

[CAPABILITY PROFILE · SIM-14]

AUTHREX-DA · DATA ADMISSIBILITY LAYER (ENGINEERING PREVIEW)

Extend evidence-to-authority mapping from actions to data: every record or federated model contribution offered to a system receives a verdict on its admissibility, non-compensatory and fail-closed, before it is allowed to influence anything.

IMPLEMENTED	TESTED	PROPOSED	NOT YET VALIDATED
PRIMARY FUNCTION	Fail-closed admissibility gate: every record offered receives ADMIT, ADMIT_FLAG, QUARANTINE, or REJECT with a reason code and an evidence reference, written to an append-only record; the layer never repairs, imputes, or reconstructs a payload; deterministic under AUTHREX-DA-CANON-1 numeric canonicalization.		
MISSION AREAS	Federated learning and model-update admission; sensor and data-record integrity for AI-enabled C2 and ISR pipelines; data provenance and poisoning resistance.		
EVIDENCE ANCHORS	101 of 101 local tests; 12 ordered release gates over the whole shipped tree; 14 requirements at 12 TEST_PASS_LOCAL, 1 PARTIAL_LOCAL, 1 BLOCKED; archived canonical ledger root, engine-bound, seed 20260828, 120 rounds, 1,584 entries; 17-artifact assurance package under a three-part commitment; 19 audit passes (5 internal, 14 external), which is not independent reproduction; retained negative results NEG-1 to NEG-5.		
CURRENT STANDING	Proposed engineering preview, release 1.8, core engine 1.0; locally tested and gate-checked; not certified, accredited, authorized, operationally validated, or independently reproduced; WP-0 (quorum repair) blocked; no property DA-P1 to DA-P9 model checked.		
SELF-ASSESSED TRL	TRL 2 to 3. No formal TRL determination has been performed. The self-assessed rubric of 51 of 100 is expressly not a DoD score, a TRL, a certification, an authorization, or an endorsement.		
SCOPE STATEMENT	Governance and assurance only: no detection, identification, classification, selection, prioritization, or optimization of any effect.		

[MISSION PROBLEM]

AI-enabled systems ingest data records and model contributions whose provenance and integrity cannot be assumed, and most pipelines treat admission as a data-quality question answered by cleaning or imputation. A poisoned contribution admitted on the strength of agreement, or a record silently repaired into plausibility, changes what the system believes without any authority decision having been made. The consequence is a model or picture that was never authorized to change.

[OPERATIONAL RELEVANCE]

- Federated model contributions across platforms or partners, where a majority capture by contaminated contributors is the named open failure (NEG-3).
- Data records feeding a common operating picture or ISR product.
- Software supply chain and provenance: the same admissibility logic applies to artifacts as to records.
- Zero-trust data principles: never admit by default; verify before influence.

[CAPABILITY DESCRIPTION]

AUTHREX-DA is a variant configuration of the governance layer. Each offered record passes an admissibility gate that applies the evidence-to-authority mapping to data rather than to actions: required evidence conditions are evaluated independently, a strong condition never compensates for a failed one, and the default on any failure is to withhold admission. The four verdicts carry a reason code and an evidence reference and are written to an append-only hash chain with an external commitment check. Numeric canonicalization (AUTHREX-DA-CANON-1) makes the engine deterministic across platforms so that a reviewer can reproduce the archived ledger root from the seed. The layer records what it refused and why; it never alters a payload.

[AUTHREX-DA · ARCHITECTURE, ASSURANCE, EVIDENCE]

[TECHNICAL ARCHITECTURE]

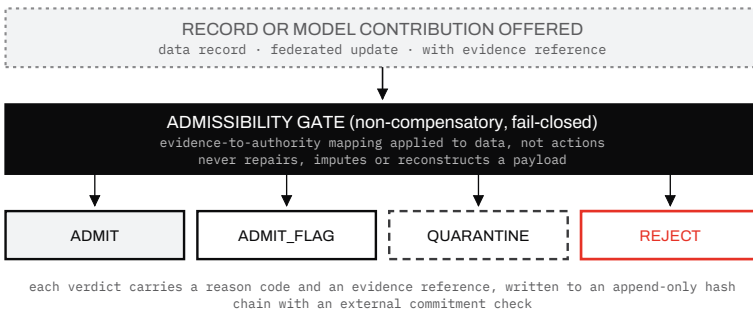


Figure 1. AUTHREX-DA technical architecture. Encoding: solid = implemented; dashed = specified; gray = external; filled = enforcement point.

[TECHNICAL DIFFERENTIATION]

Data-quality tooling cleans and imputes; DA refuses and records. Anomaly detection flags; DA converts the flag into an admissibility verdict that downstream consumers must honor. The architectural difference is that admission becomes an authority decision with an audit trail, not a preprocessing step.

[ASSURANCE MECHANISMS: DESIGN PROPERTY VERSUS ESTABLISHED PROPERTY]

Mechanism	Status
Fail-closed default on evaluation failure	Design property; locally tested
Non-compensatory admission	Design property; locally tested
Never repairs, imputes, or reconstructs a payload	Design property; locally tested
Deterministic canonical ledger root	Reproduced on one platform (engine-bound root archived); second-platform root pending
Properties DA-P1 to DA-P9	NOT model checked (WP-0 blocked; formal work surrogate only)
Resistance to majority capture	NOT established: NEG-3 majority-capture failure retained as an open requirement

[TECHNICAL EVIDENCE]

Evidence	Result	Source / artifact
Local test suite	101 of 101 tests; 12 ordered release gates over the whole shipped tree	SIM-14 release 1.8 package
Requirements status	14 requirements: 12 TEST_PASS_LOCAL, 1 PARTIAL_LOCAL, 1 BLOCKED	release 1.8 package
Canonical ledger root	seed 20260828, 120 rounds, 1,584 entries, engine-bound; single platform	release 1.8 package
Audit passes	19 on file (5 internal, 14 external); external audit review is not independent reproduction	release 1.8 package
Negative results	NEG-1 to NEG-5 retained, including NEG-3 majority-capture failure	release 1.8 package

[EVIDENCE SNAPSHOT]

EVIDENCE SNAPSHOT	
Implemented	Yes (preview engine)
Executable artifact	Yes
Formal model	No (surrogate only)
Simulation evidence	Yes (single seed)
Hardware validation	N/A
Field validation	No
Independent validation	No
Government evaluation	No
Operational deployment	No

[LIMITATIONS]

- WP-0 (quorum repair, closing the roster-derived fault-bound defect inherited from MAIVA) is blocked; it gates every later work package.
- One seed; no preregistered campaign; no confidence intervals; single-platform canonical root.
- Majority-capture failure (NEG-3) is an open requirement: a contaminated majority of contributors can carry admission.
- 38 numbered open items are published with the release; the engineering preview is not a release candidate.

[TECHNOLOGY READINESS (SELF-ASSESSED; NO FORMAL TRA)]

CURRENT ASSESSED TRL	TRL 2 to 3 (self-assessed against the DoD nine-level scale; no formal technology readiness assessment has been performed).
BASIS	Concept implemented as a locally tested preview; the critical property set is not formally established and the named open failure prevents a proof-of-concept claim for the multi-contributor case.
EVIDENCE SUPPORTING	concept and requirements; local implementation and tests; single-seed deterministic evidence
EVIDENCE REQUIRED FOR NEXT TRL	(1) Close WP-0 and model check DA-P1 to DA-P9 with a faithful model. (2) Preregistered multi-seed campaign with confidence intervals; second-platform canonical root. (3) Government-furnished records with known poisoned or malformed entries for a Phase 2 admission evaluation.

[INTEGRATION PROFILE]

INPUTS	Records or model contributions with evidence references; admissibility policy.
OUTPUTS	Verdict with reason code; append-only ledger; assurance package.
INTERFACES	Standalone console today; a pipeline stage in a data or federated-learning flow by design.
DEPLOYMENT	Client-side, deterministic browser build; no network.
SECURITY BOUNDARY	Inside: gate, canonicalization, chain. Outside: record sources, downstream consumers that must honor QUARANTINE and REJECT.
DATA REQUIREMENTS	Synthetic; government-furnished records with ground truth would enable evaluation.

[TRANSITION ROADMAP]

Phase	Activity for this capability	Who can execute it	Exit evidence
1 Technical review	Review of the artifacts listed in the evidence table	Program alone, with a government reviewer	Reviewer findings; correction log entries
2 Government-defined simulation	Sponsor scenarios on the seeded console	Program with sponsor scenarios	Deterministic, replayable results; hash-chained records
3 Degradation and failure injection	Evidence lapse, spoofing, delayed human response	Program with sponsor parameters	False-restriction, miss, and contraction-latency figures
4 Government testbed / SIL	Integration with a representative controller or interface	Requires sponsor interface and testbed	SIL integration report
5 Hardware-in-the-loop	Representative interference; timing on real hardware	Requires sponsor laboratory or rig	Measured latencies; TRL 4 to 5 evidence
6 Relevant-environment demonstration	Independent evaluation and red team	Requires independent evaluator	Independent report
7 Program integration	Only after earlier gates succeed	Requires transition partner	Not claimed to be available

[GOVERNMENT ENGAGEMENT REQUEST (SPECIFIC)]

- Review of the admissibility requirement set by a data-integrity or federated-learning program.
- A government dataset with labeled poisoned or malformed records for Phase 2.
- Independent reproduction of the canonical ledger root on a second platform.

[REVIEWER QUESTIONS THIS PROFILE ANSWERS]

What is it: see capability description. Why does DoD care: see operational relevance. Where would it fit: see integration profile. Does it exist: see evidence snapshot. What evidence supports it: see technical evidence. Has anyone independent tested it: no. Has it been tested in the real world: no. What does it rely on: see limitations and security boundary. What can cause it to fail and what does it do then: see assurance mechanisms and the published counterexamples. How mature: see the TRL block. What would the government need to provide: see the request above. Next measurable milestone: first item under evidence required for next TRL.