HALTSEAL

HALT real actions. SEAL the evidence.

Verifier → Permit → Fail-Closed Gateways for Agentic AI execution (network egress, privileged I/O, accelerator dispatch).

- Network egress
- Privileged I/O
- Accelerator dispatch

ONE-LINE

Updated 14 Feb 2026 | Public-safe draft

Block real actions (egress / privileged I/O / accelerator dispatch) until the agent presents a verifiable, expiring permit installed at a non-bypassable gateway + audit-ready receipts.

HALTSEAL IN 3 CONTROL PRIMITIVES

1 Verify-to-Activation

Append-only verifiable log publishes signed heads. Runtime checks freshness, inclusion, and consistency.

2 Permit-before-Action

On PASS: mint signed, expiring permit bound to audience (agent/tenant/mission); write an IAL receipt.

3 Fail-Closed Dispositions

On FAIL: HOLD / QUARANTINE / DENY / ESCALATE. Gateways require a valid permit ID before actions.

Outputs: signed head + proofs • permit token • IAL receipts • reason codes

WHY NOW (POLICY PULL)

Agentic AI turns model output into actions. Regulators, auditors, and procurement increasingly ask for provable pre-action controls and audit-ready evidence. HALTSEAL is built to generate receipts, not promises.

PROOF ARTIFACTS (BUYER-FACING)

- Signed head (tree size, root hash, timestamp, signatures; optional witness co-signatures)
- Inclusion proof (ICC commitment is included in the current head)
- Consistency proof (append-only evolution when the head advances)
- Permit token (signed; audience-bound; nonce + monotonic counter; expiry)
- IAL record (hash-chained receipt per decision; exportable to audit systems)
- IP + licensing: Portfolio filed under legacy title “NOVACOV” (U.S. App. Nos. 19/183,800; 19/404,229). Claim charts under NDA.

REGULATORY / POLICY MAPPING

Framework	Timing / buyer ask	HALTSEAL mapping
EU AI Act	High-risk Annex III: 02 Aug 2026 Regulated products: 02 Aug 2027	Pre-action gating + audit receipts (proofs + IAL).
Korea AI Basic Act	In force 22 Jan 2026.	Traceable approvals (tier/quorum) + evidence pack.
US Federal AI governance (OMB M-24-10)	Procurement wants proof of controls.	Controls enforced before action; exportable receipts.
NIST AI RMF + ISO/IEC 42001	Common audit language for AI risk management.	Receipts bind policy + approvals + execution evidence.

DESIGN PARTNER OFFER (6–12 WEEKS)

- Weeks 0–2: Align threat model; pick ONE gateway; lock evidence schema + reason codes.
- Weeks 3–6: Sandbox MVP; demo permit-before-action + receipts export.
- Weeks 7–12: Move enforcement to driver/firmware/hypervisor; harden + pilot-to-prod.

Note: Indicative timeline; non-binding; subject to mutual agreement.

SUCCESS CONDITION: Schedule a 30-minute technical deep dive with Security present. Two questions: (1) top action surface (egress / dispatch / actuation) • (2) evidence consumer (Security / Audit / GRC).

Acronyms: ICC = Immutable Constraint Chain; IAL = Immutable Arbitration Ledger; ELV = Encrypted Logic Vault; GLG = Licensing Gate.