

Proven — and witnessed.

Not our word. Public answer keys, independent authorities, and a seal a stranger verifies — all signing off on the same record.

PROVEN · 16 SUITES · 3,791 INDEPENDENT CHECKS · 0 FAILURES

Checked against the world's own answer keys

- ✓ Google Wycheproof — Ed25519 (RFC 8032) 150 / 150 · PASS
- ✓ NIST ACVP — ML-DSA-65 (FIPS 204) 15 / 15 · PASS

These are the public test suites the whole industry uses — not tests we wrote. Anyone can run the same vectors and reach the same result.

Attacked, and it held

Every named attack against the seal, the log, the witness, the time, and the record — rejected. Behind them, over 2,210 exhaustive forgery attempts across every position and size.

- | | | | |
|---|----------|--|----------|
| ✓ Forge an inclusion proof | REJECTED | ✓ Rewrite history as a consistent extension | REJECTED |
| ✓ Tamper the sealed record | REJECTED | ✓ Strip the post-quantum signature (downgrade to classical-only) | REJECTED |
| ✓ Substitute the verifier's public key | REJECTED | ✓ Forge the independent witness co-signature | REJECTED |
| ✓ Present a trusted-time token for a different record | REJECTED | ✓ Alter an amendment to break the chain | REJECTED |
| ✓ Replay a sealed event to double-record it | REJECTED | ✓ Push data downstream through the one-way gate | REJECTED |
| ✓ Doctor a sealed record line after the fact | REJECTED | ✓ Substitute an unknown algorithm to bypass verification | REJECTED |
| ✓ Forge a verifiable credential | REJECTED | | |

Witnessed by independent authorities

- ✓ **An independent RFC 3161 trusted-time authority**
binds the exact sealed root to a moment outside our control
- ✓ **An independent witness co-signs the public root**
so no single party can publish a root the witness never saw
- ✓ **Google Wycheproof · NIST ACVP**
public conformance authorities — the seal passes their vectors
- ✓ **The seal verifies with public libraries**
a stranger confirms it importing nothing of ours

Everything above was earned on an independent run and verifies with public tools. You never have to take our word for it — the same authorities that signed off are ones you can query yourself.