AEIP v1 Specification

Status: Reference Implementation Alignment
Scope: Transport handshake for reasoning integrity and artifact exchange

1. Protocol Summary

AEIP v1 provides a deterministic, persona-signed negotiation channel that links reasoning traces to ledger-grade artifacts. The protocol is intentionally human-auditable and uses SHA3-512 hashes plus Ed25519-compatible signatures.

2. Message Headers

Field	Description	Mandatory
`aeipVersion`	Protocol version identifier. Current: `1.0`.	YES
`temporalSeal`	RFC3339 timestamp concatenated with SHA3-512 digest.	YES
`personaSignature`	Ed25519 placeholder signature (persona bound).	YES
`governanceScope`	Governance namespace (e.g., `demo`, `production`).	YES
`dignityCompliance`	Boolean flag ensuring Persona guardrails.	YES

3. Handshake Steps

1. **Intent** Initiator declares objective and attaches Instructional Task Plan (ITP).
2. **Justify** Counterparty provides Decision Rationale Record (DRR) elements and confirms constraints.
3. **CounterSign** Initiator re-confirms, signs, and extends provenance metadata.
4. **Commit** Counterparty finalises obligations and creates Governance Directive Set (GDS).
5. **Update** Initiator issues Oversight Assurance Metrics (OAM) snapshot and requests ledger entry.

Each step MUST include provenance fields and a persona signature covering the canonical payload plus headers.

4. Serialization Rules

* JSON is the canonical wire format. YAML MAY be used for diagnostics and MUST round-trip to JSON without data loss.
* JSON-LD contexts MAY be attached under `@context` for semantic interoperability.
* Field ordering is irrelevant; canonicalization uses lexicographic JSON serialization prior to hashing.

5. Integrity Guarantees

* Hashing: SHA3-512 across canonical JSON payloads.

* Signatures: Deterministic Ed25519 placeholder (ready for HSM swap).
* Temporal Governance: `temporalSeal` is re-issued at every step and SHALL be monotonic.

6. Failure Modes

* Missing or invalid signatures SHALL abort the handshake.
* `dignityCompliance=False` SHALL propagate as a refusal and MUST block ledger submission.
* Hash drift triggers `LedgerVerificationError` within the governance node.

7. Extensibility

* Additional headers MUST be namespaced under `x-` prefixes.
* Alternative persona signature algorithms SHALL declare their algorithm name in the signature object.
* Version negotiation occurs during Intent by including `supportedVersions` array in the payload.

Refer to `/protocol/aeip_handshake.py` and `/tests/test_aeip_handshake.py` for executable reference behaviour.