Criteria and Attestation Approaches for Code Provenance

Dan Lorenc
Founder and CEO, Chainguard
dlorenc@chainguard.dev
twitter.com/lorenc_dan

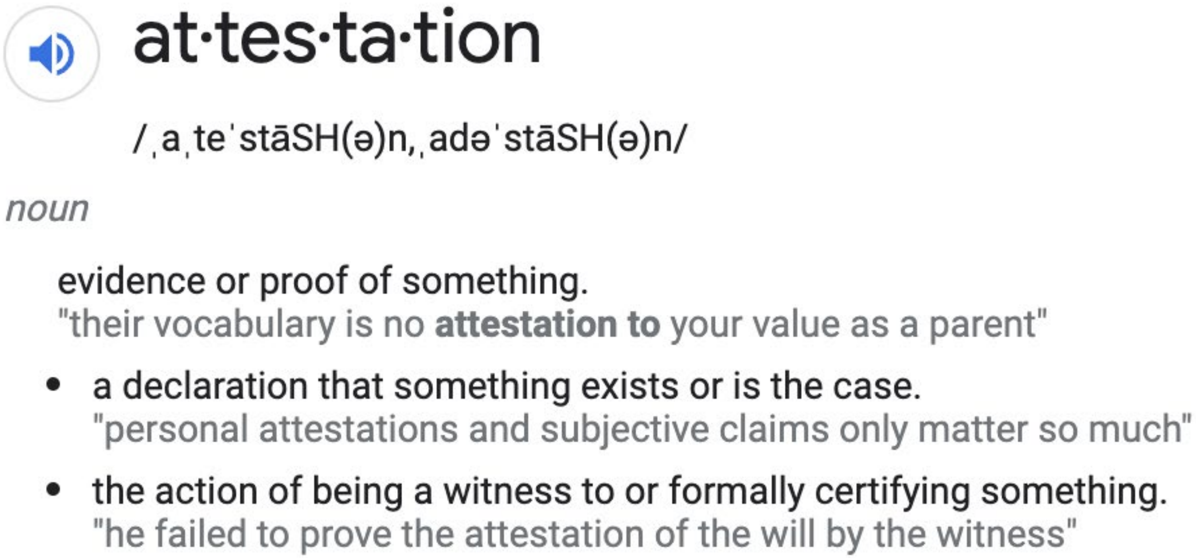
Agenda

- Attestations explained
- Different Types of Attestations
    - In-Toto, Hardware, TPM
- Attestation Use Cases
- Attestation Gotchas

Overall Goals in Code Provenance

- Cryptographically-verifiable information for every step in a supply chain
- Going from an artifact all the way back to the keyboard code was written on and the machines code was built on
- TPMs and FIDO2
- Ability to make policy decisions based on cryptographically verifiable metadata

Attestations



at·tes·ta·tion

/ˌaˌteˈstāSH(ə)n,ˌadəˈstāSH(ə)n/

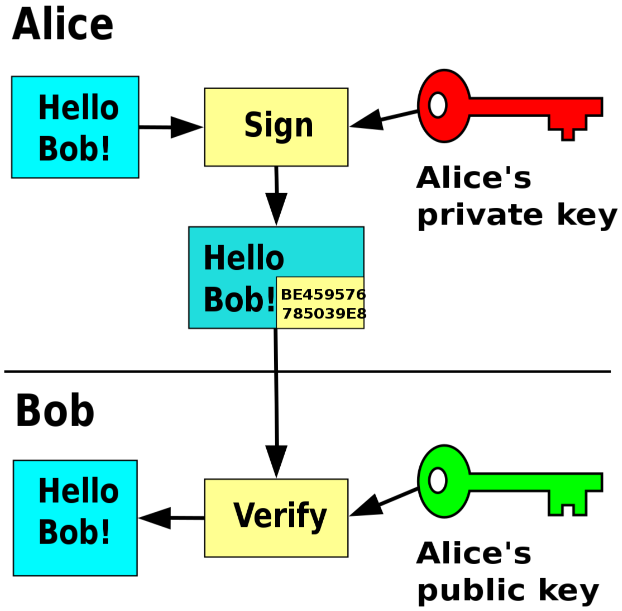
noun

evidence or proof of something.
"their vocabulary is no **attestation to** your value as a parent"

- a declaration that something exists or is the case.
  "personal attestations and subjective claims only matter so much"
- the action of being a witness to or formally certifying something.
  "he failed to prove the attestation of the will by the witness"

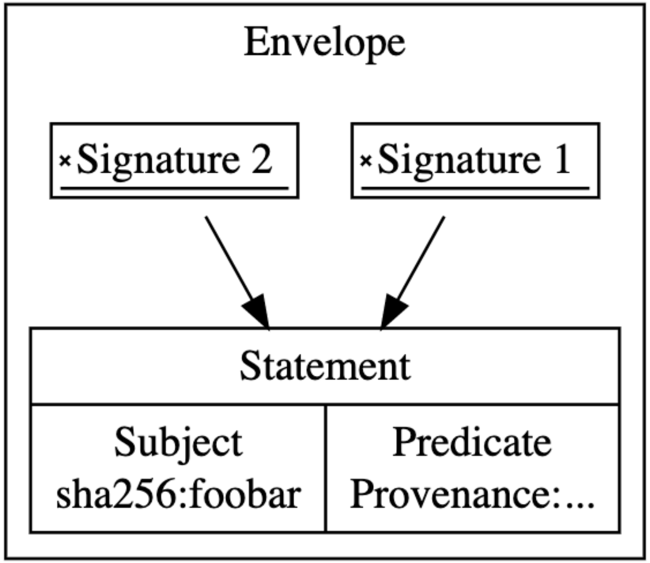
Attestations vs. Signatures

Signatures are a tool and a primitive, **not** an answer or a solution!



In-Toto Attestations

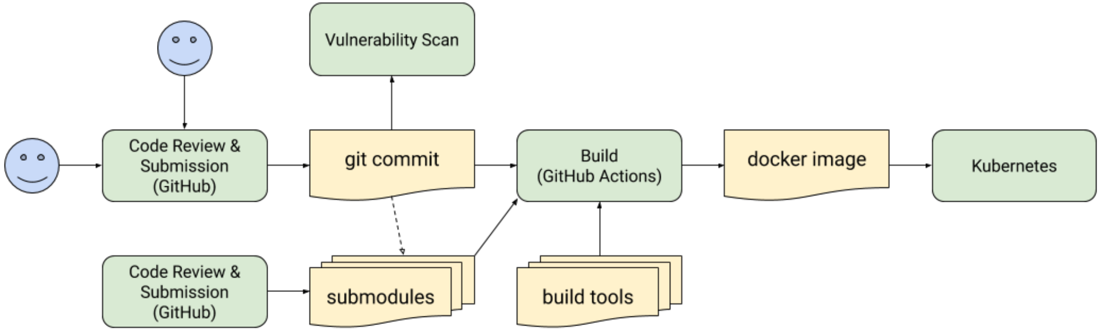
- Envelope: Handles authentication and serialization.
- Statement: Binds the attestation to a particular subject and unambiguously identifies the types of the predicate.
- Predicate: Contains arbitrary metadata about the subject, with a type-specific schema.
- Bundle: Defines a method of grouping multiple attestations together.



github.com/intoto/attestation

In-Toto Attestations - Statement Types

- Provenance (SLSA)
- Vulnerability Scan
- Code Review
- SBOMs, more!
- ...



Other Types of Attestations

Remote Attestations

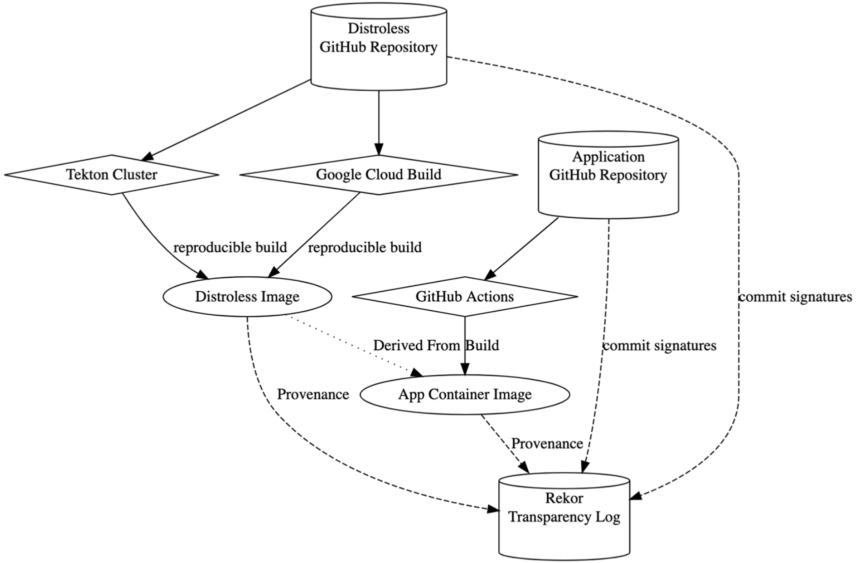
- Trusted Computing
- Allows a remote system to verify a system is in a known good state
- Two party protocol - challenge based

Hardware Attestations

- Allow KMS/HSM systems to prove that keys were generated on hardware (so they can’t be leaked)
- Allow hardware to prove it was built by a specific manufacturer (FIDO2 devices)

Combining Attestations

- Developer signs commit
    - using bound FIDO2 token with device attestation
    - On remote-attested machine (known good state)
- Build system generates provenance attestation
    - Contains input source digest and artifact digest
    - On remote-attested machine (known good state)
- Vulnerability scan system produces report attestation



Attestation Gotchas - Monotonicity

- Monotonic - Must be **positive** statements, progressing toward an approval
- The **lack of an attestation** should never allow an approval
  - Vulnerability scans are a tricky example
- **Expiration** rather than **revocation**

BAD

```
VulnerabilitiesPresent:
-   CVE123
-   CVE234
-   CVE456
```

GOOD

```
TimeStamp: 2021-11-05
VulnerabilityScanResult:
  Scanner: https://myscanner
  Results: PASS
  Policy: NO_CRITICAL
```

Attestation Gotchas - PKI

- PKI is **much** more than just signing
- This is deceptively complex - seems simple at first but gets complex very quickly
- Challenges:
    - **Key management**: rotation, revocation, discovery
    - **Diverse environments**: air-gapped data-centers, public OSS repositories, companies
    - **Complexity**: if this is too hard to use no one will
    - **Interoperability**: Need solutions to work for everyone

Project Statuses

- **SLSA:** Supply-chain Levels for Software Artifacts
  - Intel, Google, RedHat, VMWare, Datadog, Linux Foundation, Citibank, ActiveState, more!
  - Part of OpenSSF under Linux Foundation
- **Sigstore:** Supply Chain Transparency and Integrity
  - Free code signing certificates and transparency log
  - 380+ contributors, 20+ companies, ~1m entries
  - Support for In-Toto Attestations and SPDX/CycloneDX SBOM formats

Questions?

- twitter.com/lorenc_dan
- dlorenc@chainguard.dev
- openssf.org
- sigstore.dev
- slsa.dev