



JUDGEMENT SPINE

Security Model - Integrity & Signing (Public)

How the evidence pack becomes tamper-evident.

Integrity goal

Allow a third party to verify the evidence pack bundle has not been modified since sealing.

Mechanism

- A manifest.json lists files and their SHA-256 hashes.
- manifest.sha256 is the SHA-256 of manifest.json.
- signature.sig is a signature over manifest.sha256 (public-key verification).
- verify_manifest.py recomputes hashes and verifies signature when possible.

Operational guidance

- Sign packs at the moment the decision is sealed (before consequence).
- Store verification output alongside audit or dispute records.
- In production, store signing keys in an HSM or secure key management system.

Contact: founder@judgementspine.com