AAS-1

Agent Auditability Standard

Working Paper v0.1 — Draft for Comment

Published by	Kadikoy Limited, Bermuda (Reg. 202302362)
Date	9 May 2026
Status	Draft — open for public comment
Version	0.1 — initial release
Companion to	AIS-1 Agent Identity Standard (ais-1.org)
Contact	info@aiagentsservices.net
Repository	github.com/Kadikoy1/aas-1
Website	aas-1.org
License	Creative Commons CC0 — no rights reserved

v0.1 KEY FEATURES	
INTRODUCES	First open standard for evidentiary records of autonomous agent activity
DEFINES	Five record classes — Action (A), Batch (B), Continuous (C), Determination (D), Engagement (E)
SPECIFIES	Twelve standard audit assertions — seven classical, five agent-specific
BINDS	Every AAS-1 record references an AIS-1 identity for actor and (in Class D) auditor
NEUTRAL	Cipher-suite agnostic; JCS canonicalisation; SHA-256 default; technology-neutral evidence
MAPS	Designed to compose with ISA 315/330, ISAE 3000-series, AICPA AU-C, SOC frameworks
ANCHORS	PayAgent worked example — first ALA to emit AAS-1 records from production

ABSTRACT

AAS-1 defines an open standard for evidentiary records of autonomous agent activity, designed to support the formation of independent assurance opinions over actions taken by AI agents. It addresses what we call the **Unauditable Agent Problem**: agents are now executing transactions, making decisions, and producing outputs at scale, yet the records they leave behind are platform-specific, unstructured, and not designed for assurance.

AAS-1 specifies a five-class record structure — Action, Batch, Continuous, Determination, Engagement — and twelve standard assertions adapted from established audit frameworks and extended with five new assertions specific to autonomous agents. Every AAS-1 record binds to an AIS-1 identity, allowing the actor of every recorded action to be cryptographically verified.

AAS-1 is the audit complement to AIS-1 (Agent Identity Standard). Where AIS-1 answers *who is the agent*, AAS-1 answers *what did the agent do, under whose authority, and how do we know*. The standard is published as a working paper for public comment, released CC0, with reference schemas and a worked example available at the public repository.

CONTENTS

1. Motivation and Problem Statement
2. Definitions
3. The AAS-1 Standard
   3.1 The Audit Record
   3.2 Class A Action Record Attributes
   3.3 Evidence Types
   3.4 Determination Attributes
4. Record Classes
5. Audit Assertions
   5.1 Classical Assertions
   5.2 Agent-Specific Assertions
6. Schema Specification
   6.1 Class A JSON Schema
   6.2 Canonicalisation and Hashing
   6.3 Signature Object
7. AIS-1 Binding
   7.1 Identity Resolution
   7.2 Auditor Identity
   7.3 Verification Flow
8. Comparison with Existing Frameworks
9. Security Considerations
10. Regulatory and Framework Compatibility
11. Implementation Roadmap
12. Request for Comment
13. Authors

App. A Class A Record — Worked Example
App. B Auditor Verification Flow
App. C Mapping to Classical Audit Assertions

1. Motivation and Problem Statement

The global population of AI agents is now estimated in the hundreds of millions and growing at machine speed. Agents are executing financial transactions, dispatching communications, filing documents, calling tools, retaining memory, and acting on behalf of natural and legal persons across every sector. As that population grows, so does the volume of activity that would, in any human-controlled process, be subject to assurance, audit, or independent review.

Yet the records agents leave behind are platform-specific, unstructured, and not designed for assurance. We term this the **Unauditable Agent Problem**. The consequences are already visible:

- Audit firms cannot form opinions on processes that involve autonomous agents because the evidence does not exist in a portable, attestable form.
- Each platform invents its own logging, telemetry, and event format. Records are not interoperable across audit firms or regulators.
- Auditors cannot cryptographically verify that the actor of a recorded action was the agent of record, or that the agent was authorised to take it.
- Continuous and real-time assurance is impossible at agent speeds without a standard evidentiary format.
- Regulators cannot map agent activity onto existing audit frameworks (ISA, ISAE, AT-C) without an interface layer.

Existing standards do not solve this. AICPA SOC reports and ISAE 3402 govern service organisations, but the controls model assumes human operators and human-supervised systems. Blockchain attestation services (RFC 3161 timestamping, transparency logs, on-chain anchors) provide useful primitives but no semantic record format. Audit working papers exist within the audit firm and are not portable across engagements. None address the specific challenge of producing evidentiary records about an agent's activity that any independent reviewer can evaluate against a standard set of assertions.

AAS-1 addresses this gap by defining a portable evidentiary record format, anchored to AIS-1 identities, evaluable against twelve standard assertions, and designed to compose with established audit frameworks rather than replace them.

2. Definitions

Term	Definition
AI Agent	A software system that perceives its environment, makes decisions, and takes actions to achieve goals. May be autonomous or supervised. As defined in AIS-1.
Principal	The legal or natural person on whose behalf the agent acts. Typically the agent's sponsor under AIS-1, or a delegated counterparty.
Auditor	An independent reviewer — human or agent — that issues a Class D determination over a set of subject records.
Action Record (Class A)	An evidentiary record of a single agent action, with its identity, action attributes, evidence array, and signature. The atomic unit of AAS-1.
Batch Record (Class B)	An aggregation of Class A records over a defined period, with a Merkle root over the canonicalised members.
Continuous Record (Class C)	A single entry within a continuously attested stream, bound by a stream-anchor record. Designed for high-frequency or always-on agents.
Determination (Class D)	An auditor's finding over subject records, with per-assertion results and an overall finding type.

Term	Definition
Engagement (Class E)	Audit engagement metadata: scope, period, applicable framework, materiality threshold, agent population in scope.
Assertion	A standard property to be evaluated against a record. AAS-1 v0.1 defines twelve assertions.
Evidence	Any cryptographic, attestational, log-based, or human attestation supporting a Class A record. Multiple evidence entries may attach to a single record.
Canonicalisation	The deterministic serialisation of a record prior to hashing or signing. AAS-1 specifies JCS (RFC 8785) as default.
Timestamp Service	An auditable timestamping authority. AAS-1 reuses the AIS-1 §3.4 primitive — technology-neutral and optional, supporting RFC 3161, OpenTimestamps, HCS, or implementer-defined services.

3. The AAS-1 Standard

3.1 The Audit Record

AAS-1 defines the **audit record** as the fundamental unit of agent assurance. An audit record is a structured, signed, attestable document that captures a single agent action and the evidence supporting it. Every audit record contains five primitives: an actor identity (via AIS-1), a principal identity, an action description, an evidence array, and a signature.

Audit records are designed to be portable: any auditor in possession of a record and the referenced AIS-1 identity document can verify the signature, evaluate the assertions, and issue an independent determination. Records may be aggregated (Class B), streamed (Class C), or evaluated (Class D) without modification to the atomic record.

3.2 Class A Action Record Attributes

Attribute	Description	Required
aas	Standard version. v0.1.	Yes
eventId	ULID or UUID, unique within the issuer.	Yes
class	Record class. "A" for Action Records.	Yes
agentRef	URI of the AIS-1 identity that issued the action. Typically a did:ais1 DID.	Yes
principalRef	URI of the legal or natural person on whose behalf the agent acted.	Yes
delegationRef	URI of the delegation, authorisation, or mandate under which the agent acted.	Optional
engagementRef	URI of a Class E engagement record this action falls within.	Optional
timestamp	RFC 3339 timestamp of the action.	Yes
timestampServiceRef	URI of the timestamping authority. Reuses AIS-1 §3.4 primitive.	Yes
action	Action object (see §3.2.1). Captures type, hashes, tools, model.	Yes
policyRefs	Array of URIs to policies applicable to this action.	Optional
policyResult	Compliance evaluation result against policyRefs.	Optional
materiality	Monetary or risk-weighted indicator for the action.	Optional
evidence	Array of evidence entries (see §3.3). Minimum one entry.	Yes
attestations	Array of execution-environment or third-party attestations.	Optional
prevHash	Hash of the immediately preceding record, for chain integrity.	Optional
signature	Signature object over the canonicalised record.	Yes
notes	Free-text issuer notes.	Optional

3.2.1 The action object

The `action` object describes what the agent did. It contains the action type, the hashed inputs and outputs (preserving privacy while enabling integrity verification), the tools or MCP servers invoked, and the model identifier used.

Attribute	Description
type	tool_call | decision | communication | transaction | policy_check | human_handoff | other
inputsHash	Hash of canonicalised inputs.
outputsHash	Hash of canonicalised outputs.
tools	Array of tools invoked. Each entry: { name, version, serverRef }.
model	{ id, version } for the model used.
summary	Optional human-readable summary.

3.3 Evidence Types

Evidence is technology-neutral. Each entry in the `evidence` array has a `type` and a `value`; the format of the value depends on the type. AAS-1 v0.1 recognises six evidence types. Implementations MAY define additional types under a reverse-DNS namespace.

Type	Description
signature	A cryptographic signature over the record or a specified subset.
attestation	An attestation from an execution environment — TEE quote, MPC quorum, secure enclave.
witness	A co-signing witness — an independent party that signs alongside the issuer.
log	Reference to an external append-only log entry.
hash_anchor	Content hash anchored to a public ledger or notary service (e.g. Ethereum, OpenTimestamps).
human	Human attestation — auditor, principal, Commissioner for Oaths, or other authorised person.

3.4 Determination Attributes

A Class D determination captures an auditor's finding. The auditor — which under AAS-1 may be either a human or an agent, since `auditorRef` is itself an AIS-1 identity — evaluates a set of subject records against the twelve assertions and issues an overall finding.

Attribute	Description
aas	Standard version. v0.1.
eventId	ULID or UUID, unique within the auditor.
class	"D"
auditorRef	URI of the AIS-1 identity of the auditor (human or agent).

Attribute	Description
engagementRef	URI of the Class E engagement under which this determination is issued.
subjectRefs	Array of URIs to records under examination.
finding	unmodified | modified | adverse | disclaimer | exception
assertionResults	Per-assertion evaluation. Each entry: { assertion, result, notes }.
timestamp	RFC 3339.
timestampServiceRef	URI of timestamping authority.
signature	Signature object over the canonicalised determination.

4. Record Classes

AAS-1 v0.1 defines five record classes. Class A is the atomic unit. Classes B and C are aggregations over multiple Class A records. Classes D and E are auditor outputs. A complete audit trail typically comprises many Class A records, organised by Class B or Class C aggregations, evaluated against a Class E engagement, and concluded with Class D determinations.

Class	Name	Issuer	Purpose	v0.1 Status
A	Action	Agent / operator	Single agent action with evidence. Atomic unit.	Schema published
B	Batch	Operator	Aggregation of Class A records over a period. Merkle root over members.	Schema in v0.2
C	Continuous	Operator	Single entry within a continuously attested stream. Bound by stream-anchor.	Reserved; v0.2
D	Determination	Auditor	Finding over subject records. Per-assertion results and overall finding type.	Attributes specified
E	Engagement	Auditor	Engagement metadata: scope, period, framework, materiality, population.	Attributes specified

5. Audit Assertions

AAS-1 records support twelve standard assertions. Seven are adapted from established audit frameworks (ISA 315/330, AICPA AU-C, ISAE 3000-series). Five are new assertions specific to the audit of autonomous agents. An auditor evaluates every applicable assertion in a single pass before issuing a Class D determination.

5.1 Classical Assertions

Assertion	Definition	Source
Existence	The recorded action actually took place.	ISA 315 / AU-C
Completeness	All relevant actions in scope are recorded.	ISA 315 / AU-C

Assertion	Definition	Source
Accuracy	Inputs and outputs are faithfully captured.	ISA 315 / AU-C
Authorisation	The agent acted within delegated authority.	AU-C 315 / SOC
Cutoff	The action is recorded in the correct period.	ISA 315
Classification	The action is correctly categorised by type.	ISA 315
Presentation	Records are presented and described accurately.	ISA 315 / IFRS

5.2 Agent-Specific Assertions

Assertion	Definition	Why agent-specific
Identity	The recorded actor is the agent of record.	Agents lack natural identity continuity; AIS-1 binding is required.
Provenance	Model, tools, prompt context and data sources are captured.	Agent outputs are a function of model + context + tools.
Reproducibility	Sufficient state to permit re-derivation under stated determinism.	Agents may be probabilistic; reproducibility must be asserted, not assumed.
Policy Compliance	Applicable policies and the action's compliance result are recorded.	Policy enforcement is the primary control surface for autonomous agents.
Independence	Agent action is recorded separately from any operator override.	Agent autonomy and operator intervention must be distinguishable on the record.

6. Schema Specification

6.1 Class A JSON Schema

The Class A schema is published as JSON Schema 2020-12 at `github.com/Kadikoy1/aas-1/blob/main/schemas/aas-1-class-a.schema.json`. It is normative for v0.1. Class B, C, D and E schemas are deferred to v0.2.

6.2 Canonicalisation and Hashing

Records MUST be canonicalised before hashing or signing. v0.1 specifies **JCS (RFC 8785)** as the default canonicalisation. The hash algorithm is declared per-record in the `signature` object; **SHA-256** is the default. Implementations MAY use other algorithms by setting the `hashAlg` field, but verifiers SHOULD reject unknown algorithms unless they are present in a published algorithm registry.

6.3 Signature Object

Field	Description
alg	Signature algorithm identifier (e.g. EdDSA, ES256K).
hashAlg	Hash algorithm. Default SHA-256.
canonicalisation	Canonicalisation method. Default JCS.
keyRef	Verification method identifier within the AIS-1 identity document.

Field	Description
value	The signature value, base64url-encoded.

7. AIS-1 Binding

AAS-1 is designed to compose with AIS-1, the Agent Identity Standard. Every AAS-1 record MUST reference an AIS-1 identity in `agentRef`. Class D determinations MUST reference an AIS-1 identity in `auditorRef`. The two standards together provide a complete actor-and-action evidentiary system.

7.1 Identity Resolution

A verifier dereferences `agentRef` using the AIS-1 §7.1 resolution algorithm. The returned DID Document contains the verification methods (public keys) used to validate the record signature, the agent class ("ala" or "soa"), and — for SOA — the parent ALA DID. A verifier MAY also confirm the agent's bond is active by calling `verifyBond(bondId)` on the AIS-1 contract.

7.2 Auditor Identity

The `auditorRef` in a Class D record is itself an AIS-1 identity. This means the auditor may be either a natural person (typically with a Sovereign-tier sponsor card identifying them as a qualified auditor in their jurisdiction) or an AI agent (with an ALA bond and an appropriate Assurance Container). Agent-on-agent audit is a first-class capability of the standard, not an extension.

7.3 Verification Flow

```
// Verifier flow — evaluating an AAS-1 Class A record

const record    = await aas1.fetch(eventId);
const identity  = await ais1.resolve(record.agentRef);

// 1. Validate the signature against keys in the AIS-1 DID Document
assert(verifySignature(record, identity.verificationMethod));

// 2. Optionally confirm the bond is active
const bond = await ais1.verifyBond(identity.bondId);
assert(bond.valid &amp;&amp; bond.amlStatus === 'cleared');

// 3. Evaluate the twelve assertions
const findings = await auditor.evaluate(record, {
  identity,
  assertions: AAS1.ALL_ASSERTIONS,
  policies:   record.policyRefs
});

// 4. Issue a Class D determination
if (findings.allSatisfied) {
  await auditor.issueClassD({ finding: 'unmodified', ... });
} else {
  await auditor.issueClassD({ finding: 'modified', exceptions: findings.exceptions });
}
```

8. Comparison with Existing Frameworks

AAS-1 is designed to compose with — not replace — established audit and assurance frameworks. The table below summarises the gap each existing framework leaves and the contribution AAS-1 makes.

Framework	Scope	Gap addressed by AAS-1
ISA 315 / 330	Auditor's risk identification and response.	No standardised evidentiary record format for agent activity.
ISAE 3000-series	Assurance over non-financial subject matter.	No agent-specific assertion catalogue or identity primitive.
AICPA SOC 1 / SOC 2	Service organisation controls.	Controls model assumes human operators; no agent identity binding.
AT-C 105	Concepts common to all attestation engagements.	No record format that can carry assurance from issuer to reviewer.
RFC 3161 / OpenTimestamps	Trusted timestamping.	Provides primitive only; no semantic record format.
W3C Verifiable Credentials	Claims about an entity.	No agent-action semantics; not designed for continuous activity.
AIS-1	Agent identity (companion standard).	Identity only; AAS-1 provides the activity layer.
AAS-1 (this standard)	Agent activity records and determinations.	First open standard for portable, attestable agent auditability evidence.

9. Security Considerations

9.1 Record Integrity

Every Class A record MUST be signed by the agent or operator identified in `agentRef`. Records MAY include a `prevHash` field referencing the canonical hash of the immediately preceding record, creating a per-issuer hash chain. A verifier presented with a complete chain can detect omission, reordering, or substitution of records.

9.2 Privacy and Selective Disclosure

Class A records contain hashed inputs and outputs by default rather than raw values. This preserves privacy while enabling integrity verification: a counterparty in possession of the raw inputs can recompute the hash and verify the record without the auditor needing access to the underlying data. Selective disclosure of attributes (e.g. revealing only the materiality amount and not the counterparty) is a v0.2 work item.

9.3 Replay and Substitution

A signed AAS-1 record is bound to its `eventId`, `timestamp`, and `agentRef`. Replay of a record under a different identity requires re-signing and is therefore detectable. Substitution of inputs or outputs is detectable through the hash fields in the action object.

9.4 Determination Independence

AAS-1 does not enforce auditor independence at the protocol level. Independence is an engagement-level property captured in the Class E record (e.g. by reference to applicable ethical standards) and is the responsibility of the auditor and the engaging party. The standard supports independence by making the auditor's identity and engagement metadata verifiable.

10. Regulatory and Framework Compatibility

10.1 Mapping to Audit Frameworks

AAS-1 records are designed to map cleanly onto the assertion frameworks of major audit standards. Appendix C provides a draft mapping table. The mapping is normative in spirit but not yet definitive; v0.2 will publish a formal mapping annex agreed with practising auditors.

10.2 Regulatory Profiles

The standard supports regulatory profiles — domain-specific overlays that add required fields, evidence types, or assertions for a particular jurisdiction or sector. Profiles in scope for v0.2 include:

- Bermuda DABA Class M and Class F digital asset business profile.
- SOC 2 / ISAE 3402 service organisation profile.
- Statutory audit profile for entities whose financial statements rely on agent-controlled processes.
- Tax-authority profile for agent-issued invoices and receipts.
- FATF Travel Rule profile for agent-initiated payments.

10.3 Continuous Assurance

Class C streams enable continuous assurance — the issuance of Class D determinations on a rolling basis as new Class A records arrive. Continuous assurance is supported architecturally in v0.1 through the Class C reservation and is fully specified in v0.2.

11. Implementation Roadmap

Phase	Deliverable	Target
0.1 — This document	Specification, Class A schema, worked example, public website	May 2026
0.2 — Schemas	Class B, C, D, E schemas. Materiality methodology. ISA 315/330 mapping annex.	Q3 2026
0.3 — Reference engagement	PayAgent emits Class A over 90 days; reference Class D determination published.	Q4 2026
0.4 — Regulatory profiles	DABA, SOC 2, ISAE 3402, statutory audit profiles published.	Q4 2026
0.5 — Conformance suite	Test vectors, conformance harness, and reference verifier.	Q1 2027
1.0 — Standardisation track	Submission to IFAC and ISO/IEC JTC 1. Stable schemas. Authorised reviewer programme.	Q2 2027
1.1 — Tooling integration	Reference adapters for major audit-tooling platforms; continuous assurance pipelines.	Q3 2027
2.0 — Agent commerce	AAS-1 as the assurance layer for agent payment and settlement protocols (Clavus, x402).	2027

12. Request for Comment

AAS-1 v0.1 is published as a draft for public comment. Feedback is invited from practising auditors and assurance professionals; AI agent developers and framework maintainers; blockchain and cryptography engineers; legal, regulatory, and compliance professionals; enterprise deployers of AI agents; government and regulatory bodies; and standards organisations including IFAC, AICPA, IAASB, ISO, IEEE, and W3C.

Feedback may be submitted via:

- Feedback form: aas-1.org/#feedback
- Email: info@aiagentsservices.net
- GitHub: github.com/Kadikoy1/aas-1/issues

The comment period for v0.1 closes **31 July 2026**. A revised draft will be published as v0.2.

13. Authors

Field	Value
Author	Kadikoy Limited, Bermuda
Affiliation	BDA Law; BDA AI Agent Services
Companion	AIS-1 — Agent Identity Standard (ais-1.org)
Contact	info@aiagentsservices.net
Website	aas-1.org
Repository	github.com/Kadikoy1/aas-1
License	Creative Commons CC0. No rights reserved. Open for free implementation.

Appendix A: Class A Record — Worked Example

The following is a complete Class A action record. PayAgent (Bond No. 1, an ALA under AIS-1) executes a stablecoin transfer of USD 2,500 on behalf of its sponsor, Kadikoy Limited, pursuant to a documented invoice. The record carries four pieces of evidence: an issuer signature, an execution-environment attestation, a hash anchor, and a log reference.


```
{
  "aas": "0.1",
  "eventId": "01HZ8KQ3M7YPB4N9XJ2VQ5RTFW",
  "class": "A",
  "agentRef": "did:ais1:base:payagent-001",
  "principalRef": "did:ais1:sponsor:kadikoy-bm-202302362",
  "delegationRef": "https://kadikoy.bm/delegations/2026-q2-payments",
  "engagementRef": "https://audits.example.com/engagements/kadikoy-2026-h1",
  "timestamp": "2026-05-09T14:32:11Z",
  "timestampServiceRef": "rfc3161:tsa.example.com",
  "action": {
    "type": "transaction",
    "inputsHash": "sha256-9f86d081...",
    "outputsHash": "sha256-2c26b46b...",
    "tools": [
      { "name": "stablecoin-transfer", "version": "1.4.0",
        "serverRef": "https://mcp.payagent.ai/transfer" }
    ],
    "model": { "id": "claude-opus-4-7", "version": "2026-04" },
    "summary": "Outbound USDC transfer 2,500.00 to vendor wallet"
  },
  "policyRefs": [
    "https://kadikoy.bm/policies/payments/v3",
    "https://kadikoy.bm/policies/aml-screening/v2"
  ],
  "policyResult": { "outcome": "compliant",
    "details": "Counterparty cleared screening; within delegated USD 5,000 limit." },
  "materiality": { "currency": "USD", "amount": 2500.00, "basis": "transaction-value" },
  "evidence": [
    { "type": "signature",   "value": "z3JmTpXq...",
      "issuerRef": "did:ais1:base:payagent-001#key-1" },
    { "type": "attestation", "value": "TEE-quote-base64...",
      "issuerRef": "https://attest.example.com/tee/0xabc123" },
    { "type": "hash_anchor", "value": "ethereum:0x4f3edf...",
      "issuerRef": "https://etherscan.io" },
    { "type": "log",         "value": "https://logs.payagent.ai/2026/05/09/01HZ...",
      "issuerRef": "did:ais1:base:payagent-001" }
  ],
  "prevHash": "sha256-7d865e95...",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:payagent-001#key-1",
    "value": "z58dYMy3..."
  },
  "notes": "Routine treasury payment. No human override invoked."
}
```


Appendix B: Auditor Verification Flow

How an independent auditor verifies an AAS-1 Class A record and issues a determination:

1. Receive the Class A record (and, where applicable, the enclosing Class B batch or Class C stream).
2. Resolve `agentRef` via the AIS-1 §7.1 resolution algorithm. Retrieve the DID Document.
3. Validate the record `signature` against the verification method declared in the DID Document.
4. Confirm the AIS-1 bond is active by calling `verifyBond(bondId)` on the AIS-1 contract.

5. Evaluate the secondary timestamp via `timestampServiceRef` if present.
6. Recompute `inputsHash` and `outputsHash` against the underlying data, where the auditor has access. Where the auditor does not have access, accept the principal's attestation.
7. Evaluate every applicable assertion (§5) against the record. Record exceptions.
8. For batch or continuous evaluation, apply the auditor's sampling methodology and aggregate findings.
9. Issue a Class D determination with the appropriate finding type (unmodified, modified, adverse, disclaimer, exception) and per-assertion results.
10. Sign the Class D determination using the auditor's AIS-1 verification method.

Appendix C: Mapping to Classical Audit Assertions

The following draft mapping shows how AAS-1 fields support evaluation of each classical assertion. v0.2 will publish a formal mapping annex agreed with practising auditors.

Assertion	AAS-1 fields supporting evaluation
Existence	evidence[type=signature, attestation, hash_anchor]; timestamp; timestampServiceRef
Completeness	prevHash chain; Class B Merkle root; Class C stream-anchor
Accuracy	action.inputsHash; action.outputsHash; recomputed against principal's data
Authorisation	delegationRef; principalRef; AIS-1 bond verification
Cutoff	timestamp; timestampServiceRef (independent timestamp)
Classification	action.type; action.tools; action.summary
Presentation	Canonicalisation (JCS); record self-description
Identity	agentRef; AIS-1 DID Document; verifyBond()
Provenance	action.model; action.tools; action.inputsHash
Reproducibility	action.inputsHash; action.outputsHash; action.model; action.tools
Policy Compliance	policyRefs; policyResult
Independence	Separation of agent signature from any operator override evidence entry