Nowhere to Hide

Using Transparency Logs to Secure Your Supply Chain with Sigstore

Google Open Source Security Team

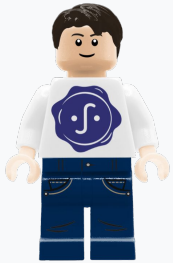
Hayden Blauzvern

Oct 2024

Who am I?

Google Open Source Security Team, aka GOSST

- Software Engineer & Manager at Google
- Focused on making open-source software more secure
- Bribable with LEGO
- Self-proclaimed expert chef



Agenda

01 What is Supply Chain Security?

02 Intro to Sigstore

03 Sigstore's Usage of Transparency Logs

04 Real-World Learnings

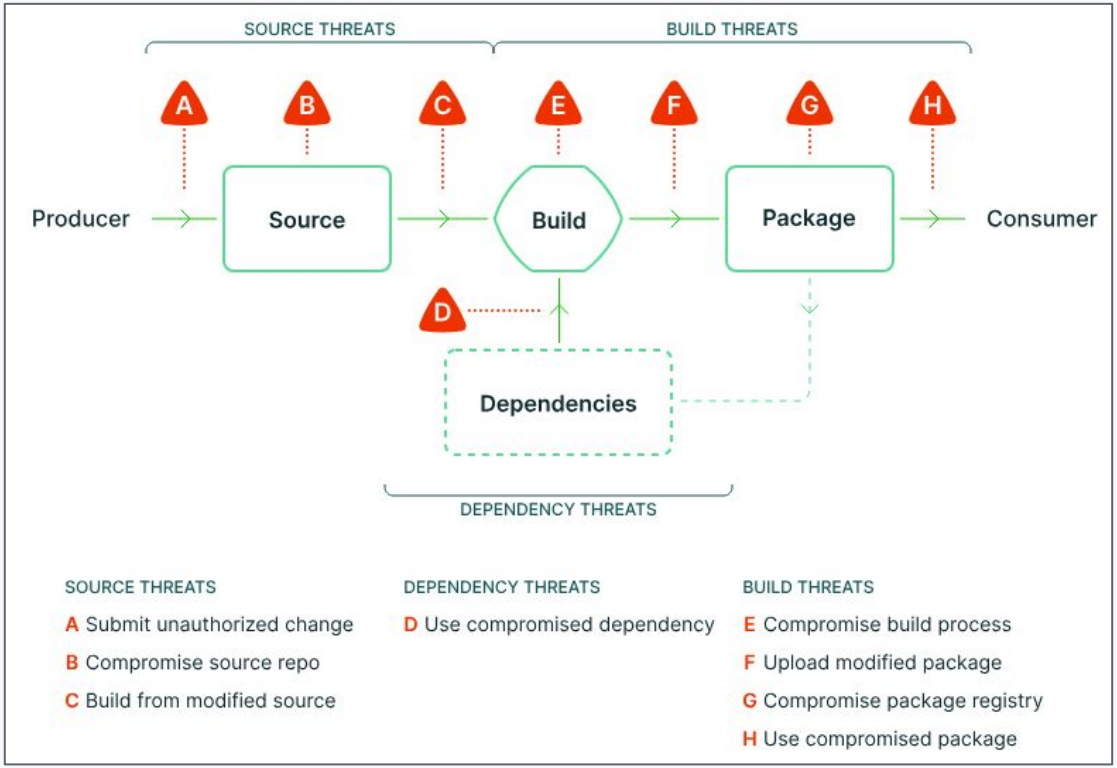
05 What's Next

01

What is Supply Chain Security?

Software Development Lifecycle

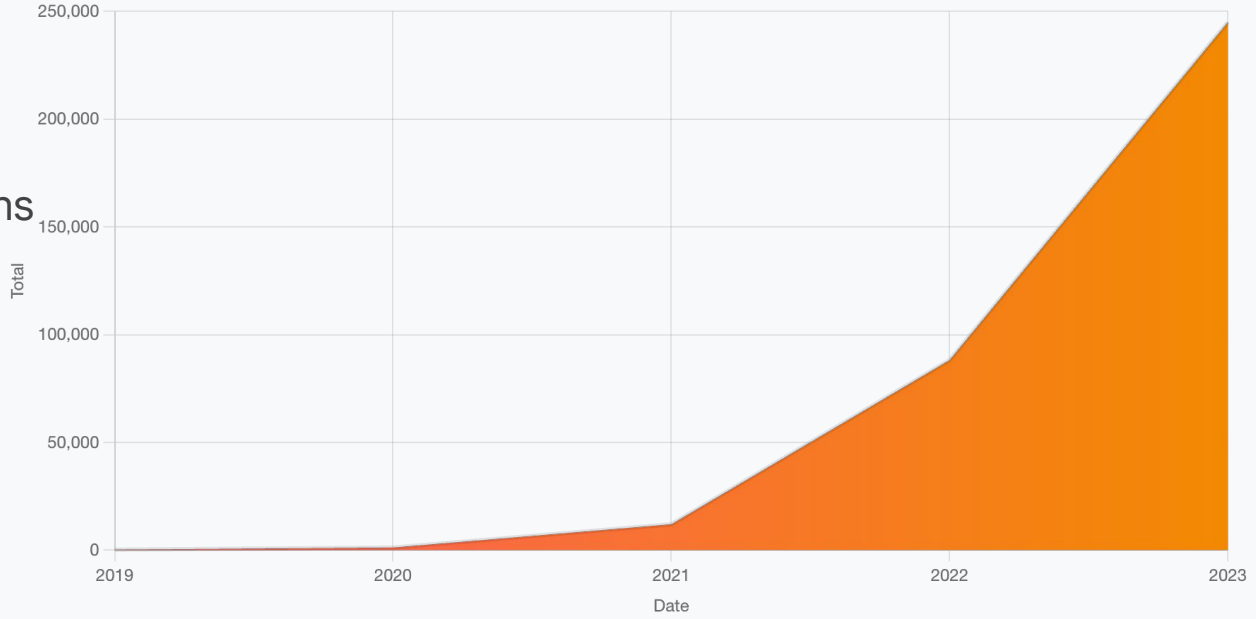
Threats to Mitigate



Source: https://slsa.dev/spec/v1.0/threats-overview

Supply Chain Attacks on the Rise

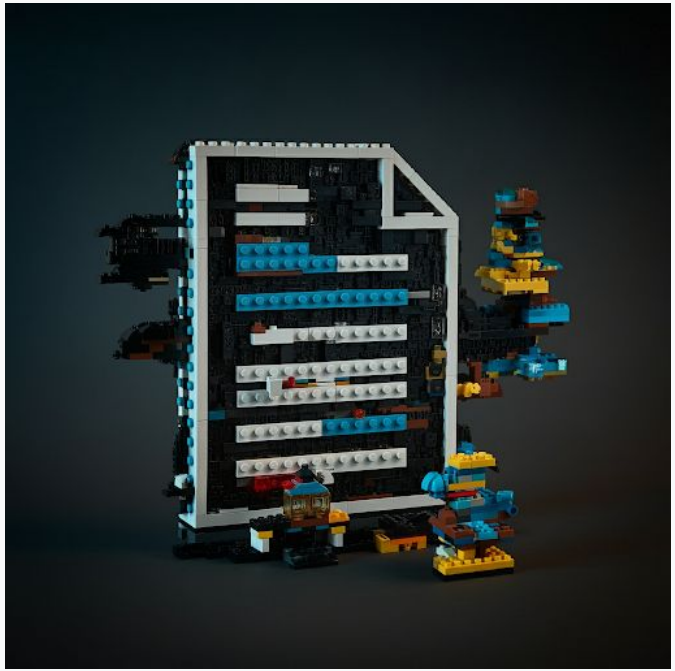
- Dependency confusion
- Typosquatting
- Malicious code injections
- Compromised build processes
- Major incidents: xz, Solarwinds, log4shell



Source: https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

Need for Trusted Artifacts

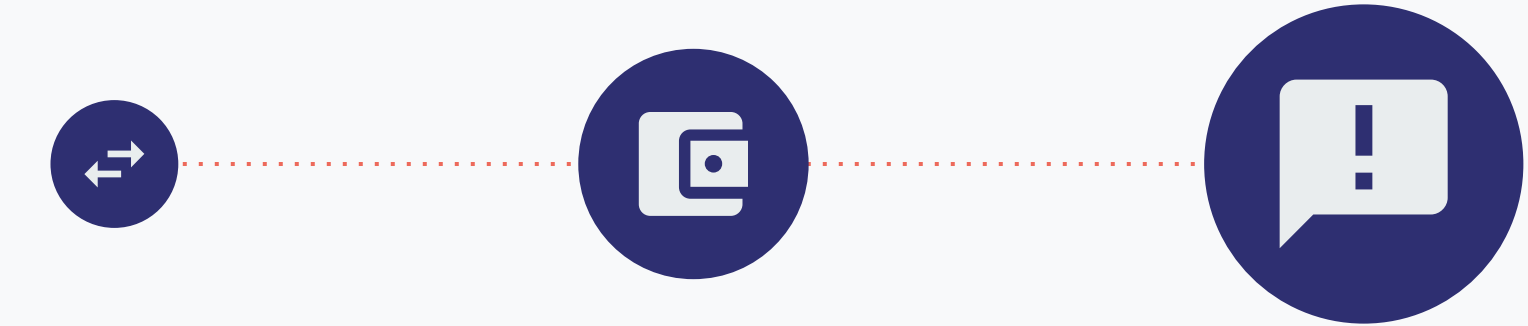
- Build provenance
- SBOMs
- Vulnerability scan results
- VEX
- Artifacts themselves
- Project policies
- ... and more!



Source: Gemini

Solution: Signatures!

Problem: Key Management is Hard



Problem: Signing is Uncommon in OSS

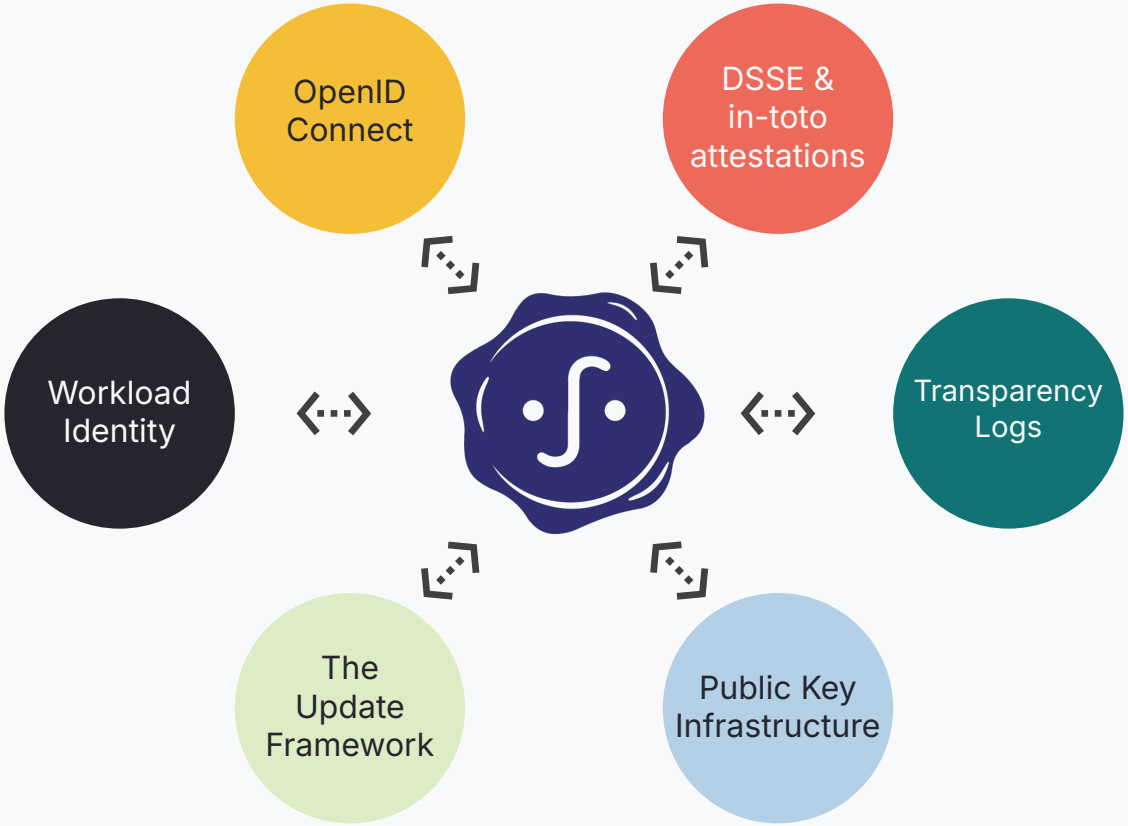
- Key management
- UX
- Lack of registry support
- Developers just don't care! (And they shouldn't have to!)

Source: Gemini

02

Sigstore

Convergence of Industry Standards



Sigstore: Trust Foundation

Sigstore Overview

Projects (Open Source)

- **Rekor**: Transparency Log
- **Fulcio**: Code Signing CA
- SDKs & Clients
  - Cosign
  - sigstore-go
  - sigstore-java
  - sigstore-js
  - sigstore-python
  - sigstore-ruby
  - sigstore-rs
  - gitsign
- Supporting projects
  - helm-charts
  - scaffolding
  - policy-controller
- Trust root (TUF-based)

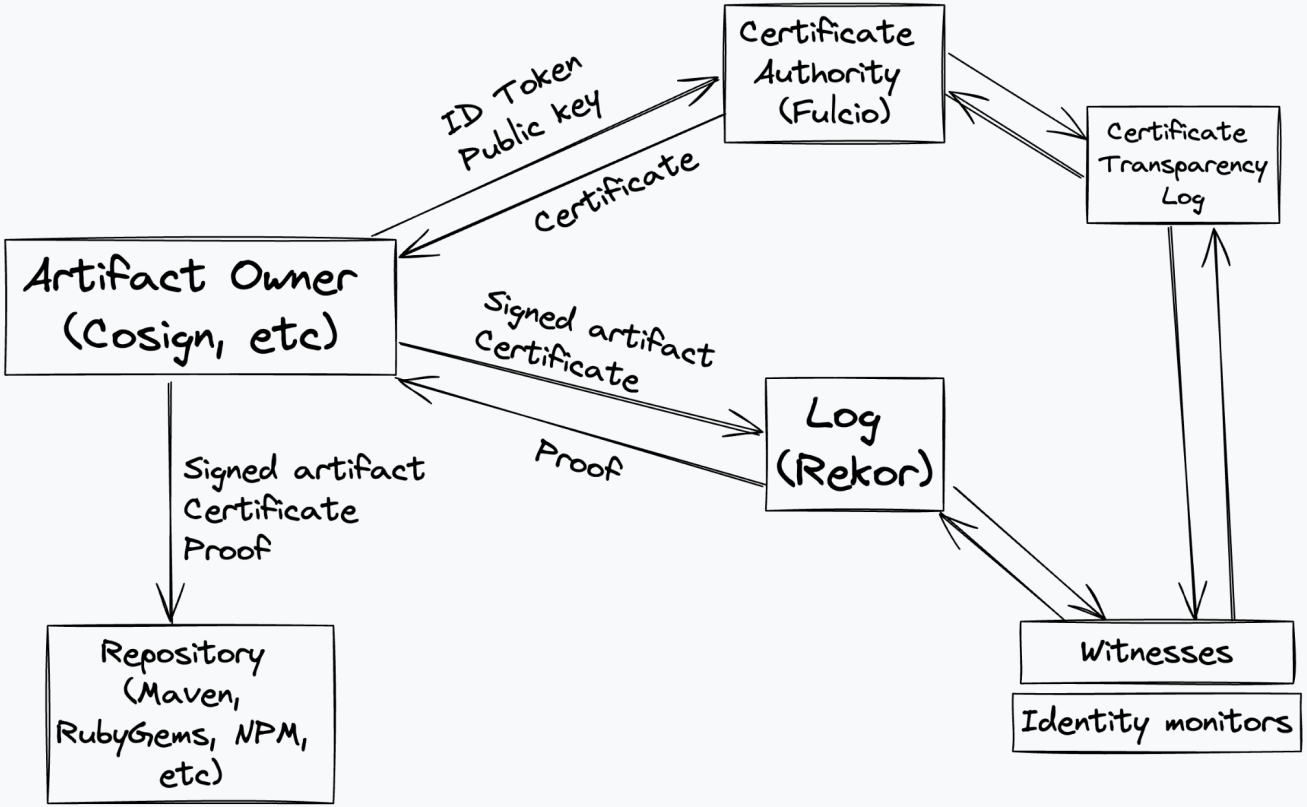
Services

- Public good instances (free to use!)
  - rekor.sigstore.dev
  - fulcio.sigstore.dev
  - oauth2.sigstore.dev
- Community-operated
  - Multi-vendor team
  - 24/7 oncall
  - Cloud hosted
  - Gitops-based infrastructure
- Productionized and running at scale since October 2022

Community

- An OpenSSF project
- Vibrant community of 2,600+ members in Slack
- Community meetings
  - Biweekly project review / office hours
  - "SIGs" (e.g. clients, on-call, architecture docs)

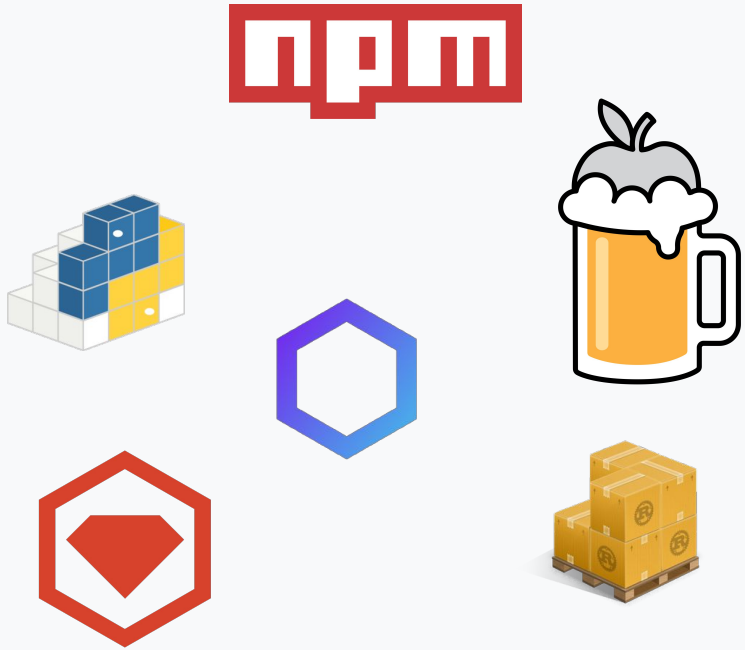
Sigstore Overview



Sigstore Adoption in Package Registries

Sigstore Adoption by Ecosystem

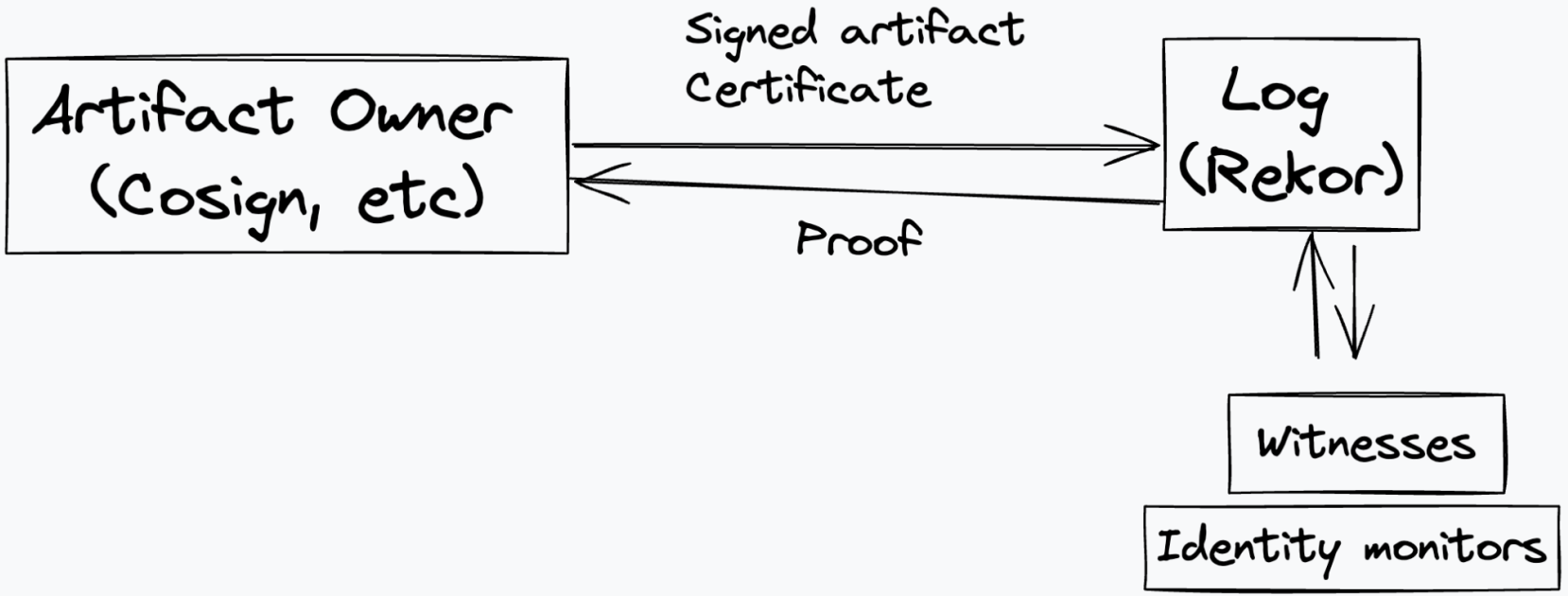
Ecosystem	State	Status
npm	Sigstore-signed SLSA provenance	GA LAUNCHED
PyPI	Trusted Publishing PEP 740 - Index Attestations	IN PROGRESS (Soon)
RubyGems	Trusted Publishing Signing & verification	IN PROGRESS
Maven Central	Signing (PGP & Sigstore)	GA LAUNCHED
GitHub Actions	Sigstore-signed SLSA provenance	GA LAUNCHED
Homebrew	Sigstore-signed SLSA provenance	BETA
Bazel Central Registry	Sigstore-signed SLSA provenance	RFC



03

Rekor: Sigstore's Transparency Log

Rekor



Rekor Deep-Dive

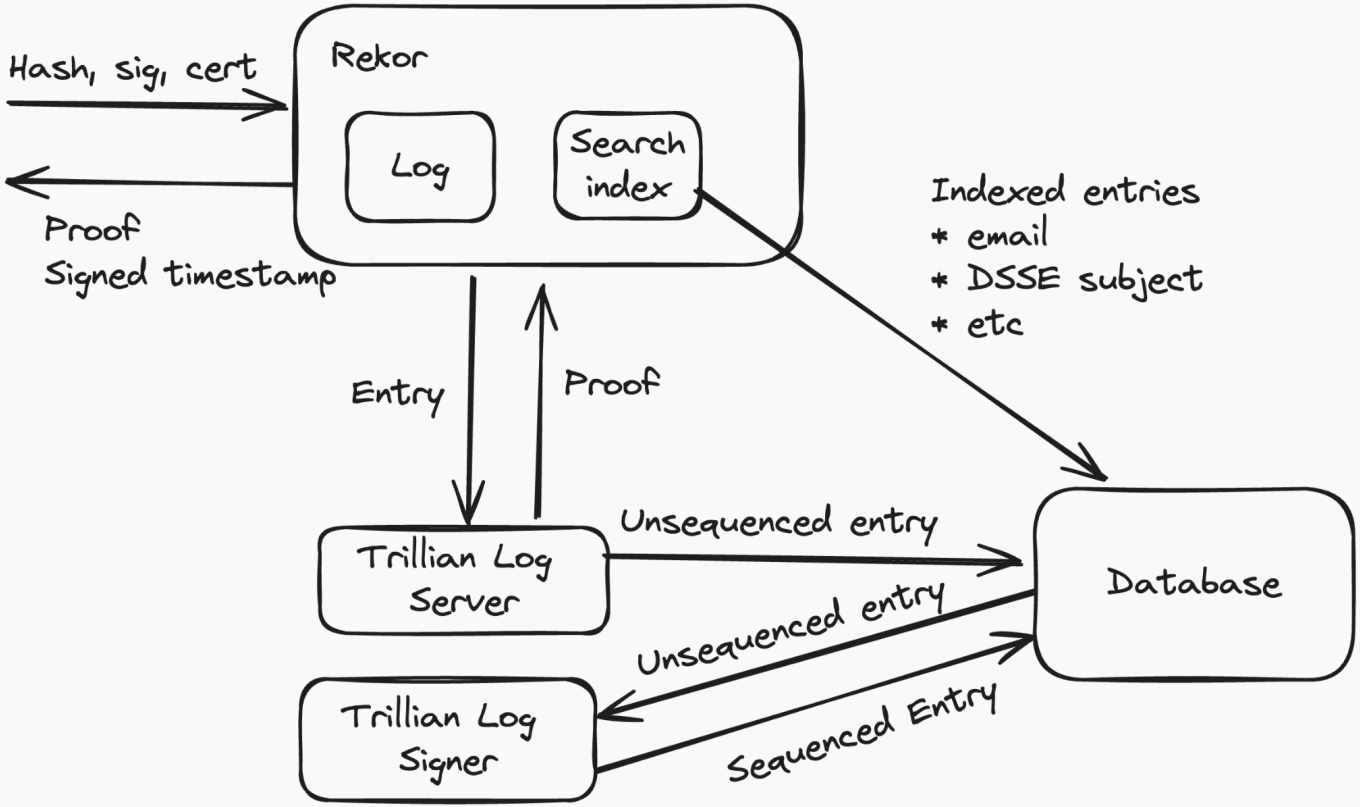
Request:

* Artifact Hash
* Signature
* Verifier
  * Certificate
  * Public key (RSA, ECDSA, Ed25519)
  * PGP public key
  * SSH public key

Response:

* Inclusion proof / checkpoint
* Signed Entry Timestamp
  * Log index
  * Log ID
  * Request body
  * Timestamp

Rekor Deep-Dive



04

Real-World Learnings

API Design

Client vs Server Canonicalization

Double Duty: Proofs, Timestamping, Attestation Storage, and Search

Source: lego.com

Online Queries: Save the Proof

Redactable Content

Deployment

Cost:

Deployment, storage, SREs

Source: bricklink.com

Source: Gemini

Many Components

Source: Gemini

Lack of Batch Processing

Source: https://www.lego.com/en-us/product/the-bad-batch-attack-shuttle-75314
It's Clone Force 99, aka "the Bad Batch".....

Complex Sharding

05

What's Next

Tile-based log:
Trillian-Tessera
Lower cost
Simpler to maintain

Stronger offline proofs:
Proofs, and checkpoints,
and witness co-signatures,
oh my!

Source: lego.com

Batching:
Wait a second...

Simplified API:
Less types, less verifiers

More Logs!

More Log Operators

Logs by domain

Simplified Sharding

Thank you!

SigstoreCon: Nov 12, 2024
Salt Lake City

Community and Slack