Security Analysis of OIDC-Based Software Signing with Sigstore and Cosign

Stavros Kousidis

Bachelor thesis · Published: 2026-10-15

Research question

Which supply-chain attacks can OIDC-based artifact signing with Sigstore prevent or detect, and which remain possible despite a valid signature and transparency-log evidence?

Description

Sigstore supports short-lived signing credentials bound to OpenID Connect (OIDC) identities. Cosign can sign artifacts with certificates issued by Fulcio, and transparency evidence can be recorded in Rekor. A valid signature establishes cryptographic properties and an authenticated identity; it does not by itself establish that a build was authorized or that the resulting software is trustworthy.

This thesis investigates how these distinctions affect practical verification. The focus is on explicit assumptions about artifact origin, signer identity, build environment and verification policy rather than merely setting up a signing pipeline.

Scope and evaluation

Implement a small, controlled CI/CD workflow with synthetic artifacts and Sigstore verification. Construct a threat model covering artifact substitution, unauthorized signing identities and a compromised build step that retains an authorized identity. Compare signature-only verification against policies that additionally constrain identity, issuer and expected workflow context. Determine which scenarios are rejected, which are detected later and which remain indistinguishable to the verifier.

Tests must use an owned or local laboratory environment. A deployment tutorial alone is not sufficient.

Expected outcome

A working demonstrator, an evidence-based comparison of verification policies and a threat model clarifying the security guarantees and limitations of keyless signing.

Starting points

- Sigstore: Keyless signing overview.
- Sigstore: Threat model.
- Okafor et al., *DiVerify: Diversifying Identity Verification in Next-Generation Software Signing* (2024).

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).