CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

So You Want to Run Your Own Sigstore: Recommendations for a Secure Setup

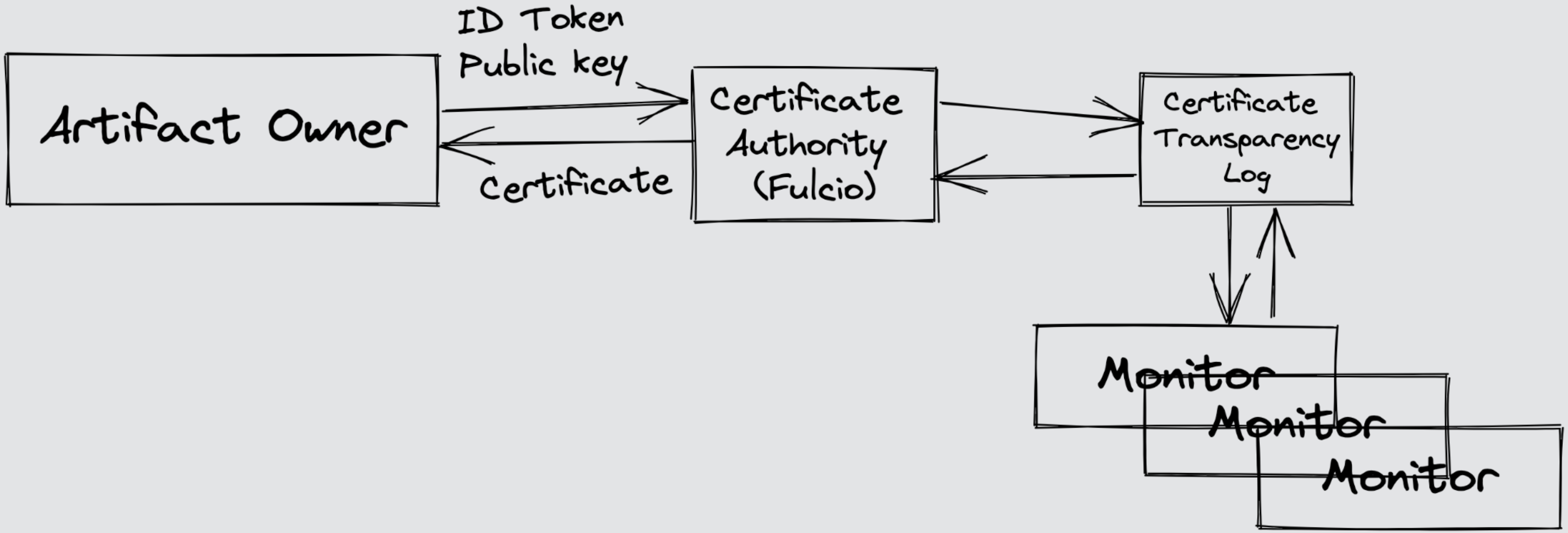
Hayden Blauzvern
Google Open Source Security Team

Sigstore Overview

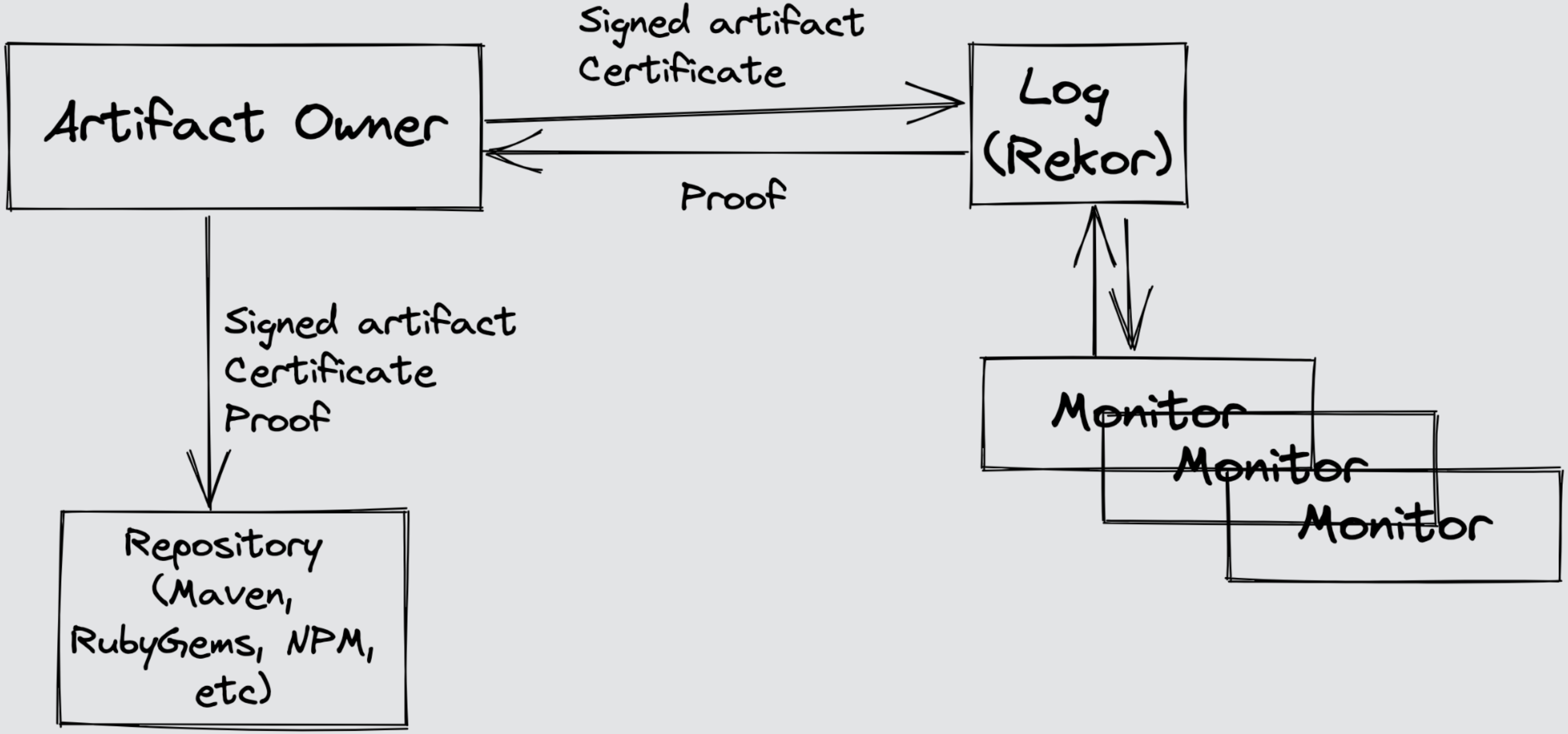
Sigstore Overview

- Project under the OpenSSF (Linux Foundation)
- Simplify code-signing for artifacts
- Free, publicly available transparency log and certificate authority
- No key management

Sigstore Overview - Fulcio

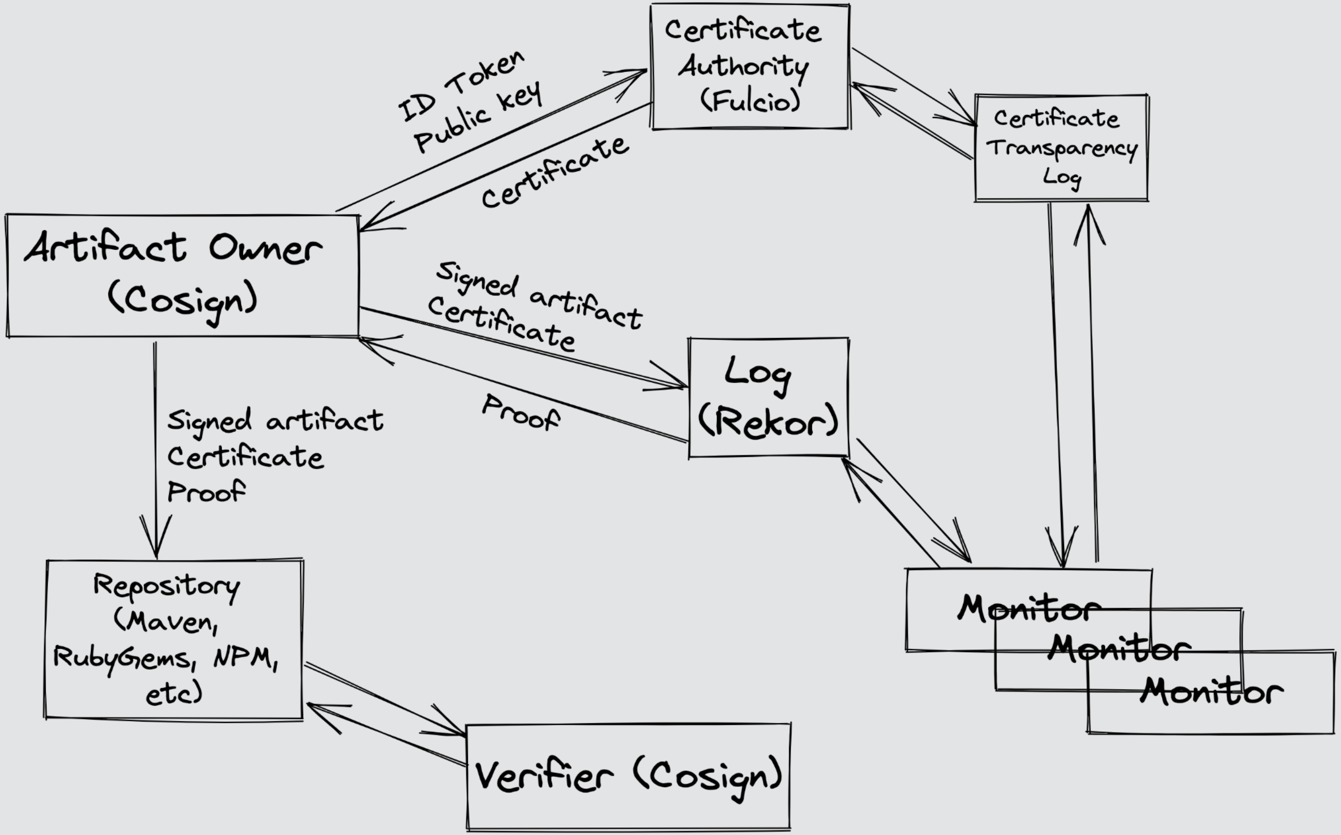


Sigstore Overview - Rekor



Sigstore Overview

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



Why a Private Sigstore?

- Performance/availability
- Compliance
- Privacy

Recommendations for a Secure Setup

Self-Managed PKI

Artifact Signing Keys

Distribution

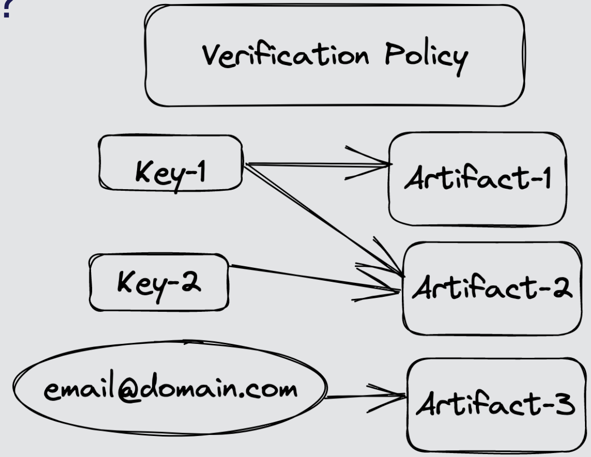
Storage

Compromise

Artifact Signing Keys

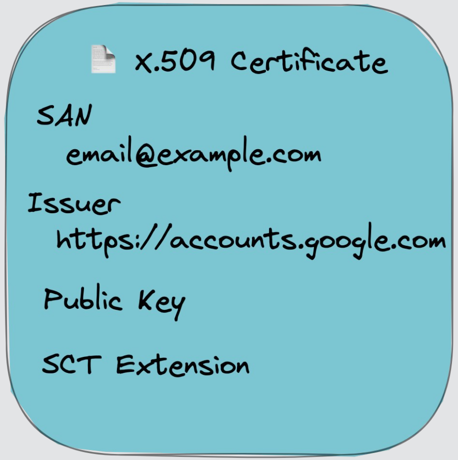
CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

- Sigstore defaults to ephemeral keys
- Can issue identity-based certificates for long-lived keys (blog post)
- What do you want for a verification policy?



Private CAs

- Existing CAs (step-ca, GCP CA Service, AWS Private CA, etc) issuing certificates that conform to the Fulcio certificate profile
- Consider key management, access controls, and rotation



X.509 Certificate

SAN
email@example.com

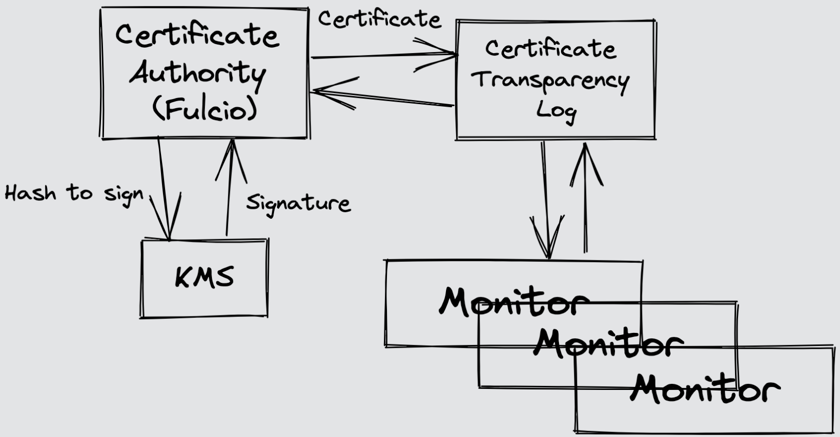
Issuer
https://accounts.google.com

Public Key

SCT Extension

Private Fulcio

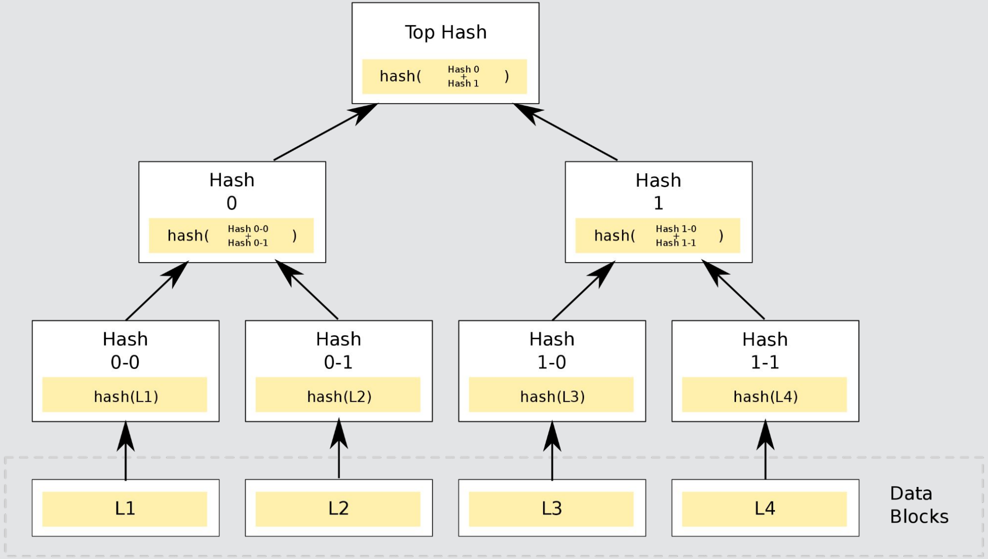
- Certificate Transparency for an immutable issuance log
- Same key management considerations for signing backend



Private Transparency

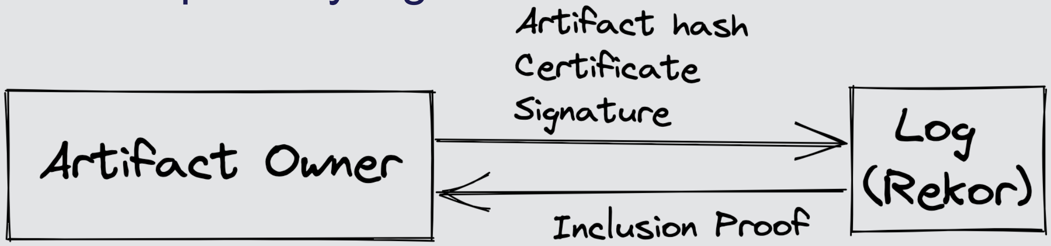
What's a Transparency Log?

- Based on Merkle Trees
  - Immutable and append-only
- Applications
  - Certificate Transparency
  - Binary Transparency
  - Key Transparency



Transparency Logs in Sigstore

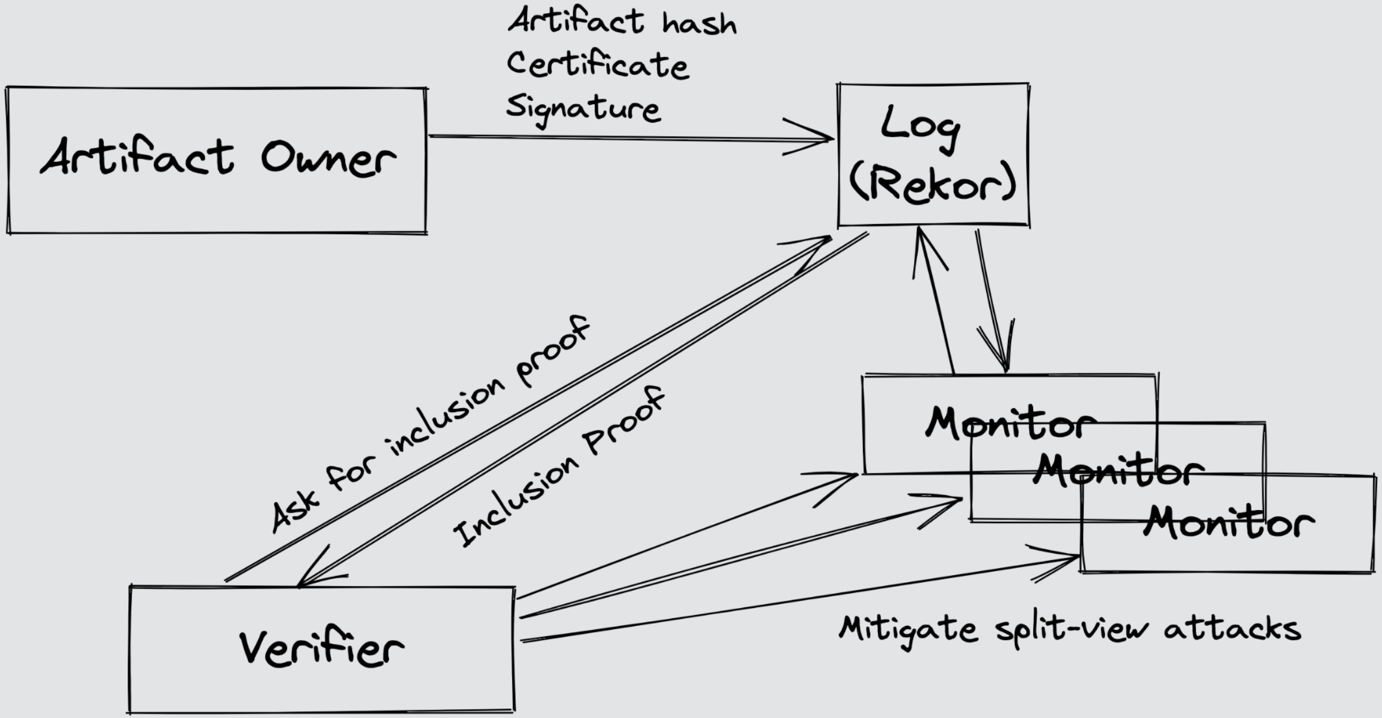
- Fulcio writes issued certificates to a certificate transparency log
- Rekor entries are appended to a transparency log



Do I Need Transparency Logs?

- Do you have an existing system for audit logging?
- Will artifacts ever be released publicly?
- Do you want an immutable record of issuance and signing?
- Can you use a database instead?

You Must Monitor!



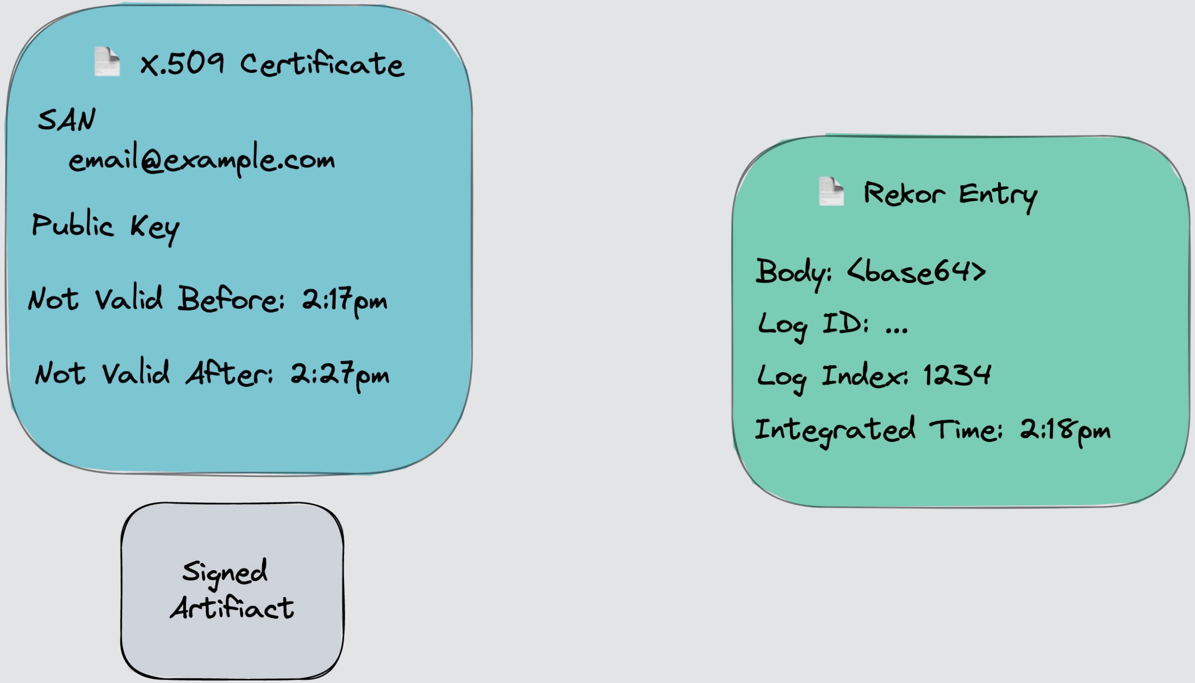
You Must Monitor!

OSS monitors:

- https://github.com/sigstore/rekor-monitor
- https://github.com/google/trillian-examples/tree/master/witness/golang

Timestamping

Timestamping in Sigstore



X.509 Certificate

SAN
email@example.com

Public Key

Not Valid Before: 2:17pm

Not Valid After: 2:27pm

Signed Artifiact

Rekor Entry

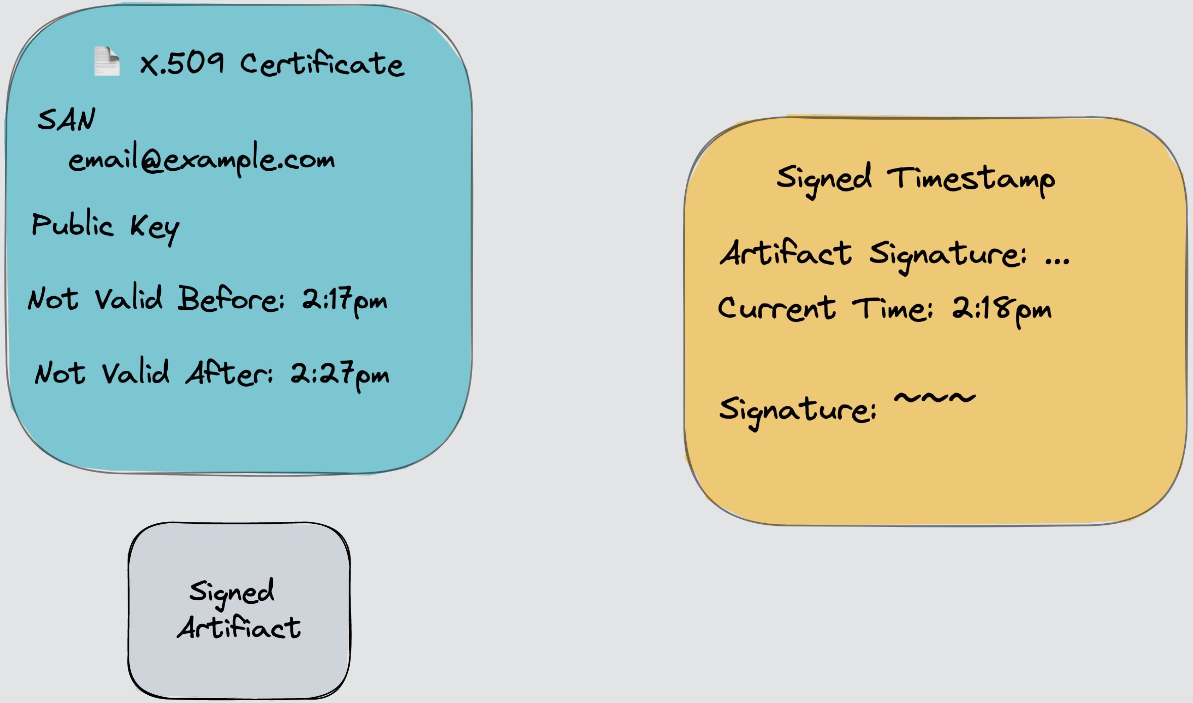
Body: <base64>

Log ID: ...

Log Index: 1234

Integrated Time: 2:18pm

Timestamping in Sigstore



X.509 Certificate

SAN
email@example.com

Public Key

Not Valid Before: 2:17pm

Not Valid After: 2:27pm

Signed Timestamp

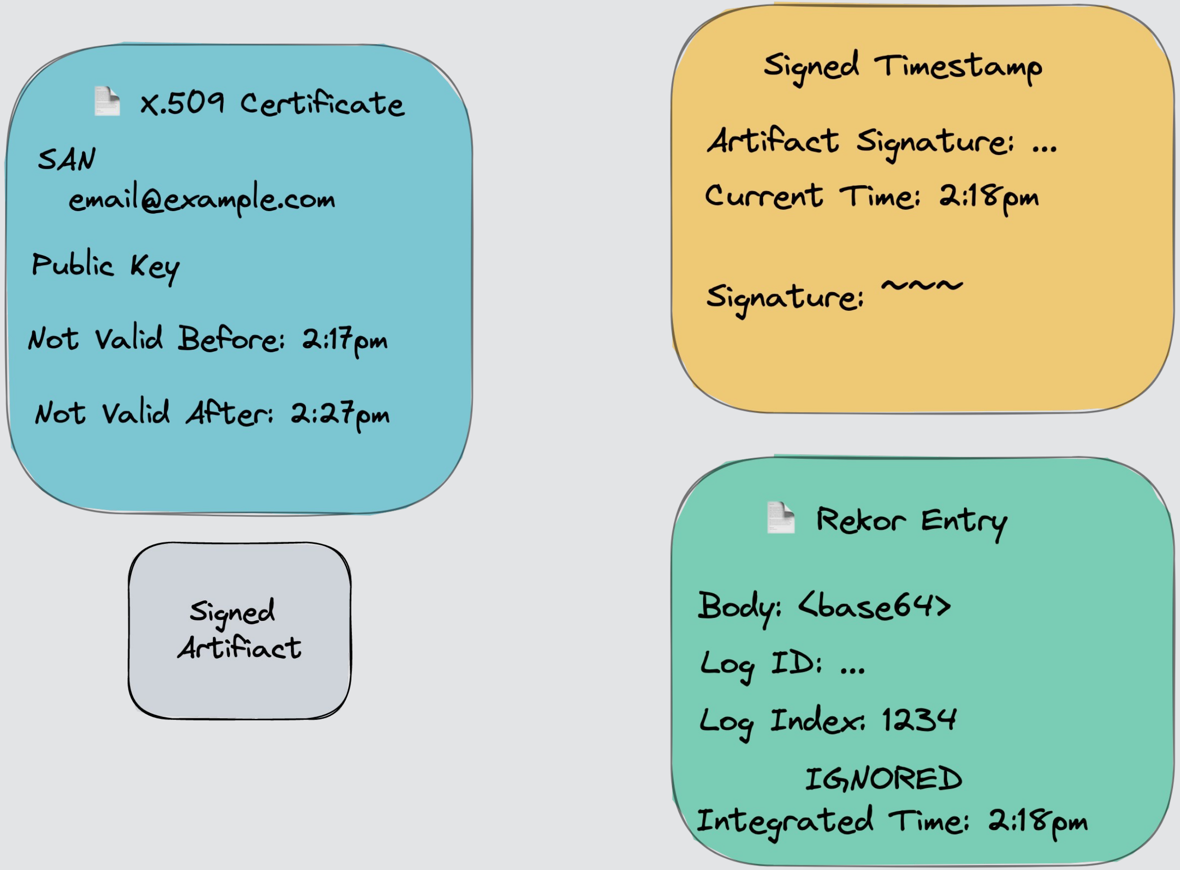
Artifact Signature: ...

Current Time: 2:18pm

Signature: ~~~

Signed Artifiact

Timestamping in Sigstore



X.509 Certificate

SAN
email@example.com

Public Key

Not Valid Before: 2:17pm

Not Valid After: 2:27pm

Signed Artifiact

Signed Timestamp

Artifact Signature: ...

Current Time: 2:18pm

Signature: ~~~

Rekor Entry

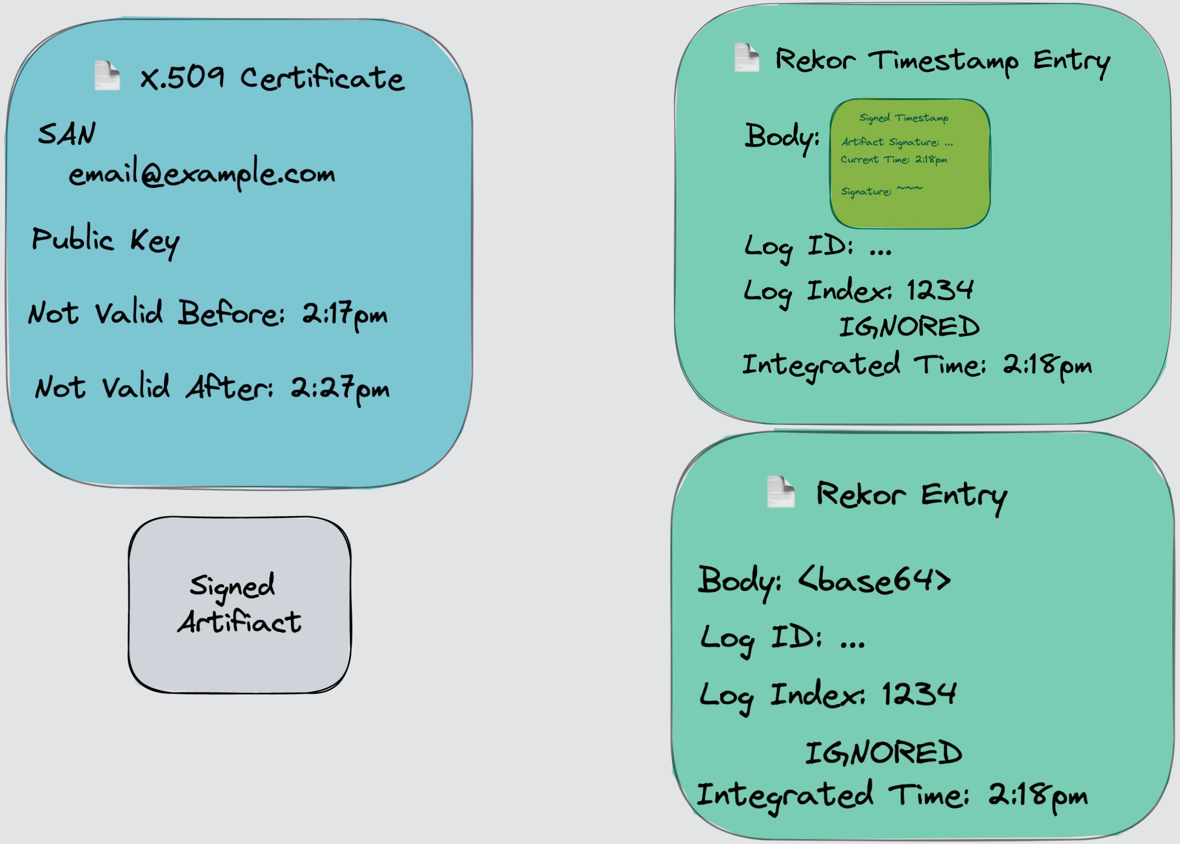
Body: <base64>

Log ID: ...

Log Index: 1234

IGNORED
Integrated Time: 2:18pm

Timestamping in Sigstore



X.509 Certificate

SAN
email@example.com

Public Key

Not Valid Before: 2:17pm

Not Valid After: 2:27pm

Signed Artifiact

Rekor Timestamp Entry

Body:

Signed Timestamp

Artifact Signature: ...

Current Time: 2:18pm

Signature: ~~~

Log ID: ...

Log Index: 1234

IGNORED

Integrated Time: 2:18pm

Rekor Entry

Body: <base64>

Log ID: ...

Log Index: 1234

IGNORED

Integrated Time: 2:18pm

Roots of Trust

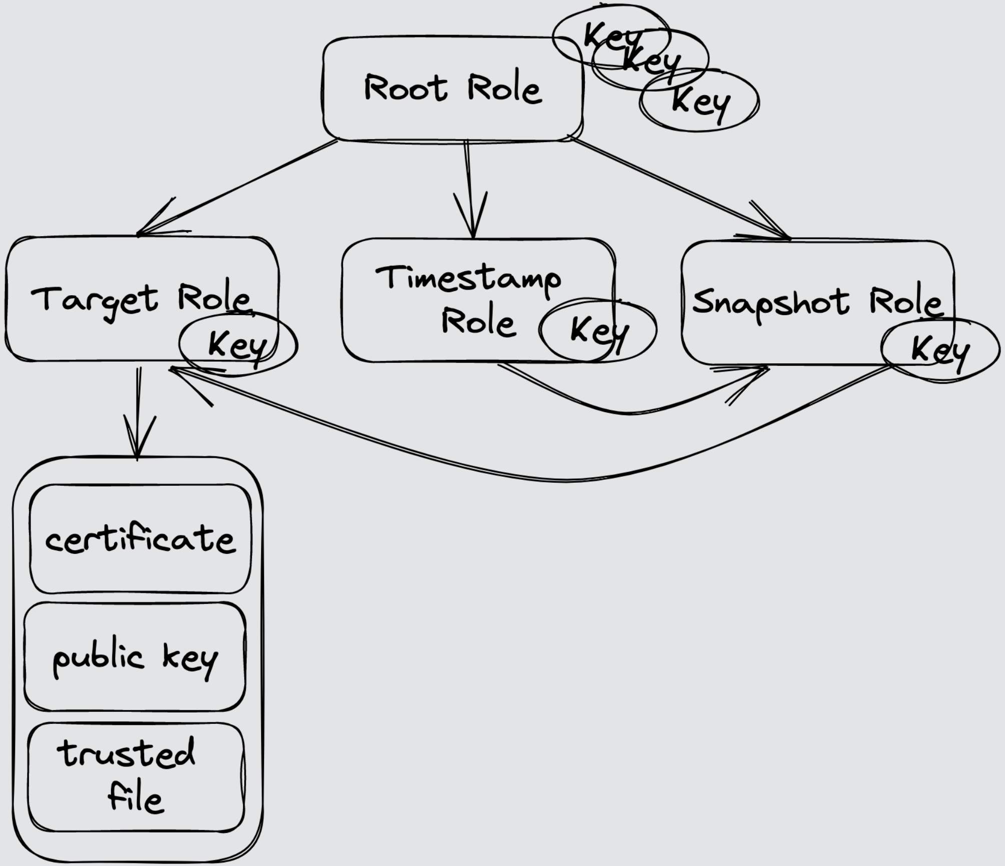
Problems with Key Management

Distribution

Storage

Compromise

The Update Framework



Takeaways

Key Management is Hard

Auditability is Critical

How to Deploy Sigstore

#private-sigstore-users on Slack

Thank you! Questions?

CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023