# ZeroVaultID × Velmère

Independent reproduction of one public Cert Seal Rung 6 evidence kit

This is a bounded historical verification summary for one public evidence kit. It does not certify ZeroVaultID or establish overall system security. No new verification run was performed to prepare this revision.

## Exact subject and public anchor

| | |
|---|---|
| Run | rung6r3b-542e60f5 |
| Archive | zerovaultid-certseal-rung6.zip |
| Archive SHA-256 | fe876ce644321c2f22b3cd2c565b25ea6c5452912dfdc905a100f31b49e3efac |
| Verifier SHA-256 | e9fa708bf48ae88354d60ebc379dacb277d2f425b64895aeb6b5206c6114cdb4 |
| Signing key | 234374010ba7c648e59f26003b7915ce2c70899cd101c770cb046f5d6e3b5286 |
| Key anchor | ZeroVaultID-Inc/evidence-signing-keys. Commit 9a3ef7ee published the current key and retroactively revoked the previous key. Archive digest appears at commit 4650672. |

## Recorded September checks

Authenticity and replay. The September verification record states that the signing key fingerprint matched the public anchor, the manifest Ed25519 signature was verified, the verifier digest agreed with the manifest and the supplied verifier returned 7 of 7 checks passed.

Negative controls. The same record reports rejection of changed artifact bytes, altered verifier bytes and a substituted signing key. These are previously documented outcomes, not tests newly executed for this revision.

## Controlled lifecycle harness, not changes to the published kit

In Velmère's controlled harness, synthetic changes to signing key, release ID, archive hash, verifier or relevant dependencies caused the old record to become stale for a changed subject while preserving the historical result. These were controlled scenarios, not actual alterations to ZeroVaultID's evidence kit.

A simulated revocation of an authoritative signing key was treated as INVALID for current authenticity, not merely STALE. The public anchor's actual retroactive revocation of the former key is a separate historical fact, recorded at commit 9a3ef7ee.

## Limitations and scope

Not assessed: whole-system or production security; signer identity beyond the published key anchor; regulatory compliance; Canton ledger truth or enforcement; later releases; rail checks 1 and 2; Close_C confidentiality and unlinkability.

Scope: the exact public Cert Seal Rung 6 kit and the September evidence record only. No security audit, certification or broader endorsement is implied.