WHITE PAPER

Replayable Evidence Infrastructure

A constitutional architecture for governing consequential effects and preserving challengeable decision evidence

VERSION 0.5 · 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

ABSTRACT

Logs preserve activity. They do not necessarily preserve the evidence required to reconstruct why a consequential action was reachable, whether its authority was valid, what information was missing, what changed afterward, or whether the action should have been refused before execution. Hackett Meta OS addresses both sides of that gap: a constitutional enforcement kernel governs a bounded action path, while PACP preserves the resulting decision evidence as a portable, challengeable object.

> **CENTRAL REQUIREMENT**
>
> **The system must preserve not only what it did, but why the effect was reachable, which authority permitted it, what evidence was expected, what remained unknown, and which invariant would force refusal.**

1 · THE CONSTITUTIONAL-SURFACE PROBLEM

As systems become more autonomous and compositional, their behavior is no longer explained by one model output or one application log. Authority, policy, information flow, delegation, expected observations, external assertions, and persistent effects interact across components. A credible assurance layer must represent those relationships without inventing certainty that the evidence does not support.

2 · KERNEL, PROFILE, APPLICATION

The constitutional enforcement kernel carries invariant rules. Mission profiles map domain-specific interfaces, observations, effects, authority, and evidence into that core. Applications request bounded actions but do not redefine or bypass the kernel.

3 · PACP

The Phase-Anchored Consensus Protocol organizes evidence according to the phase in which a claim acquired meaning. Assertion, observation, verification, amendment, acceptance, and closeout remain distinct. Later confidence does not overwrite earlier uncertainty.

4 · EVIDENCE BEFORE EXPLANATION

Narrative explanations are useful only after the evidentiary boundary is preserved. PACP first captures the declared request, inputs, context, authority, expectations, omissions, constraints, and results. Explanations can then point to that record rather than replace it.

5 · OMISSION PHYSICS

Absence is meaningful only against a prior expectation. The architecture therefore separates registration of an expected artifact from later observation that it did not appear. A **NullReceipt** records non-satisfaction; it does not establish why the artifact is missing or authorize a substitute.

6 · NON-TRANSITIVE AUTHORITY

A valid signature establishes a narrow integrity claim. It does not by itself establish real-world authority, local trust, operational acceptance, or factual truth. Each transition requires its own evidence and governing authority. This prevents a remotely verified artifact from silently becoming a command.

7 · GOVERNING EFFECTS BEFORE EXECUTION

Replay after the fact is necessary but insufficient. The constitutional kernel evaluates the bounded action path *before* the consequential callback executes. In the current Objective 1 path, storage integrity, anchor match, witness, authority binding, and information-flow policy must all pass. **A failed gate produces refusal rather than a best-effort warning.**

8 · COMPOSITION AND INHERITED EXPOSURE

Delegation can create a laundering problem: a component with restricted lineage passes a result through another component that appears less restricted. The bounded implementation retains inherited exposure relevant to its declared public-write policy so composition cannot silently erase the restriction.

9 · CONSTITUTIONAL AUTODISCOVERY

A future compiler can ingest machine-readable interface descriptions, standards, schemas, policies, and telemetry definitions to construct a candidate constitutional profile. The output must remain bounded: known interfaces, possible effects, authority requirements, evidence expectations, and explicit unknowns. Autodiscovery must refuse to invent semantics or authority that the source material does not establish.

10 · ADVERSARIAL-EFFECT ENVELOPES

Design-intent descriptions explain what a system is supposed to do. Threat corpora explain what an adversary may make it do. Combining interface/effect models with threat knowledge enables a richer constitutional surface: intended effects, adversarially reachable effects, required evidence, and refusal conditions can be evaluated together without claiming exhaustive threat coverage.

11 · INDEPENDENT VERIFICATION

A proof bundle should be inspectable in an environment that inherits no credentials, operational authority, or institutional memory from the producer. The verifier emits a bounded finding about the supplied bundle and declared checks. It does not certify the originating system or decide whether an action was correct.

12 · EVALUATION METHOD

1. Declare the exact claim and implementation boundary.
2. Construct representative success and refusal cases.
3. Attack tamper, omission, substitution, reordering, authority escalation, composition, and amendment behavior.
4. Replay outside the producer environment.
5. Record known limits, unresolved findings, and evidence gaps without converting them into success.

13 · CROSS-DOMAIN RELEVANCE

The architecture is domain-independent; the profiles are not. Defense, healthcare, cybersecurity, aerospace, logistics, critical infrastructure, and regulated research each require their own authority models, standards, effects, evidence, and evaluation criteria. Cross-domain applicability is a research and product strategy, not a claim that one profile already governs every domain.

14 · CURRENT IMPLEMENTATION AND LIMITS

The current reference implementation runs a bounded PACP API and Assurance Gateway together in one local Docker workflow. Objective 1 governs a five-gate public-write path. Proof bundles, typed receipts, omission evidence, and browser-based verification are operational. The implementation is not independently audited, certified, accredited, cloud-operated, or production-authorized. External evaluation, integration studies, and formal assurance work remain ahead.

CONCLUSION

Accountability is not a dashboard produced after the event. It is an architectural property: consequential effects pass through explicit authority and evidence rules, refusal remains possible, history is not silently rewritten, unknowns remain visible, and the resulting record can survive challenge outside the system that created it.

> **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.

BOUNDED · VERIFIABLE · INDEPENDENT · ACCOUNTABLE