



What a Record Must Prove

North Canterbury · © John Stroh

Version 0.4 · revised 13 September 2026 · [this version as a PDF](#)

Current instruments require operators of automated systems to retain records. None requires those records to be capable of proving anything to a party other than the operator.

Policy paper · Version 0.4 · September 2026

Evidential quality in records of automated systems, and the case for a conformance mark

Summary

Current instruments require operators of automated systems to retain records. None requires those records to be capable of proving anything to a party other than the operator.

An operator can satisfy every retention duty in force with a log it can edit, on infrastructure it controls, stamped by its own clock. Such a record is evidence about the operator's conduct only to the extent the operator is already trusted, which is the question the record was meant to settle.

The instruments that close this gap are standardised and in production use. European law already attaches a legal presumption to one of them. We have found no product in this class that uses them, and have not described that search. What can be stated from the instruments themselves is that nothing requires their use, and that no mark exists by which a purchaser could establish whether they had been used.

Recommendation: specify the evidential properties a record must have, and require a conformance mark applied by a party other than the maker.

This paper concerns the record substrate only. Detection of an agent acting outside its authority is the subject of MIO-POL-02 and depends on this paper being satisfied first.

1. The distinction that is not currently drawn

Three different things are commonly described in identical terms.

1.1 A record is a statement that something happened. Its correctness rests on the trustworthiness of whoever holds it. Where the holder is a party to the dispute, it has no evidential weight against them.

1.2 An integrity check is a cryptographic fingerprint of the content. It establishes that the content has not changed since the fingerprint was taken. It establishes nothing about when the content was created or by whom.

1.3 An attestation introduces a party who was not the author: a signature binding the fingerprint to a key, and a timestamp binding it to a moment, issued by an authority independent of the operator. It does not establish that the underlying statement is true. It removes the possibility of the record having been created later and dated earlier.

Only 1.3 has weight against the party holding the record. A product may stop at 1.1 and describe themselves in the vocabulary of 1.3 — audit log, immutable, tamper-proof. A purchaser comparing two products has no means of distinguishing them.

2. What the law currently provides

2.1 The presumption already exists in European law. Regulation (EU) No 910/2014, Article 41(2): a qualified electronic time stamp *“shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.”* Regulation (EU) 2024/1183 extends comparable standing to qualified electronic ledgers. A published register of qualified providers is maintained.

2.2 Nothing requires a product to use it. These provisions regulate trust service providers. They place no obligation on the platform whose records such a provider would attest. A qualified timestamp is available to any operator, and nothing in these provisions requires one to obtain it.

2.3 The AI Act duties are duties to keep. Article 12 requires high-risk systems to permit automatic recording of events over their lifetime; Article 19 places retention duties on providers and Article 26(6) a parallel duty on deployers. None of these requires that a record be unal-

terable by its holder, that its time come from an independent source, that any other party be able to verify it, or that claims drawn from it disclose whether they are independently attested.

2.4 Those duties are not yet in force. Following the amendments approved in June 2026, the high-risk obligations for stand-alone systems apply from 2 December 2027 and for product-embedded systems from 2 August 2028.

2.5 The gap, stated precisely. It is not an absent legal instrument. It is an absent obligation to use the instrument that exists, and the absence of any mark by which a purchaser could establish whether it had been used.

3. The properties

Three properties. Each is testable. None requires anything to be invented.

3.1 Immutability, with an isolated sealing function. Corrections are appended; nothing sealed is altered or removed; each seal commits to all records preceding it, so that a record cannot be removed from the sequence without invalidating what follows. The component performing the sealing is not reachable by the systems whose conduct it records — an append-only store administered by the party under examination is append-only at that party's discretion.

3.2 Independent time. Sealed batches attested by authorities independent of the operator, under at least two distinct legal jurisdictions not reachable under a single compulsion instrument. A single authority is a single point of both failure and coercion.

3.3 Graded claims. Every assertion drawn from the record discloses whether it is independently attested or rests on the operator's word.

3.4 What grading actually discloses

Records are sealed in batches. Ordering **across** batches is fixed by the outside authority and may be relied on by a third party. Ordering **within** a batch rests on the operator's own clock.

The batch interval is therefore not a performance setting but the resolution of the evidence. A product advertising independently timestamped records at a twenty-four-hour interval offers independent evidence about days and operator testimony about anything shorter. That may be adequate; a purchaser should be able to establish which they are acquiring.

4. The conformance mark

4.1 Precedent. Under the Hallmarking Act 1973 it is an offence, in the course of a trade or business, to describe an article as gold, silver, platinum or palladium without a hallmark. The mark carries three elements: a sponsor's mark identifying who made or submitted the article; a fineness mark stating the metal's actual composition; and an assay office mark identifying who verified it. The sponsor's mark is the maker's own. **The two elements carrying the assurance may be applied by nobody but the assay office.** The scheme dates from a statute of 1300.

4.2 The analogous mark. Which agent acted and under what recorded authority; which tier of proof the records reach; which independent authority attested them and when. The assurance elements applied by a conformity assessment body, not by the maker.

4.3 Proportionality. The hallmarking exemptions are per article, by weight, and do not scale with the size of the business. They therefore supply the principle that a compulsory mark may carry a de minimis floor, but not a ready-made threshold for records. A threshold by scale of deployment, shared attestation services, or a co-operative model are each available and require argument rather than assertion. A scheme that bore most heavily on the smallest organisations would fail its own purpose.

4.4 Who accredits. A conformance scheme under this proposal maintains a published, append-only register of eligible attestation authorities, maintained independently of any operator claiming conformance, recording for each: identity, jurisdiction, audit status and date, practice-statement reference, and dates of entry and removal. This is ordinary conformity assessment. It also answers the objection that content-provenance schemes attract, where any party may sign and trust reduces to the governance of the accepted-signer list. No particular scheme or critic is cited for that objection here.

5. Personal data

5.1 The substrate does not record content. It records that an actor touched a record, under which authority, in what order relative to other events. It does not record what the record contained.

5.2 That property does not extend upward. A reviewer examining a sampled record may need to read what was written. Content-blindness is a real property of the substrate and is not a property of any examination layer built on it. Such a layer requires its own access rule.

5.3 Erasure is unresolved. A right to erasure requires removal; property 3.1 provides that nothing sealed is removed.

The European Data Protection Board addressed this collision in its Guidelines 02/2025 on processing of personal data through blockchain technologies. It describes keyed hashing with the key held separately as one available measure and qualifies it heavily: the hash is itself personal data, and unlinkability following key destruction holds only while the construction is unbroken and neither key nor salt has been disclosed. It advises that registering personal data in an immutable structure in clear, encrypted or hashed form is not advisable, and recommends alternative tools where the integrity property is not required.

5.4 The position taken here. A scheme that seals the shape of events and never their content is a materially different object from the ledgers that guidance addresses. Any instrument adopting these properties must specify its erasure mechanism and defend it against that guidance rather than assume the distinction is accepted. The mechanism proposed is at MIO-STD-01 §4.6.

5.5 Workplace surveillance. A construct sealing every read creates a record of individuals' attention to their own records. This is a question of legitimacy prior to any question of detection, and is properly answered by those governed rather than by those building.

6. Position in New Zealand

6.1 The standards are adopted. Standards New Zealand has nationally adopted the international AI suite, including NZS ISO/IEC 42001:2025 for AI management systems and NZS ISO/IEC 23894:2025 for AI risk management.

6.2 No assurance programme accompanies them. The national AI strategy of July 2025 contains the word “standards” once, in the phrase “standards bodies”. The words assurance, audit, certification and conformity do not appear, and the International Organization for Standardization is not named.

6.3 This is closeable without new regulation. The strategy states that the approach is “light-touch and principles-based” and “does not require additional regulatory overlay beyond existing law.” On this paper’s reading, conformity assessment is not regulatory overlay: it is the machinery by which a claim becomes checkable, and it is the ordinary route for regulated goods.

6.4 Mechanism. Influence in international standards development runs through a national body vote, a working-group seat or an editorship rather than through a tabled paper. That is the author’s reading of how those bodies work and is not sourced here. New Zealand chairs the 2027 Digital Nations meeting — a scheduled platform, stated in the strategy.

6.5 Constituency. The party served is not the frontier laboratory. It is the public agency, health service, local authority, community organisation and small firm running agents it did not build, inside software it does not control.

7. Recommendations

R1. That regulation specify the evidential properties a record of automated conduct must have, rather than only a retention period.

R2. That software operating autonomous agents carry a conformance mark stating the tier of proof its records reach, with the assurance elements applied by a conformity assessment body and not by the maker.

R3. That a published, append-only, independently maintained register of eligible attestation authorities be established, with stated eligibility criteria and no named suppliers.

R4. That any such instrument specify its erasure mechanism rather than leave it to implementers, and defend that mechanism against published data protection guidance.

R5. That thresholds be set so that the smallest deployments are exempt, on an argued basis.

8. Limitations

8.1 This proposal prevents nothing. It evidences conduct after the fact.

8.2 It does not detect an agent acting improperly. A trustworthy record is the precondition for that and not the achievement of it. See MIO-POL-02.

8.3 It does not reach conduct that never touches the record. What it can show is the use made of what was obtained, since use generally touches the record where acquisition does not.

8.4 An attestation does not establish that a record is true. It establishes what the record stated at a given time, which removes retrospective adjustment and no more.

8.5 None of the components is novel. This is intentional: the proposal requires nothing to be invented.

Status

Draft for comment by an independent author. Drafted with AI assistance and adversarially reviewed by AI agents; the judgements and errors are the author's.

Statutory provisions are quoted from public instruments and represent the author's reading, not a legal opinion. eIDAS is European law; the weight a New Zealand tribunal would give any instrument described here is a question for counsel in that jurisdiction.

How this was made. The version number counts drafts of the text. It does not measure the inquiry behind it, which has run over days and across several AI systems, with argument between those systems and within them, directed, refused and repeatedly redirected by the author. The source material was AI-generated, and then adversarially and iteratively refined across a range of tools — systems built by different companies in different jurisdictions, set against each other and against the author. No one of them produced this text, and no one of them reviewed it alone. **The plurality is deliberate rather than incidental.** A single model carries a single set of priors about which sources are authoritative, and this series argues that an evidence base narrowed in exactly that way is how a contested question comes to look settled. Using one model to investigate that claim would have been the claim refuting itself. To name a single model on it would credit that model with work that was neither its own nor done in a single pass. **The plurality was also necessary, and the record should say why.** In drafting, the assisting model repeatedly led with United States institutional sources — a national laboratory, an industry association, a market study nineteen years old — and presented conclusions drawn from them as the state of knowledge. On one occasion European measured data contradicting those conclusions was present in the same research return and was placed below them. Framings were proposed that would have argued against this series' own position using that evidence base, and offered as rigour. Each was refused by the author and the material rebuilt. That is the mechanism these documents describe, occurring in their own making, and it is recorded because a series arguing that evidence bases narrow without anyone deciding to narrow them cannot credibly claim its own production was exempt. The framing, the corrections and the judgements are the author's, and so are the errors. [How this site is written](#) sets out what is declared on every piece, who checks it, and where the per-piece record lives.

Cite this version

What a Record Must Prove, version 0.4 (September 2026).
`agenticgovernance.digital/downloads/what-a-record-must-prove-v0-4.pdf`

Licensed CC BY 4.0. Reuse is free, including commercially, provided the author is credited and the reuse does not suggest that the author endorses it. This link is frozen at version 0.4; [/what-a-record-must-prove](#) always shows the current one.

PREVIOUS

What we know and what we don't

Series contents

NEXT

When an Agent Exceeds Its Authority

Alongside: questions and answers · sources and provenance