Network Working Group
Internet-Draft
Intended status: Informational
Expires: 17 November 2026

F. B.
Independent Researcher

16 May 2026

External Admission Boundary for Pre-Execution AI Action Control
draft-b-external-admission-boundary-00

Abstract

This document defines an external admission boundary for pre-execution AI action control. The boundary is a control point at which execution cannot proceed unless an allow decision has been issued by an authority outside the executor trust domain. The document distinguishes evidence records, policy evaluations, approval logs, and signed pre-execution authorization records from the stronger boundary property of authority separation.

A signed pre-execution record can prove that a decision was made before dispatch. It does not by itself prove that final execution authority was outside the executor trust domain. This document provides a practical test for determining whether a claimed pre-execution control is a real external admission boundary or a surrogate boundary.

1. Introduction

AI agents, CI/CD workflows, automated remediation systems, tool-calling models, and other execution-capable systems increasingly act before a human can inspect every material step. In such environments, review, monitoring, audit logging, rollback, and post-execution evidence are useful but insufficient to answer the boundary question: who has final authority before execution begins?

This document defines an external admission boundary. The boundary exists when execution depends on an allow decision issued outside the executor trust domain, denial fails closed, and the executor cannot proceed, bypass, rewrite, or self-issue the admission path.

The central rule is: No admission = no execution.

1.1. Scope

This document specifies boundary conditions and verifier expectations for pre-execution AI action control. It does not specify a policy language, a runtime gateway, a transport protocol, a transparency log, a cryptographic envelope, or a particular storage format.

This document is intended to compose with signed authorization records, transparency systems, policy engines, runtime identity systems, and execution-boundary cryptographic mechanisms. It defines the boundary test those mechanisms must satisfy if they are to be treated as external admission rather than internal evidence.

1.2. Relationship to Pre-Execution Records

Pre-execution records are evidence. External admission boundaries are authority separation.

A signed authorization record, permit, receipt, or request-dispatch binding can prove that a decision was recorded. Such a record does not by itself prove that execution was unable to proceed without an external allow decision. If the executor can self-approve, bypass, overwrite, or self-issue the admission path, the resulting control is a surrogate boundary even if the record is cryptographically strong.

2. Terminology

Executor:
: The system, workflow, agent, runtime, platform, or tool environment capable of carrying out the action.

Admission Authority:
: The authority that issues an allow, deny, or equivalent admission decision before execution.

External Admission Boundary:
: A pre-execution control boundary where execution depends on an allow decision from an authority outside the executor trust domain.

Surrogate Boundary:
: A claimed boundary that appears to control execution but remains inside the executor trust domain or can be bypassed, rewritten, self-approved, or self-issued by the executor.

Admission Record:
: Evidence that an admission decision was made. An admission record is not itself sufficient to establish an external admission boundary.

3. Boundary Requirements

A claimed external admission boundary MUST satisfy all of the following:

1. Execution MUST require an allow decision before the action begins.

2. The allow decision MUST be issued outside the executor trust domain.

3. Denial, timeout, missing evidence, invalid response, or unavailable admission authority MUST fail closed.

4. The executor MUST NOT be able to approve, bypass, overwrite, forge, or self-issue its own admission path.

5. The admission decision MUST exist before execution and MUST be

bound to the action that is executed.

6. A verifier MUST be able to distinguish admitted execution from non-admitted execution.

4. The Surrogate Boundary Test

A verifier SHOULD ask the following questions:

1. Can execution proceed without an external allow decision?

2. Can the executor approve, bypass, overwrite, or self-issue the admission path?

3. Is the admission record created before execution?

4. Does denial, timeout, missing evidence, invalid response, or missing authority fail closed?

5. Is final authority outside the executor trust domain?

If the answer to question 1 or 2 is yes, the boundary is surrogate. If the answer to question 4 is no, the boundary is fail-open. If final authority remains inside the executor trust domain, the mechanism may be useful policy or evidence, but it is not an external admission boundary.

5. Non-Boundaries

The following mechanisms are not sufficient by themselves:

* Internal policy inside the same runner, workflow, model gateway, or platform trust domain.

* Mutable approval flags controlled by the execution environment.

* Human approval that can be routed around by the executor.

* Monitoring, audit logs, dashboards, and rollback.

* Policy-as-code that the same trust domain can change or skip.

* Signed pre-execution records that are issued, bypassed, or rewritten by the executor trust domain.

6. Composition with Evidence Records

Evidence records are valuable. A deployment MAY use signed statements, transparency receipts, request-dispatch bindings, policy evaluation results, or closure records to prove what was authorized and what was executed.

Such records strengthen verification only when the execution path also enforces the external boundary. The record proves the evidence layer. The boundary proves that execution authority was separated.

7. Security Considerations

A deployment that records admission decisions but permits the executor to continue when the admission authority is unavailable is fail-open.

A deployment that allows the executor to rewrite or bypass admission evidence after a decision is made does not provide an external boundary.

A deployment that places policy evaluation and final execution authority inside the same trust domain may reduce risk but does not separate final

execution authority from the executor.

8. Privacy Considerations

This document does not require raw prompts, raw provider responses, credentials, personal data, or sensitive operational content to be exposed. Implementations that create admission evidence SHOULD minimize logged identifiers and SHOULD avoid placing secrets or raw sensitive content into public records.

9. IANA Considerations

This document makes no IANA requests.

10. References

[SCITT] IETF SCITT Working Group, Supply Chain Integrity, Transparency, and Trust architecture work in progress.

[KEYWORDS] RFC 2119 and RFC 8174 define requirement keywords.

Appendix A. Summary

Pre-execution records are evidence.
External admission boundaries are authority separation.
No admission = no execution.

Author Address

Felix B.
Independent Researcher
URI: https://ai-admissibility.com/