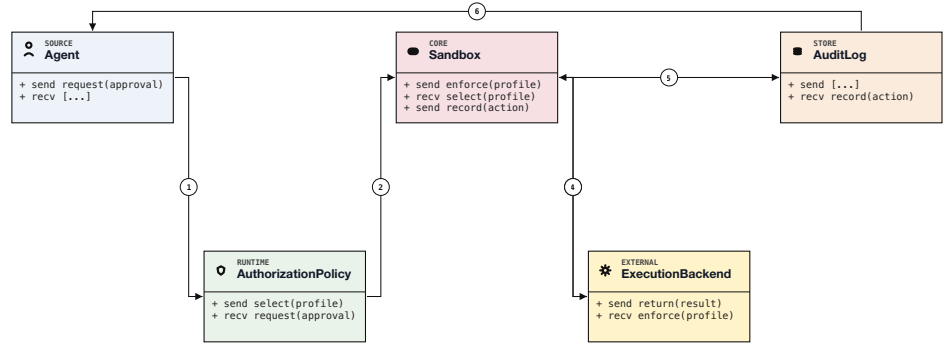
P23 Layered permission and sandbox

Primitive · A² A2 · layered role collaboration

Combine policy decisions with execution isolation.

STRUCTURE · PARTICIPANT COLLABORATION



PATTERN INTERFACE

context
A tool action is evaluated by policy and executed in a controlled environment.

trigger
A privileged operation or command is dispatched.

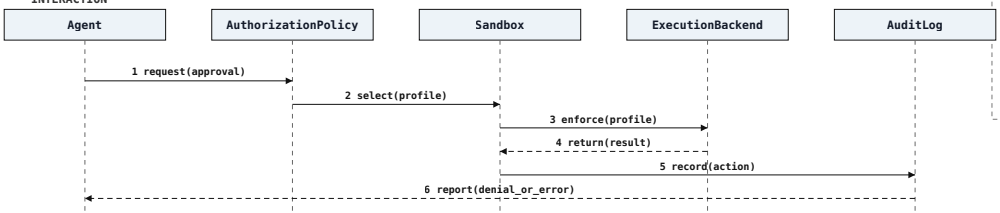
structure
Authorization decision, sandbox profile, environment adapter, and enforcement point.

effect
The effective capability equals the authorized capability, including filesystem and network.

CONTRACT ANNOTATIONS

requires	Requested operation and active environment policy are both observable.
ensures	Any difference between approval and enforcement fails closed or asks for escalation.
invariant	A policy decision cannot be bypassed by switching sandbox or transport backend.
violation	Enforcement errors deny execution and preserve actionable diagnostics.

INTERACTION



MESSAGE TRACE `1 request(approval) → 2 select(profile) → 3 enforce(profile) → 4 return(result) → 5 record(action) → 6 report(denial_or_error)`

Evidence: 40/41 repositories, 36/36 families; 40 trajectories (19 multi-checkpoint); exact audit: not sampled.

Variation: OS sandbox, container, mount policy, network rules, and approval mode.

Negative control: A prompt warning without execution enforcement is not a sandbox.