

Technical Architecture Overview

Current public specification of the Hackett Meta OS constitutional enforcement kernel

VERSION 3.0 · AUGUST 2026 · PUBLIC

CORE PROPOSITION

Consequential systems should not be trusted because they are intelligent. They should be governable because their authority is bounded and their consequential actions leave evidence that can survive independent challenge.

HACKETT META OS LLC

Andrew D. Hackett, Founder & Principal Inventor · andrew@hackettmetaos.com · hackettmetaos.com
SAM.gov Registered · UEI Z3XNP7JTYGL2 · CAGE 1A7X7

1 · ARCHITECTURAL THESIS

Consequential systems need a governing layer that remains stable as models, applications, vendors, and mission profiles change. Hackett Meta OS separates the invariant constitutional core from the profiles that adapt it and the applications that consume those profiles.

Layer	Responsibility	Must not imply
Kernel	Authority, policy, evidence, lineage, information-flow, refusal, and amendment invariants.	Mission correctness or certification.
Mission profile	Domain vocabulary, interface mappings, expected evidence, constraints, and local authority structure.	A new constitutional core.
Application	Requests actions and consumes bounded outcomes.	The ability to bypass kernel refusal.
Verifier	Checks a declared bundle and emits bounded findings.	Operational command authority.

HACKETT META OS LLC

Andrew D. Hackett, Founder & Principal Inventor · andrew@hackettmetaos.com · hackettmetaos.com
SAM.gov Registered · UEI Z3XNP7JTYGL2 · CAGE 1A7X7 · Public technical overview — no award, certification, or production-readiness claimed

2 · REFERENCE DEPLOYMENT

The current reference deployment runs the PACP API and Assurance Gateway together through one local Docker workflow. Authenticated health checks bind to loopback interfaces. Runtime state is temporary unless the operator explicitly configures durable storage.

3 · BOUNDED ENFORCEMENT PATH

Gate	Question	Failure behavior
Storage integrity	Is the referenced state intact and available?	Refuse callback.
Anchor match	Does the supplied request match its declared evidence anchor?	Refuse callback.
Witness	Is the required witness evidence present and valid within the profile?	Refuse callback.
Authority binding	Is the actor bound to the declared authority and scope?	Refuse callback.
Information-flow policy	Does inherited lineage remain compatible with the requested public write?	Refuse callback.

OBJECTIVE 1 BOUNDARY

The five-gate claim applies to the declared lineage-scoped public-write path. It is not a claim that every possible action, integration, or deployment path is governed identically.

4 · PACP EVIDENCE MODEL

- Typed receipts distinguish action, observation, omission, verification, amendment, and repair evidence.
- Phase anchoring preserves the lifecycle context in which a claim acquired meaning.
- Canonical representation provides stable material for hashing and signatures.
- Previous-hash relationships make declared insertion, deletion, mutation, and reordering detectable.
- Proof bundles package the declared evidence needed for bounded replay outside the originating environment.

HACKETT META OS LLC

Andrew D. Hackett, Founder & Principal Inventor · andrew@hackettmetaos.com · hackettmetaos.com
SAM.gov Registered · UEI Z3XNP7JTYGL2 · CAGE 1A7X7 · Public technical overview — no award, certification, or production-readiness claimed

5 · AUTHORITY AND NON-TRANSITIVITY

Cryptographic validity, signer standing, local trust, proof acceptance, operational acceptance, and closeout are different claims. One does not automatically confer the next. A valid replay finding returns as evidence, not command authority.

6 · OMISSION EVIDENCE

An absence becomes evidence only against a prior registered expectation. A **NullReceipt** records bounded non-satisfaction within a declared scope or interval. It does not establish cause, blame, suppression, or a synthetic substitute for the missing artifact.

7 · COMPOSITION RESISTANCE

For the declared Objective 1 path, delegation and composition cannot discard inherited confidential exposure to manufacture a public-write authorization. The implementation retains lineage relevant to the configured information-flow decision.

8 · VERIFICATION AND FLAGSHIP CASE

The public verifier checks proof bundles entirely in the browser. The public Decision Evidence Lab lets a reviewer replay a synthetic consequential decision and attack the record by altering evidence, removing an omission receipt, or substituting identity. The repository flagship AI-change case independently exercises deterministic packet construction, nested input binding, reviewer findings, transition refusal, and tamper detection.

9 · THREAT-ORIENTED EVALUATION

Attack lane	Required evaluator question
Tamper	Can one byte change without detection, and which relationship identifies the break?
Omit	Can required evidence disappear, and was its expectation registered beforehand?
Substitute	Can a signer, policy, input, key, or verifier be exchanged without identity changing?
Reorder	Can phase or receipt order change without invalidating continuity?
Authority escalation	Can a valid artifact exercise authority it never possessed?
Composition	Can delegated or combined lineage erase inherited restriction?
Amend	Can correction occur without erasing the original?

10 · INTEGRATION CONTRACT

- Existing identity, access-control, policy, mission, safety, and enforcement systems remain responsible for their operational functions.
- HMOS receives declared inputs and constraints, applies the configured constitutional boundary, and emits bounded outcomes and evidence.
- Domain profiles must name observations, effects, commands, authority, expectations, persistent consequences, evidence sources, and unknowns.
- Unknown or unestablished properties remain explicit; Constitutional Autodiscovery must not invent interfaces or authority.

11 · SECURITY AND OPERATIONAL BOUNDARY

The current implementation is a working reference for evaluation. It has not been independently audited, penetration-tested, cryptographically reviewed, certified, accredited, or production-authorized. Operational deployment requires separate assessment against the actual mission, safety, security, and regulatory boundary in scope.

12 · PUBLIC EVALUATION SEQUENCE

1. Run the synthetic Decision Evidence Lab.

HACKETT META OS LLC

Andrew D. Hackett, Founder & Principal Inventor · andrew@hackettmetaos.com · hackettmetaos.com

SAM.gov Registered · UEI Z3XNP7JTYGL2 · CAGE 1A7X7 · Public technical overview — no award, certification, or production-readiness claimed

2. Mutate, omit, reorder, and substitute evidence.
3. Inspect the exact failed invariant and bounded refusal.
4. Verify a proof bundle independently in the browser.
5. Review the technical architecture and repository evidence.
6. Define a controlled evaluation with explicit success criteria, failure cases, and known-limit reporting.

DECLARED MATURITY BOUNDARY

Working local reference implementation. Not independently audited, certified, accredited, highly available, cloud-operated, fielded, or production-authorized. Domain integration and operational use require separate evaluation against the actual mission, safety, security, and regulatory boundary.

Andrew D. Hackett

Founder & Principal Inventor, Hackett Meta OS LLC
andrew@hackettmetaos.com · hackettmetaos.com

*When systems shape reality,
the record must survive the systems.*

B O U N D E D · V E R I F I A B L E · I N D E P E N D E N T · A C C O U N T A B L E

HACKETT META OS LLC

Andrew D. Hackett, Founder & Principal Inventor · andrew@hackettmetaos.com · hackettmetaos.com
SAM.gov Registered · UEI Z3XNP7JTYGL2 · CAGE 1A7X7 · Public technical overview — no award, certification, or production-readiness claimed