Integrity Attestation Report

Resethiq™ • Integrity Infrastructure for AI & Regulated Data

Executive Summary

Dataset / Artifact: package.json
Bytes: 559
Run ID: 9c379327-c0c6-4f2d-a670-cb08ee9aed77
Created: 2026-02-15T05:04:34.566Z
Engine: Resethiq Integrity Engine v0.1.0
Runtime: v20.20.0 • darwin • arm64

This report provides cryptographic and reproducible evidence that the submitted artifact matches the fingerprints and Merkle commitment recorded in the attestation bundle. The bundle is signed with Ed25519 to enable independent verification.

Appendix: Sample Merkle Inclusion Proofs

Below are sampled inclusion proofs for selected chunks. Each proof contains the leaf hash and the sibling path required to recompute the Merkle root.

Proof Type: merkle_inclusion_v1
Merkle Root:
`e938fe52cbeb7696b000879e7c12d0ae8eec799d209974d3bbf5ea50c43edd334d9523aaf51852a6eb55e3453b78acae545d0e5ffa18f2a3d3cc942d61e01b9c`
Algorithm: blake2b512

Proof • Leaf index 0 • verifies=true
leaf_hex:
`e938fe52cbeb7696b000879e7c12d0ae8eec799d209974d3bbf5ea50c43edd334d9523aaf51852a6eb55e3453b78acae545d0e5ffa18f2a3d3cc942d61e01b9c`
siblings_hex (bottom!’top):

Canonicalization & Determinism

Canonicalization Spec: cdr-stream-v1

Deterministic fixed-size chunking over byte-stream; schema-aware canonicalization comes in v2.

Cryptographic Fingerprints

File Digest (BLAKE2b-512):

`e938fe52cbeb7696b000879e7c12d0ae8eec799d209974d3bbf5ea50c43edd334d9523aaf51852a6eb55e3453b78acae545d0e5ffa18f2a3d3cc942d61e01b9c`
File Digest (SHA-512):
`35706a1e837d60ab4610c918ca08a258d82962ddda5d884485d0a4c716874e327be0c919b1a97aaf77949627959c9dc22f742c4115890a93304505c6743836cb`
Merkle Commitment:
- **Algorithm:** blake2b512
- **Chunk size:** 4194304
- **Leaf count:** 1
- **Root:**
`e938fe52cbeb7696b000879e7c12d0ae8eec799d209974d3bbf5ea50c43edd334d9523aaf51852a6eb55e3453b78acae545d0e5ffa18f2a3d3cc942d61e01b9c`

Signature & Verification Material

Signature Algorithm: ed25519

Signed Message Digest (SHA-512):

85d7b60c676edd03348fcf9bba00173f35cf7395369ed11d6267a5d95e544ddc57ccd1284040f63e76b92705556b124a984c32b4b4c2b3cac970bff5f69ad614

Signature (base64):

e/RP/Id2mAtr4EHB9Bqgj8PsLnW5gABj7Ynz5g5eNGFejQ+/eBhmCik69m/MdFAVU97iO6m0qHuTtziIHtqQCA==

Public Key (PEM):

-----BEGIN PUBLIC KEY-----
MCowBQYDK2VwAyEA0VgXx+SHWvvczMnNK8steBQY46wm7+hWlGGyxui9J70=
-----END PUBLIC KEY-----

How to Verify (Independent)

To independently verify this report, recompute the file digests and Merkle root using the stated chunk size, then validate the Ed25519 signature over the signed payload contained in the attestation JSON.

Local verification command (engine CLI):

```
resethiq verify --bundle out/attestation.json --file package.json
```