

Time-anchored integrity record (TAIR)

Append-only event logging with signed checkpoints and independent time anchoring. October 2026.

1. SCOPE

This note describes a record-keeping extension to the Attesso authorization platform: the append-only event log, signed checkpoints, verification proofs, and RFC 3161 time anchoring, as implemented and verified in the current release.

2. SYSTEM DESCRIPTION

2.1 Journal. Every mandate event is appended, in order, to a single log with densely numbered entries. Entries are immutable; no operation updates or deletes them.

2.2 Checkpoints. Signed checkpoints over an RFC 6962 Merkle tree are issued on a bounded interval. Each checkpoint covers the complete preceding log prefix and chains to its predecessor.

2.3 Proofs. The service provides inclusion proofs for individual events and consistency proofs between checkpoints. The verification procedure and a reference verifier are published.

2.4 Time anchoring. Each checkpoint is timestamped by an RFC 3161 time authority. The token is retained unmodified and binds the checkpoint hash to an independent generation time.

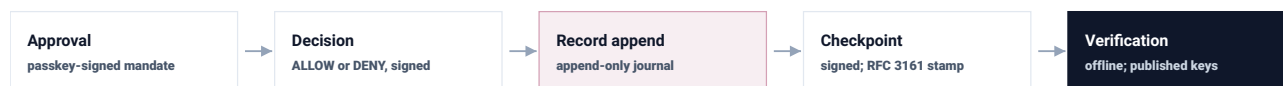


Figure 1. Lifecycle of an authorized action and its record.

3. VERIFICATION

Verification is offline and requires no Attesso software. The published key set, SHA-256, and open implementations of RFC 6962 and RFC 3161 are sufficient; the published procedure reproduces every check with standard tooling (docs.attesso.com/guides/check-the-record).

4. ASSURANCE PROPERTIES

Integrity. Consistency proofs demonstrate that each earlier log state is contained in the current state; modification of committed history invalidates the checkpoint chain.

Completeness. Inclusion proofs place each event within a signed checkpoint; an event absent from the log cannot be shown to be present.

Time. Checkpoint existence is attested by an independent time authority; it does not depend on the operator's clock.

5. STATUS

Implemented in the current release. Integrity audits and proof-level fuzzing run in continuous integration; the full chain has been exercised against a public time authority and verified offline with standard tooling.