

What this record proves, and how to check it yourself

You have been given an evidence bundle covering decisions an AI agent made inside a vendor's system. This page states exactly what it does and does not establish. The next page lets you verify it in about five minutes, without an account and without contacting anyone.

HOW THE RECORD IS BUILT

Each decision emits a signed Decision Receipt. Receipts are hash-chained in order, committed to a Merkle tree, and bound by a signed checkpoint covering the count, head, and root of the set. A verifier holding the public key and the published format can confirm offline that a presented history is authentic and internally consistent: nothing in it added, altered, reordered, or truncated relative to what was signed. Raw tool arguments never enter the record; receipts carry only their SHA-256 hash, so verification never requires disclosing argument contents.

WHAT A PASSING VERIFICATION ESTABLISHES

1. **The integrity of every receipt present.** Each is authentic, correctly ordered, and Merkle-included, and none has been added, altered, reordered, or truncated since it was signed.
2. **Who issued it, but only if you pin the issuer's public key** from a channel other than the bundle. Without that pin the result is integrity-only, and an honest report will label it so. A bundle re-signed under a different key is internally consistent too; the pin is what rules that out.

WHAT IT DOES NOT ESTABLISH

3. **That every action was recorded.** A pass says nothing about decisions that were never written down. Completeness is bounded by the tamper-evidence of the interception point, which sits outside the bundle. If non-omission matters to your review, ask the vendor where that interception point sits and how it is protected.
4. **That a permitted call executed, or what it returned.** A receipt records the governance decision. Whether a denied action was actually blocked is a property of how the vendor wired the deployment, not of this record.

IF YOU READ NOTHING ELSE

This record is built to be checked by someone with no reason to trust the party that produced it. That is the point of it. It is not a claim that the vendor logged everything, and it should not be accepted as one.

Verify it yourself, in about five minutes

No account, no sign-up, and no call back to the vendor or to us. You need Node.js and the bundle you were given.

OPTION A: THE COMMAND LINE

The verifier is published on npm as a standalone package that does not depend on the system which produced the bundle:

```
npx -y @attested-intelligence/aga-verify@2.2.0 evidence-bundle.json
```

It prints VERIFIED, FAILED, or UNSUPPORTED_PROFILE. There is no partial pass and no silent downgrade: an algorithm it does not recognise is reported as FAILED, never as a qualified success.

OPTION B: THE BROWSER, WITH NOTHING INSTALLED

Open the offline verifier at attestedintelligence.com/verify and drag the bundle onto the page. It runs entirely client-side. You can disconnect from the network first and it will still work, which is the simplest way to satisfy yourself that nothing is being sent anywhere.

TO ALSO ESTABLISH WHO ISSUED IT

Ask the vendor for their gateway public key through a channel other than the bundle: a signed email, a contract exhibit, their security page. Pin that key when you verify. Without an out-of-band key you have integrity only, and the tools will say so rather than implying more.

TEST THE TOOLING BEFORE YOU TRUST ITS VERDICT

Two checks worth five minutes of a skeptical reviewer's time:

- A. Change one byte anywhere in the bundle and verify again. It must fail. If a tamper does not produce a failure, stop and escalate.
- B. Verify a sample published by us rather than by the vendor. attestedintelligence.com/verify carries, under Take it offline, a fixed sample bundle whose signing key begins `b900a315c50d9516`, so you can confirm the verifier agrees with an artifact the vendor did not produce.

THE FORMAT IS PUBLISHED

The construction is specified so you can re-implement the check or have your own engineers audit it. The conformance vectors are downloadable from attestedintelligence.com/spec, so a verifier can be checked against them. Nothing here depends on taking our word for the cryptography.

Attested Intelligence Holdings LLC. Verifiable decision records for AI agents. Questions about a specific bundle go to the vendor who gave it to you. Questions about the format or the verifier go to admin@attestedintelligence.com. This document states scope; it is not legal or compliance advice.