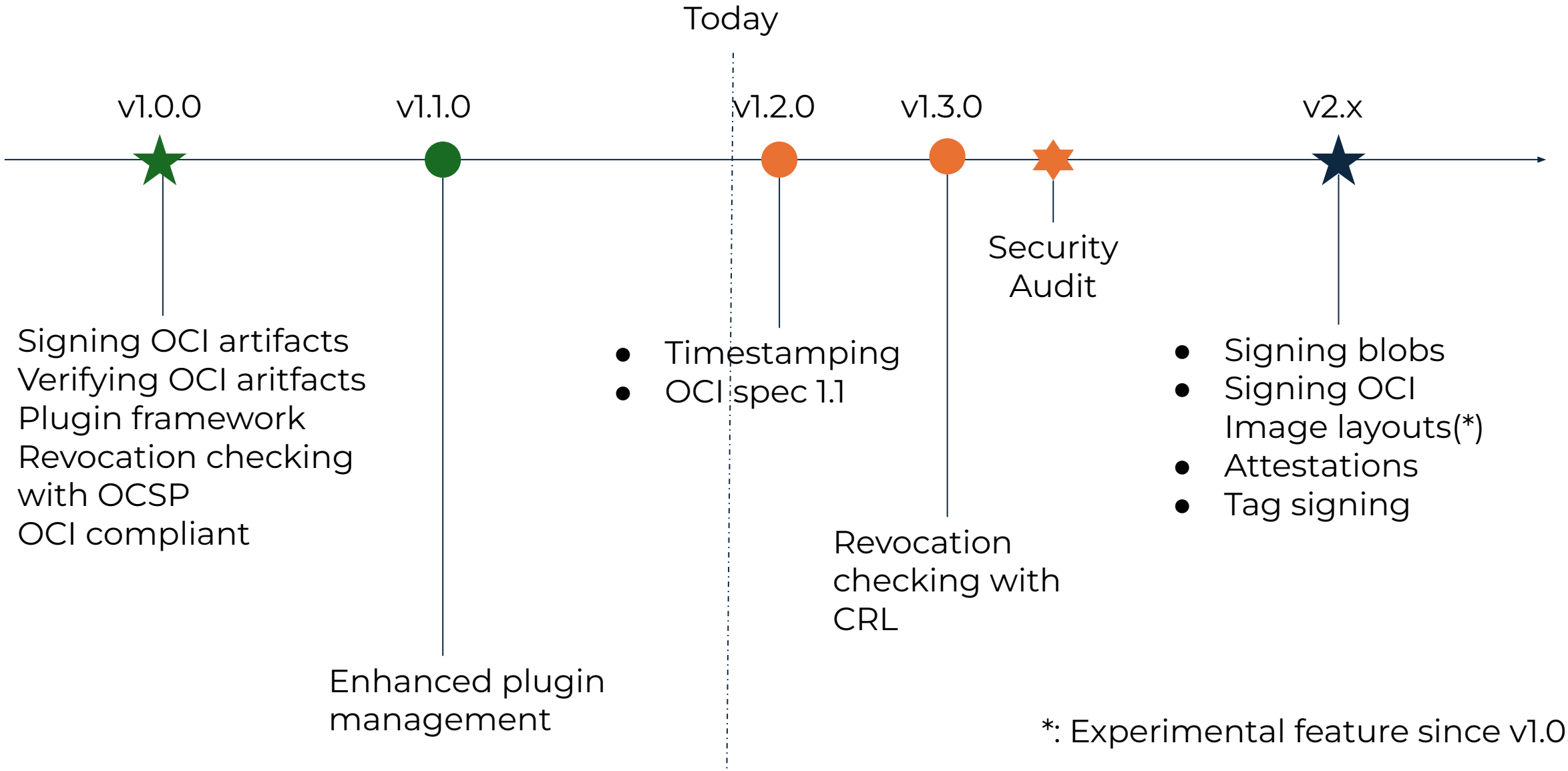
The client tool

- Notation Go Libraries
- TSP Client Go library

- AWS Signer
- Azure Key Vault
- Azure Trusted Signing
- Venafi CodeSign
- Hashicorp Vault
- Alibaba Cloud Secret Manager

- Signature spec (OCI 1.1 compliant)
- Signing and verification spec
- Trust Policy and Trust Store spec
- Plugin spec

Notation Features & Milestones



*: Experimental feature since v1.0.0

User Stories

Harbor, an open source registry, secures artifacts with policies ensuring images are scanned for vulns and signed as trusted using Cosign or Notation

While primarily a Kubernetes policy engine, Kyverno can be used alongside other tools to enhance container image security by verifying signatures

Demo

- Signing container images
  - notation sign
  - notation list
  - notation inspect

- Verifying container images
  - Trust policy & Trust store
  - notation verify

- Trust policy & Trust store

- Timestamping

Q & A

Thank You!

KubeCon CloudNativeCon China 2024 | THE LINUX FOUNDATION OPEN SOURCE SUMMIT | AI_dev

Connect with us :

Yi Zha yizha1@microsoft.com

Mostafa Radwan mr@cloudroads.com

Slack: https://app.slack.com/client/T08PSQ7BQ/CQUH8U287

Community meeting: https://notaryproject.dev/community

Website: https://notaryproject.dev

Notary Project