Chainguard

Keyless Signing with Tekton and Sigstore

Billy Lynch

September, 2022

About Me

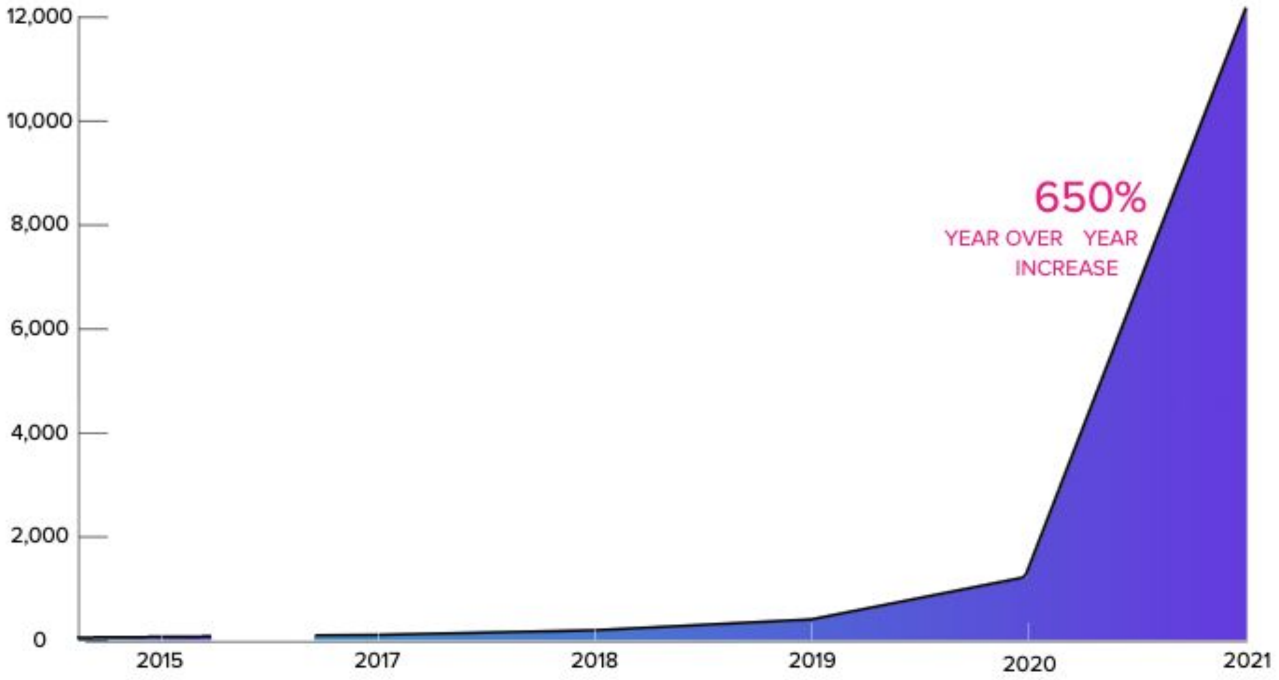
Chainguard

- Staff Software Engineer @ Chainguard
- Maintainer for:
  - [tektoncd/chains]
  - [sigstore/gitsign]

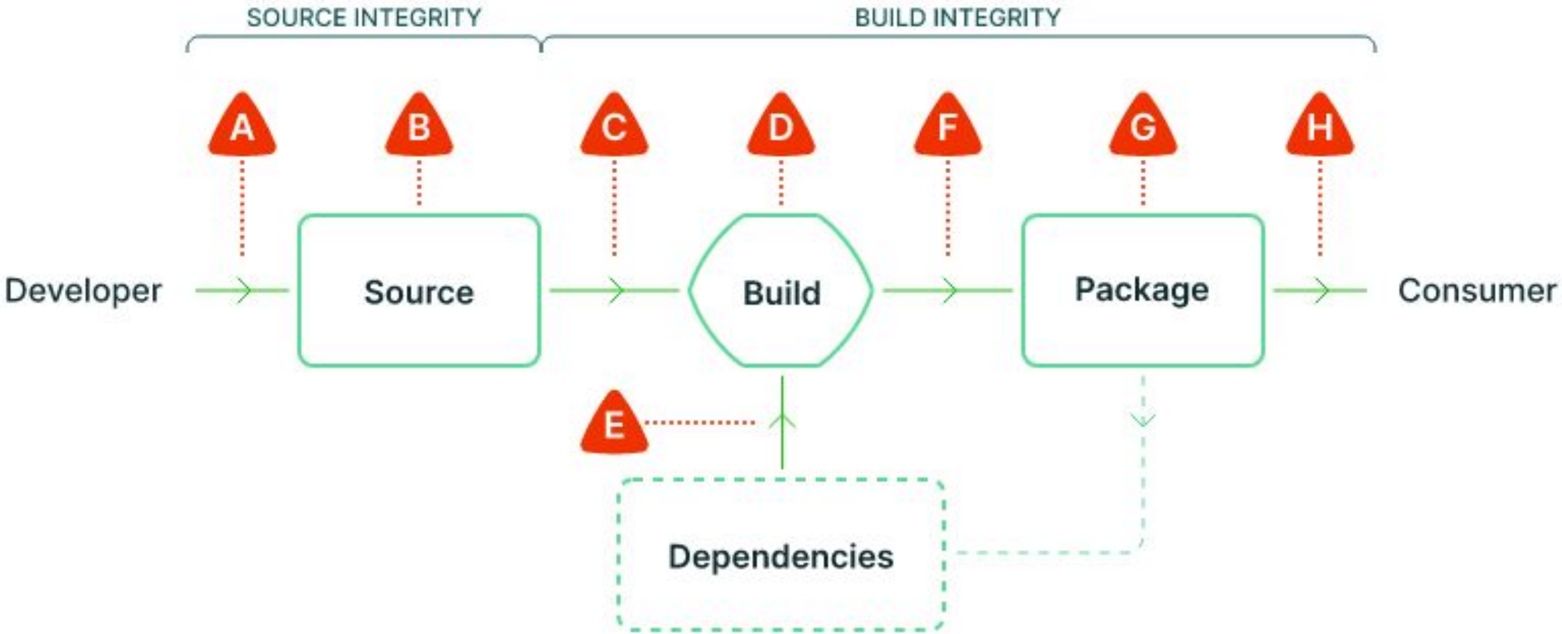
Previously:

- Cloud Build
- Cloud Source Repositories
- Google Code

Software supply chain attacks increased 650% in 2021.



https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021



SOURCE INTEGRITY

BUILD INTEGRITY

A

B

C

D

F

G

H

Developer

Source

Build

Package

Consumer

E

Dependencies

A Submit unauthorized change

B Compromise source repo

C Build from modified source

D Compromise build process

E Use compromised dependency

F Upload modified package

G Compromise package repo

H Use compromised package

https://slsa.dev/spec/v0.1/threats

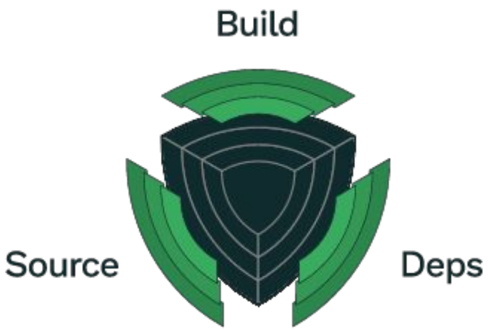
Supply chain Levels for Software Artifacts, or SLSA (salsa).

The industry road map for software supply chain integrity.
slsa.dev

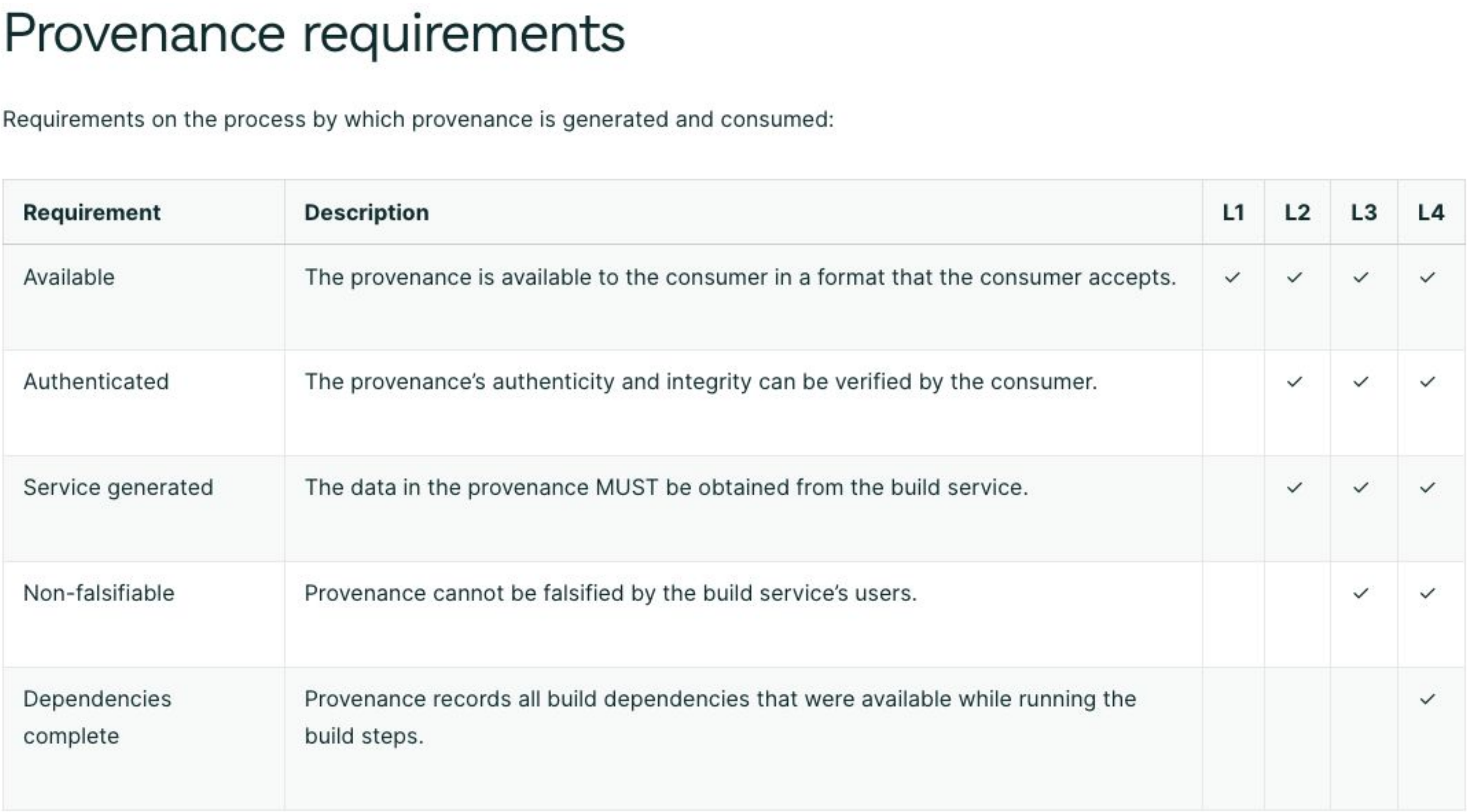
SLSA

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SLSA Levels



Level 1	Easy to adopt, giving you supply chain visibility and being able to generate provenance
Level 2	Starts to protect against software tampering and adds minimal build integrity guarantees
Level 3	Hardens the infrastructure against attacks, more trust integrated into complex systems
Level 4	The highest assurances of build integrity and measures for dependency management in place



Provenance requirements

Requirements on the process by which provenance is generated and consumed:

Requirement	Description	L1	L2	L3	L4
Available	The provenance is available to the consumer in a format that the consumer accepts.	✓	✓	✓	✓
Authenticated	The provenance's authenticity and integrity can be verified by the consumer.		✓	✓	✓
Service generated	The data in the provenance MUST be obtained from the build service.		✓	✓	✓
Non-falsifiable	Provenance cannot be falsified by the build service's users.			✓	✓
Dependencies complete	Provenance records all build dependencies that were available while running the build steps.				✓

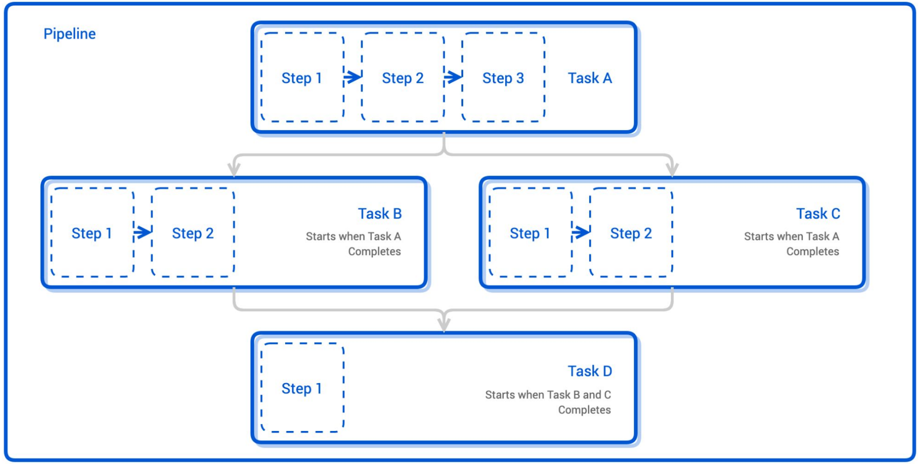
https://tekton.dev

https://sigstore.dev

Tekton

Cloud Native CI/CD

```
apiVersion: tekton.dev/v1beta1
kind: Task
metadata:
  name: hello
spec:
  steps:
  - name: echo
    image: distroless.dev/alpine-base
    script: |
      echo "Hello World!"
```



Pipeline

Step 1 Step 2 Step 3 Task A

Step 1 Step 2 Task B Starts when Task A Completes

Step 1 Step 2 Task C Starts when Task A Completes

Step 1 Task D Starts when Task B and C Completes

Demo

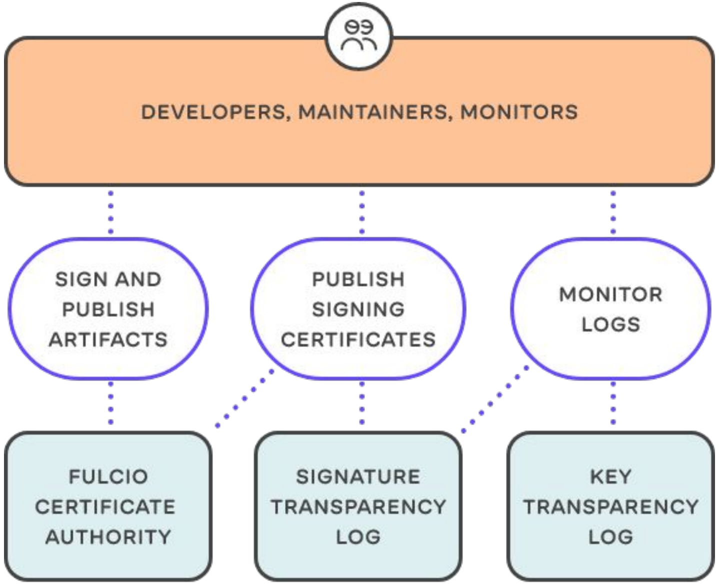
Tekton Chains

- Observes your Tekton TaskRuns and PipelineRuns, automatically signs:
  - Build configuration
  - Images
- Runs in a different namespace separate from user code.
- Supports Sigstore keyless mode w/ Cosign signatures!

Sigstore

sigstore

- Three main components:
  - **Tooling**: Developer tooling for signing software using Rekor and Fulcio (i.e. cosign, gitsign, etc.)
  - **Rekor**: Public transparency log for supply chain metadata
  - **Fulcio**: Free, OpenID Connect based Certificate Authority



DEVELOPERS, MAINTAINERS, MONITORS

SIGN AND PUBLISH ARTIFACTS

PUBLISH SIGNING CERTIFICATES

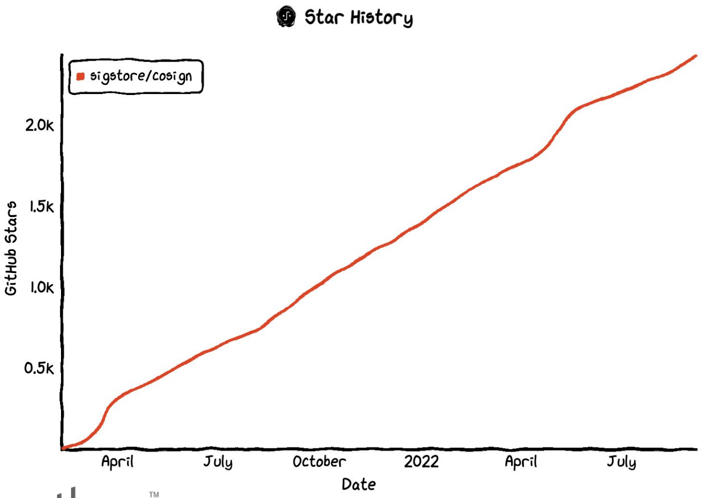
MONITOR LOGS

FULCIO CERTIFICATE AUTHORITY

SIGNATURE TRANSPARENCY LOG

KEY TRANSPARENCY LOG

Sigstore Adoption



python™ Package Index

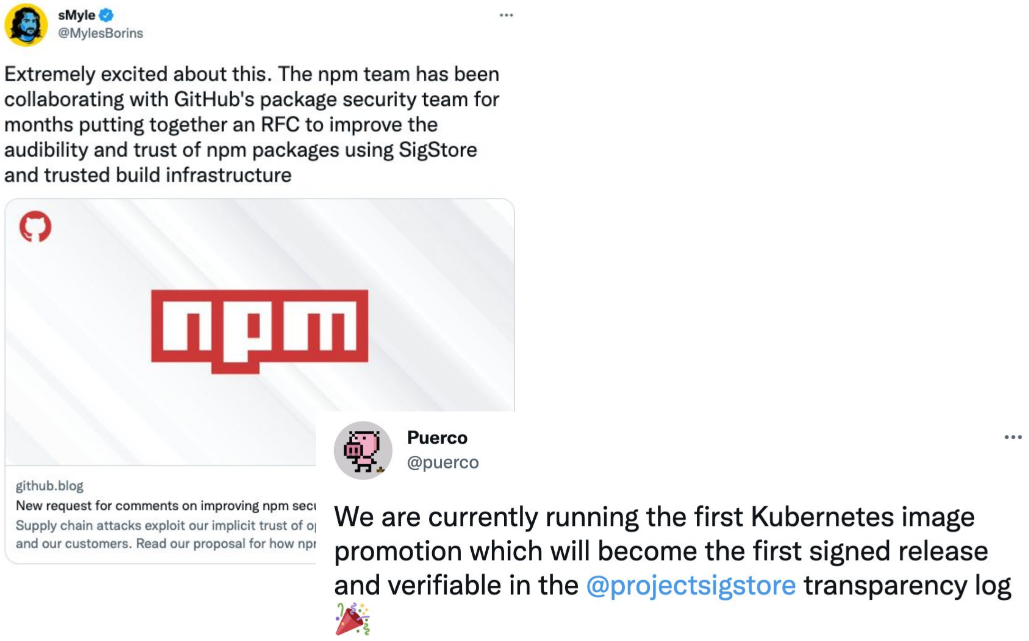
npm

Maven

OPEN CONTAINER INITIATIVE

RubyGems

TEKTON



sMyle
@MylesBorins

Extremely excited about this. The npm team has been collaborating with GitHub's package security team for months putting together an RFC to improve the audibility and trust of npm packages using SigStore and trusted build infrastructure

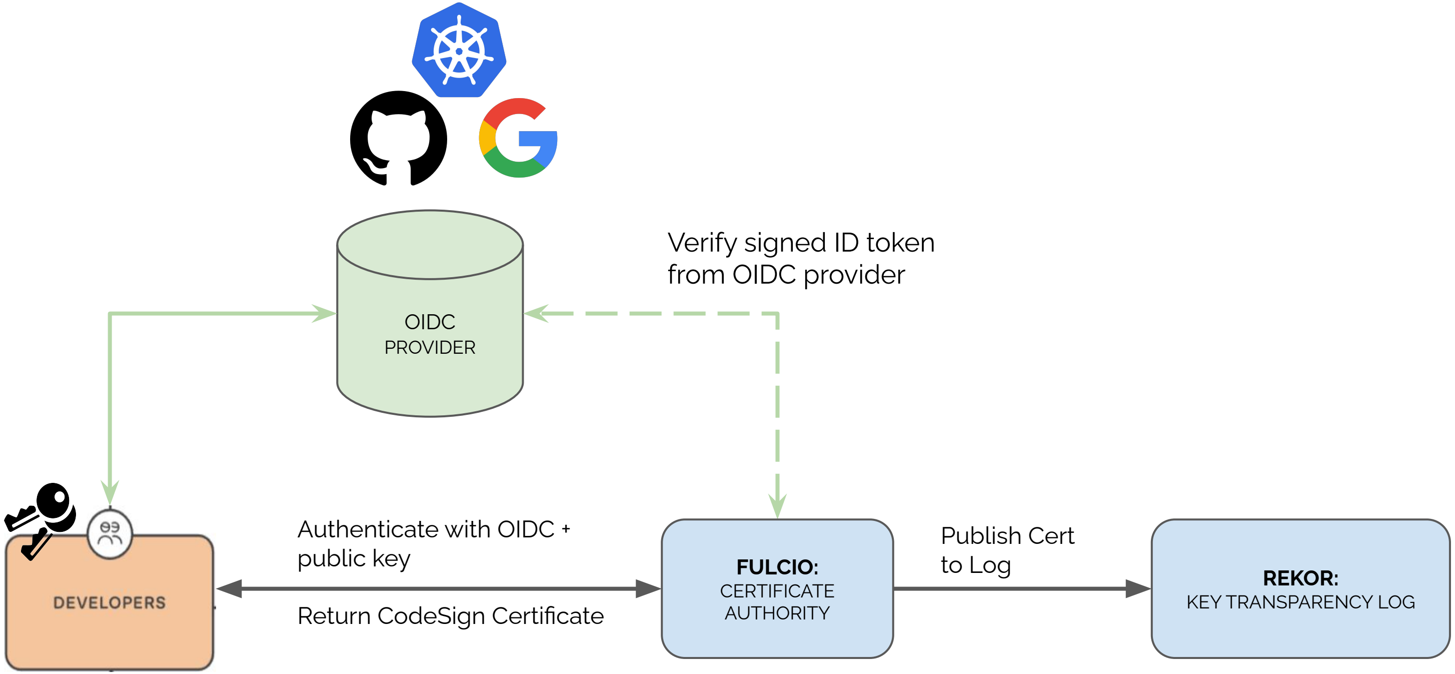
github.blog
New request for comments on improving npm secu
Supply chain attacks exploit our implicit trust of o
and our customers. Read our proposal for how npr

Puerco
@puerco

We are currently running the first Kubernetes image promotion which will become the first signed release and verifiable in the @projectsigstore transparency log 🎉

[From Kubernetes With ❤️ Open Tools For Open, Secure Supply Chains - Adolfo García Veytia]
Tuesday, September 13 • 09:00 - 09:40

Sigstore - Keyless Signing



OIDC
PROVIDER

Verify signed ID token
from OIDC provider

DEVELOPERS

Authenticate with OIDC +
public key

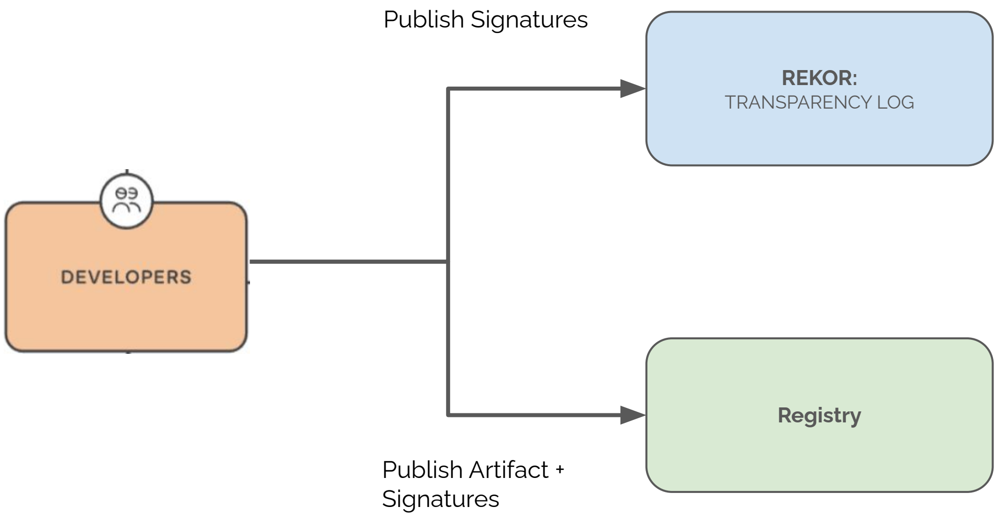
Return CodeSign Certificate

FULCIO:
CERTIFICATE
AUTHORITY

Publish Cert
to Log

REKOR:
KEY TRANSPARENCY LOG

Sigstore - Keyless Signing



Demo

What's next

TEKTON

Non-falsifiability

- Trusted resources
- SPIFFE/SPIRE

SLSA Level 4

- Hermetic builds
- More artifact types

sigstore

- Sigstore GA
- More artifact types
    - Git, RubyGems, PyPI, npm, Rust crates, Java, …
- Enforcement - Policy controllers, etc.

How to get involved

- Tekton Community
- Tekton Working Groups
  - Supply Chain Security
  - Chains

- Sigstore Community
- SLSA Community
- OpenSSF Working Groups
  - Supply Chain Integrity
  - Securing Software Repositories

Thanks!

Billy Lynch

billy@chainguard.dev

github.com/wlynch

https://tekton.dev

https://sigstore.dev

https://slsa.dev

sigstore gitsign

Gitsign – Keyless Git Commit Signing - Billy Lynch
Wednesday, September 14 • 15:15 - 15:55