IETF Hackathon
AOA

IETF 125
14–15 March 2026
Shenzhen, China

Champions
Dapeng Liu
Suresh Krishnan
Fan Yang

AOA

➢ Agent Operation Authentication

- Draft: https://datatracker.ietf.org/doc/html/draft-liu-agent-operation-authorization-01

➢Repository

- https://github.com/alibaba/open-agent-auth

Problem Statement & Design Goals

Current OAuth Limitations in AI Agent Context:

1. Permission ≠ Behavior (The Injection Risk)

- **Current OAuth**: Grants broad Permissions (e.g., scope=write).
- **The Risk**: Since LLMs struggle to distinguish **Data vs. Instruction**, a **Prompt Injection** can trick the Agent into executing malicious actions that are still technically within the granted Permission.
- **Gap**: A mechanism to **bind specific behavioral policies** with OAuth authorization.

2. The Agent Delegation Challenge (Intent Decoupling)

- **Hallucination in Parsing intent:** The Agent may misinterpret the user's natural language intent.
- **Missing Contextual Binding:** Current OAuth proves who the user is, but not **which Agent is acting which user and what specific task** was authorized.
- **Gap:** Lack a cryptographic link for "Agent X acting for User Y to do Task Z".

Design Goals: Bind behavioral Policy +Agent Delegation + User Intent Evidence

Solution: Agent Operation Authorization (AOA)

AOA Solution: Policy-Based Authorization with AS-signed evidence binding **User + Agent + Operation**

The agent_operation_proposal Mechanism (PAR)

Core Concept:

- *A structured, machine-readable proposal generated by the Agent, serving as the **binding contract** between User, Agent, and Operation.*

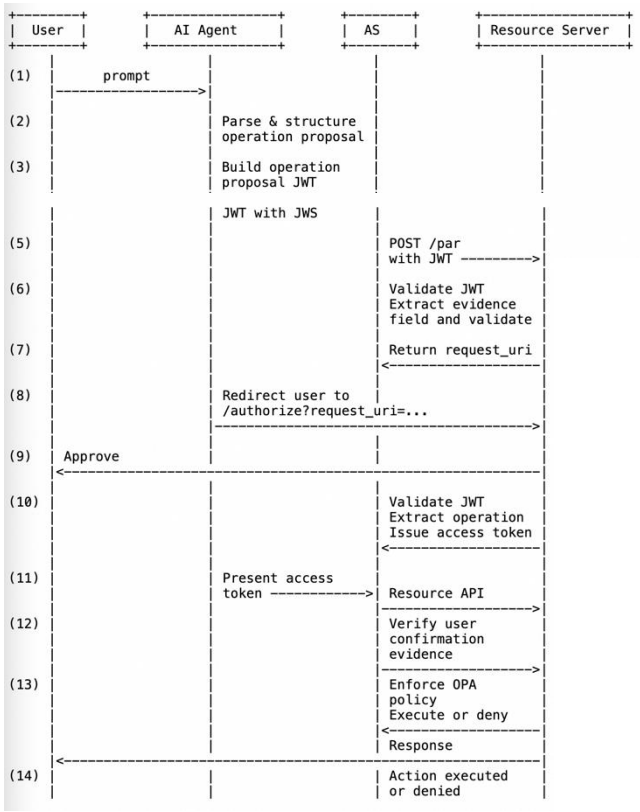
1. Explicit Tripartite Binding (The "Who-What-Which" Gap Solved)

AOA explicitly cryptographically binds three elements:

- ✓ **Which User**: Identifies the Resource Owner (user identity).
- ✓ **Which Agent**: Identifies the specific Agent instance (agent identity).
- ✓ **What Specific Behavior**: Defines the exact operation policy constraints (e.g., amount <= 50, time == ”Nov. 11 night").

Agent → [Structured Proposal] → AS validates User + Agent + Intent + Policy → Signed Token → RS → [Enforces Policy]

Workflow & Native Multi-Agent Support



(1) User says: “Add something cheap to cart on Nov 11 night”

(2) AI Agent parses intent → builds operation proposal object

(3) Agent creates operation proposal JWT

(4) Agent creates JWT with operation proposal claim, signs with JWS

(5) Agent sends JWT to AS via PAR: POST /par { "request": "<jwt>" }

(6) AS validates JWS, extracts evidence field and validate

(7) AS issues request_uri to agent

(8) Agent redirects user to /authorize?request_uri=...

(9) User reviews the displayed operation and confirms the authorization

(10) AS register the policy and issues Agent Operation Authorization Token as access token which includes the policy_id

(11) Agent uses token to access Resource Server

(12) AS verifies user confirmation evidence

(13) RS enforces OPA policy

(14) Action executed or denied

Sessions

New Session

i want to buy some programmi...
1m ago

Open Agent Auth Chat
Intelligent Assistant - Always at Your Service

i want to buy some programming books, can you give me some advices?

2026-03-15 12:20:24

I'd be happy to help you find programming books! Let me search for some options for you.

2026-03-15 12:20:28

I've found a programming book that might interest you:

- **Java Programming Guide** - A comprehensive Java tutorial priced at $89.00 (Product ID: PROD-009)

Would you like more specific programming books on a particular language or topic? I can search for additional options if you're looking for something different.

12:21:51

Clear

Type your message...

Send

Tool Calls

search_products SUCCESS

SERVER

shopping

ARGUMENTS

"{\"keywords\":\"programming\",\"category\":\"books\"}"

1m ago

search_products INITIATED

search_products AUTHORIZED

AO

Authorization

Agent Operation Access

APPLICATION REQUEST

Client ID

wimse://default.trust.domain/workload/dfa7a470-a7b5-4a00-a591-d2ac8a35ab14

User

user_admin_001

Permissions

openid profile

Verify Origin

Confirm you recognize this application before proceeding.

© 2025 Agent Operation Authorization

Operation Authorization Details

Review the agent operation details before approving

Operation Policy

Search for programming books in the shopping resource. The agent can only search for products in the books category with programming keywords.

Interpretation: medium

Raw Policy (Rego)

```
package agent
allow {
  input.operationType == "search_products"
  input.resourceId == "shopping"
  # Additional context constraints
  input.context.category == "books"
  input.context.keywords == "programming"
}
```

By approving, the agent may act on your behalf within the scope described above. You can revoke this authorization at any time.

Deny

Approve

AO

Authorization

Agent Operation Access

APPLICATION REQUEST

Client ID

wimse://default.trust.domain/workload/dfa7a470-a7b5-4a00-a591-d2ac8a35ab14

User

user_admin_001

Permissions

openid profile

Verify Origin

Confirm you recognize this application before proceeding.

© 2025 Agent Operation Authorization

Operation Authorization Details

Review the agent operation details before approving

Channel web | Lang zh-CN | User user_agent_001 | Agent sample-device | Platform sample-agent.platform

Client sample-agent-client | Device sample-device

Identity Binding

User Identity Token

Agent Workload Token

Device sample-device

Request Metadata

Issuer	http://localhost:8081
Subject	user_agent_001
Request ID	34b02d31-6e81-4f29-915d-4e19aae06e4a

By approving, the agent may act on your behalf within the scope described above. You can revoke this authorization at any time.

Deny

Approve

Thanks!