WHITE PAPER

Sealed Evidence.

What makes audit proof trustworthy.

Signing, sealing and verifying the record of a human decision, so that it holds long after the review.

REVYCORE RESEARCH

DECEMBER 2026

EXECUTIVE SUMMARY

A record that can be edited is a story.

Evidence is what cannot be.

Every governance programme produces records. Few of them would survive a determined question: who decided this, on what basis, and how do we know the record has not been changed since?

Evidence is not a document type. It is a set of properties: attribution to a named person, a fixed scope, a date, a link to what was observed, and protection against later alteration that a third party can check for themselves.

This paper describes the chain that turns an observation into verifiable evidence, the difference between signing and sealing, and what it takes for an auditor to verify a record without trusting the vendor that produced it.

Six links

Observation, decision, attestation, sealing, verification, reporting.

Signed, then sealed

A signature names who stands behind it; a seal shows it has not moved.

Verified without us

A package, a public key, a published contract: the verdict is recomputed offline.

Stated limits

What cannot be demonstrated is reported cause by cause, never smoothed over.

CONTENTS

01 Records are not evidence
02 The chain, link by link
03 Signed, then sealed
04 Verification without the vendor
05 The auditor's own view
06 Saying what cannot be shown
07 Where to start

01

Records are not evidence

An exported spreadsheet, an approval email, a screenshot: each describes something that happened, as told by whoever produced it. None of them can show, on its own, that it has not been changed, or that the person named in it actually decided.

Auditors know this, which is why they sample, cross-check and ask for the same fact from several sources. The cost of an audit is largely the cost of compensating for records that are not evidence.

The alternative is to produce evidence at the moment of the decision, with properties that make it checkable by anyone, at any time, without the cooperation of the system that produced it.

“A record that can be edited is a story, not evidence.”

KEY IDEA

DEFINITION

Evidence: a record attributed to a named person, bound to what was observed, fixed in time, and protected so that any later change can be detected by a third party.

02

The chain, link by link

From what was seen to what is reported, the chain has six links. A weakness in any one of them weakens all the others.

“Every link is traced, chained and verifiable.”

KEY IDEA

LINK	WHAT IT ESTABLISHES
Observation	What was seen. Each collection is dated, attributed to a connection, and kept. The absence of observation is recorded as a fact.
Decision	Who decided. A named person, with their authority at the time, their justification and the rules they decided under.
Attestation	What is certified. The object, its observed state, the validity conditions, the maximum term and the evidence references.
Sealing	Events are chained by fingerprint and sealed by segment. Any alteration breaks the chain, and the break shows.
Verification	A verification package, the authority's public key and a published contract. The verdict is recomputed offline.
Reporting	What was certified, valid and demonstrable on the day requested, read as it was, not as it has become.

03

Signed, then sealed

An attestation becomes evidence in two moves. First, a named person signs the closure of a review: the decisions, the reviewers, the timestamps and the frozen scope. Then the record is sealed, so that any later change becomes detectable.

The two are often confused. A signature tells the auditor who stands behind the record. A seal tells the auditor that the record has not moved since it was produced. Neither replaces the other, and evidence needs both.

Sealing applies to the audit trail as a whole, not only to closures. Events are chained by fingerprint, so that removing or editing one breaks the chain at that point, visibly.

“A signature says who. A seal says unchanged since.”

KEY IDEA

Who decided
Named reviewers, with their authority at the time.

On what scope
The systems and rights reviewed, frozen at launch.

When
Timestamps for each decision and for the closure.

Unchanged since
A seal that any third party can verify.

04

Verification without the vendor

Evidence that can only be checked inside the platform that produced it is still a matter of trust. For a record to stand on its own, an auditor must be able to verify it offline, without an account, years after the review, and without calling the vendor.

“Your auditor should not have to take your word for it.”

KEY IDEA

That requires three things: a verification package that contains the records and their seals; the public key of the sealing authority, published at a known address and anchored on its root key; and a published contract describing how the verdict is computed. The same verifier then gives the same answer in the console and on the command line.

Verification also means being able to leave. Evidence, audit trail and configuration should be exportable in open formats, so that nothing about the proof depends on the vendor remaining in place.

DEFINITION

Offline verification: recomputing the verdict on a package from its own content and a published public key, with no call to the system that produced it.

05

The auditor's own view

An auditor needs to consult, verify and export, not to run a campaign or decide. A dedicated, read-only role, flagged by a permanent banner and bounded by an assignment end date, gives them that access without blurring responsibilities.

What they look at is an audit posture: what is attested and sealed, an audit file of selected items with their fingerprint, and the state of certifications as of a given date. The posture answers one question: what can this scope really demonstrate?

“Read-only, bounded in time, and never a decision-maker.”

KEY IDEA

- **Audit posture.** What is attested and sealed, with no smoothing.
- **Audit file.** Selected items, each with its fingerprint.
- **State as of a date.** What was valid on the day requested.
- **Not demonstrable.** Reported by cause, never as one undifferentiated total.

06

Saying what cannot be shown

Every estate has blind spots: a connection that failed, a scope that was never collected, a change of connector that broke comparability. Evidence that hides them is weaker than evidence that names them.

Reporting what cannot be demonstrated, cause by cause, turns a gap into a task. It also protects the credibility of everything else: an auditor who sees the limits stated plainly is more inclined to trust the rest.

“An honest gap is worth more than a smoothed total.”

KEY IDEA

The same principle applies to collection. Insufficient observation never means that an access is compliant. It means that compliance cannot currently be shown, and that is what the record says.

07

Where to start

Evidence is cheapest when it is produced at the moment of the decision. Retrofitting it before an audit is where the cost lies.

“Build evidence into the decision, not around it.”

KEY IDEA

1 **Attribute every decision** to a named person, with a justification and a date.

2 **Freeze the scope** of each review at launch.

3 **Sign closures, then seal the trail,** so that any later change is visible.

4 **Publish what verification needs:** the public key, the package format and the verdict contract.

5 **Give your auditor a read-only view** and report the gaps as plainly as the proof.

REVYCORE

Evidence your auditor verifies without us.

Human decisions. Verifiable evidence.

Request a demonstration in your context: your solutions, your scopes, your agents.

revycore.com

This paper describes principles of audit evidence and the corresponding capabilities of REVYCORE for information purposes; it is not legal advice. © 2026 REVYCORE SAS.