OPENAI ARCHITECTURE PRIMER

Whose Authority Is the Agent Using?

Principal, workload, mandate, delegated scope, and evidence

A visual guide to the identities, credentials, task constraints, and delegation records behind agent action.

NIST TENETS / OPENAI BEHAVIOR / LUMINITY SYNTHESIS



Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

Agent Identity and Authority · Primer 01

Sources verified Nov 5, 2026 · local review draft

OpenAI Select Partner

Authority is assembled across several control objects

The chain connects identity, authentication, task purpose, delegated scope, and execution evidence without treating them as one credential.

AT A GLANCE

4
identity layers represented in one agent run

2
credential paths: API key or federation

1
mapped principal per Codex federation rule

60–3600
seconds in the documented federated-token range

TWO DISTINCTIONS PREVENT FALSE AUTHORITY

Credential versus authority

An API key or token authenticates a request path. It does not prove the initiating principal, approved task, or delegation lineage.

Attribution versus authorization

Agent, session, run, and subagent identifiers help correlate activity. They do not independently authorize the action.

DOCUMENTED BOUNDARY

The reviewed OpenAI sources do not document an automatic cryptographic chain from a human principal through every agent, subagent, tool, and connected service.

THREE CHAPTERS

01 **Identity layers**

Separate authority origin, workload authentication, platform principal, and execution identity.

02 **Authentication path**

Trace the external issuer, federation rule, mapped principal, token, and effective roles.

03 **Delegated intent**

Bind purpose and constraints to each handoff, then preserve or narrow scope.

NIST frames the target state. OpenAI documents current primitives. Luminity supplies the cross-system binding model.

© 2026 Luminity Digital, Inc. | Local review draft

NIST design tenets + OpenAI API keys, WIF, federation-rule, RBAC, and Agents API docs · verified Nov 5, 2026

OpenAI Select Partner

Agent identity chain

Each object answers a different control question. The chain fails when a credential or runtime identifier substitutes for the missing links.

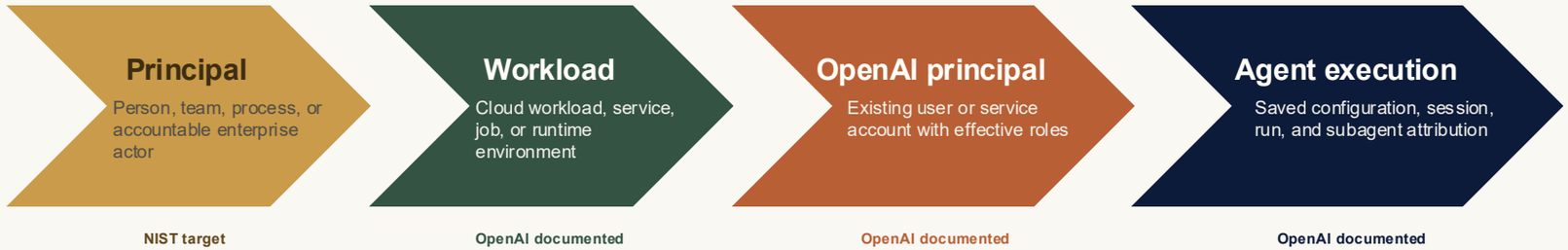
WHAT EACH OBJECT ESTABLISHES

Initiating principal	AUTHORITY ORIGIN
Enterprise workload	AUTHENTICATING RUNTIME
Mapped OpenAI principal	PLATFORM ACCESS
Agent, session, subagent IDs	ATTRIBUTION + STATE
Approved mandate	PURPOSE + CONSTRAINTS

Agent identity record

Proposed binding among owner, workload, configuration version, deployment, tools, lifecycle state, and evidence identifiers.

IDENTITY PATH



CONTROL OBJECTS THAT REMAIN SEPARATE

Credential

API key or short-lived token accepted by an authentication boundary.

Mandate

Approved outcome, limits, audience, duration, and delegation conditions.

Authorization

Current decision that a principal may perform an action on a resource.

Evidence

Identity, decisions, calls, outcomes, denials, and revocation records.

DO NOT COLLAPSE API key ≠ service account ≠ agent ID ≠ session ID ≠ mandate ≠ authorization decision ≠ evidence record

© 2026 Luminity Digital, Inc. | Local review draft

NIST tenets 01, 02 and 06 + OpenAI API keys, RBAC, Agents API configuration and sessions · verified Nov 5, 2026

OpenAI Select Partner

Workload authentication and delegated intent

Federation maps an external workload identity to platform access. Enterprise controls must still bind the human origin, mandate, agent execution, and downstream authorization.

WHAT THE PATH ESTABLISHES

External workload verified	DOCUMENTED
Existing OpenAI principal mapped	DOCUMENTED
Token scope and lifetime bounded	DOCUMENTED
Human task origin proven	NOT ESTABLISHED
Subagent authority attenuated	NOT AUTOMATIC

Mandate binding

Enterprise-owned linkage among the accountable principal, task constraints, approved configuration, expiry, delegation rule, and evidence identifier.

HOSTED AUTHENTICATION PATH

External issuer
OIDC token or supported cloud workload identity

Federation rule
Issuer, identity checks, allowed scopes, target principal, lifetime

Mapped principal
Existing OpenAI user or service account

Short-lived token
Credential used for API access within effective roles

CONTROL SURFACES AROUND THE TOKEN

Effective roles

Organization and project assignments combine to determine platform access.

Agent configuration

Instructions, model, tools, and defaults copied into a session and subject to overrides.

Run attribution

Session and subagent identifiers correlate state, delegation, commands, and outcomes.

Tool authorization

MCP servers and connected applications remain responsible for their own authorization.

AUTHENTICATION LIMIT

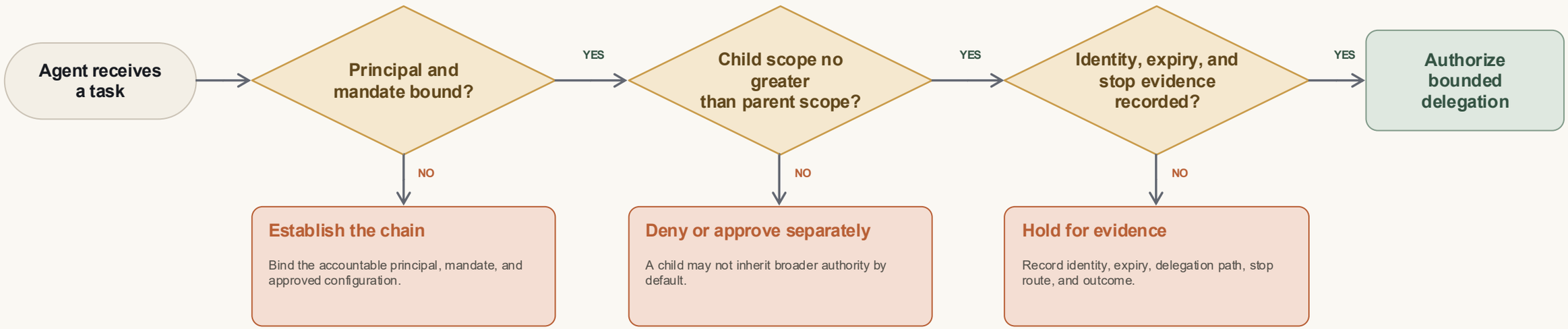
A valid token does not prove the initiating human, approved mandate, automatic scope attenuation, or authorization inside a connected service

© 2026 Luminity Digital, Inc. | Local review draft

OpenAI WIF, federation rules, RBAC, Agents API sessions and multi-agent, and MCP authentication docs · verified Nov 5, 2026

Delegated authority decision

A handoff is bounded only when the accountable origin, mandate, child scope, expiry, and evidence remain reconstructable.



REQUIRED OVERLAYS

Owner and workload

Accountable principal, runtime identity, mapped platform principal.

Configuration version

Saved agent, environment, instructions, model, tools, and overrides.

Tools and resources

Permitted actions, audiences, data boundaries, and downstream checks.

Evidence and stop path

Delegation record, approvals, calls, outcomes, expiry, revocation, and cancellation.

ARCHITECTURE RULE — **No delegation hop expands authority by default.**

OPENAI BOUNDARY — Subagent identity and inherited capabilities are documented; automatic attenuation and signed mandates are not.

© 2026 Luminity Digital, Inc. | Local review draft

NIST delegation and mandate tenets + OpenAI Agents API multi-agent and MCP documentation · verified Nov 5, 2026

OpenAI Select Partner