

LLSP

Independent authority and evidence architecture for software-engineering agents

Model output is a proposal - not execution authority.

THE PROBLEM Coding agents now inspect repositories, edit files, and run commands. Sandboxes, approvals, and enterprise policy can constrain where agents operate, but they do not by themselves answer a narrower repository question: what software action was proposed, what was authorized, and what actually changed?	LLSP PRINCIPLE LLSP separates semantic proposal from deterministic execution authority. Proposed work crosses a typed boundary; local components decide whether a repository mutation is authorized; the controlled path records structured integrity evidence around the resulting action.
---	---

ARCHITECTURE AT A GLANCE

Agent / Model proposes work	Typed Boundary normalizes contract	Local Authority decides permission	Controlled Mutation executes governed change	Integrity Evidence records action + state
---------------------------------------	--	--	--	---

CURRENT STATUS

IMPLEMENTED CORE • Typed separation between model-generated proposal and local execution authority • Strict contract validation before the governed mutation path • Repository/path boundary checks and state revalidation in the controlled path • Transactional mutation with checkpoint/rollback behavior • Structured integrity evidence, including mutation and hash-linked records	CURRENT DILIGENCE FOCUS • External coding-agent adapters and direct-write containment • Delegated process / subagent / MCP containment under the same boundary • Clean-environment reproducibility across target deployment environments • Signed or source-free third-party verification boundary • Broader adversarial and cross-agent benchmark evidence
---	--

WHY A PLATFORM BUYER MAY EVALUATE IT

Portable semantics Keep the authorization model independent of a single agent or model surface.	Earlier control point Make the decision before repository mutation, not only at review or delivery time.	Evidence boundary Tie proposed work, authorization, and resulting change into one inspectable chain.	Build-vs-buy option Evaluate an implemented architecture while external diligence is still expanding.
---	--	--	---

TRANSACTION CONTEXT

Under evaluation: a Software Engineering / Software Delivery field-of-use technology/IP transaction. **Reserved:** a separate Mission AI field.

Next step: a 25-minute architecture / build-vs-buy review, followed by structured technical diligence if relevant.

Dongyun Lee | Founder, LLSP | founder@llsp.dev