

AETERNA – INTEGRITY AUDIT REPORT

Cryptographic Integrity & Audit Assurance Report

Executive Summary

This report documents the deterministic integrity verification performed by **Aeterna** on **2026-02-01T04:22:17.984770Z**.

Aeterna evaluated the complete sequence of recorded operational events using cryptographically chained audit records.

VERDICT: PASS

No evidence of post-ingest modification, record tampering, record deletion, or chain discontinuity was detected within the evaluated scope at the time of verification.

System Identification

Instance ID	b3feb524-1ec1-42d5-baee-44c1ae5a72ba
Customer	Client
License Type	Standard
Declared Scope	ejemplo r

Verification Details

A total of **1** sequentially chained audit records were verified, forming a continuous integrity chain from session initiation through session closure.

The verification process is deterministic: any alteration, removal, or insertion of records after ingestion would irreversibly break the chain and be immediately detectable.

Scope Monitoring and Control

During operation, Aeterna continuously monitored execution activity against the declared operational scope.

No scope violations, unauthorized execution paths, or integrity anomalies were detected during the monitored period.

Technical Assurance

Aeterna implements cryptographically chained audit records using **SHA3-512 hashing**, combined with **HMAC-based digital signature generation at ingestion time**.

Each record's integrity depends on the immutability of all preceding records. Any post-ingest modification invalidates all subsequent records and compromises the audit chain in a deterministic and non-repudiable manner.

This report attests exclusively to **data integrity over time**. It does not assert the correctness, legality, or semantic validity of the underlying data itself.

Deliverable Evidence Record

Deliverable Hash	7a7b8c6a397ac12a7cb83d1908f33e033e11f79b4d3b96fa5e0b9b29cd65310355cea6556744e6cc06a5fdd8df1e90fd92762baa53d93a697fb8bc7c8b02fbb0
Hash Algorithm	SHA3-512
Declared By	Client
Purpose	ejemplo r

Evidence Integrity Statement

This document constitutes a **deterministic integrity artifact** derived exclusively from cryptographically verifiable audit records.

Any modification to the underlying records after the reported verification timestamp is cryptographically detectable and invalidates both the audit chain and this report.

Instance Binding

This report is cryptographically bound to a specific Aeterna execution instance. The following fingerprint uniquely identifies the audited system instance at the time of verification:

Instance Fingerprint	8d022f39-a653-45a0-817c-bef3eb245e14
----------------------	--------------------------------------

Sealed Deliverable

Deliverable Hash (SHA3-512)	7a7b8c6a397ac12a7cb83d1908f33e033e11f79b4d3b96fa5e0b9b29cd65310355cea6556744e6cc06a5fdd8df1e90fd92762baa53d93a697fb8bc7c8b02fbb0
Declared By	Client
Purpose	ejemplo r

Cryptographic Attestation & Non-Repudiation

Report Hash (SHA3-512)
5dbc4da4697b604fac686ee89dbf0036face9e48a0846f5be31e49716207823720097038034cc15118909656258ddf
c47de3832f786a2766d60abccfb2cb6527

Digital Signature (HMAC - Aeterna)
2cc2c9540d801e001bc23db1d77acad07686d49ff8691649e63303dadb1fb7d0fd087d8bd4331aae4dc9688a1dd9a
362215295e783d05299b66ca0a9829186d6

Report generated by **Aeterna**
2026-02-01T04:22:36.506625 UTC

Confidential – Generated for internal audit, compliance, and executive review