



DISPUTE PACK

Agentic Execution - Tool-Chained Authority Expansion

World: Agentic Execution Governance **Outcome:** ESCALATE **Evidence Pack ID:** JSP-PUBLIC-20260302-AGENTIC_EXEC-0001

1. What was claimed / requested

Agent requests production write access mid-run.

2. What the system allowed vs blocked

Allowed

- Drafting and preparation can continue.
- Execution is paused pending named authority.

Blocked

- Commit actions until approvals are recorded.

3. Why (governance rationale)

Judgement Spine enforces 'no authority expansion by momentum' at execution time. Privilege elevation becomes a governed MTM requiring dual control, scoped TTL, and signed approval tokens before the tool call can execute.

This pack is designed to survive dispute: it links decision, authority, bounds, and integrity in one exportable object.

Evidence references

4. Evidence signals

- requested_tool
- requested_scope
- ttl_requested
- current_delegation_token
- secret_access_in_scope
- blast_radius_estimate

5. Evidence artefacts in this bundle

policy_trace.ndjson	Which doctrine checks fired and why.
audit_export.ndjson	Execution-time event record.
provenance_chain.json	Illustrative provenance and chain integrity.
authority_contract.json	Named authority + bounds contract.
manifest.json + signature	Integrity references (tamper-evident).

6. Integrity verification

Run `verify_manifest.py` from the root folder and retain the output as part of the dispute file.

If the hashes and signature verify, the pack is unmodified since it was sealed.

Contact: founder@judgementspine.com