MCP Dev Summit Mumbai

Who's Calling?

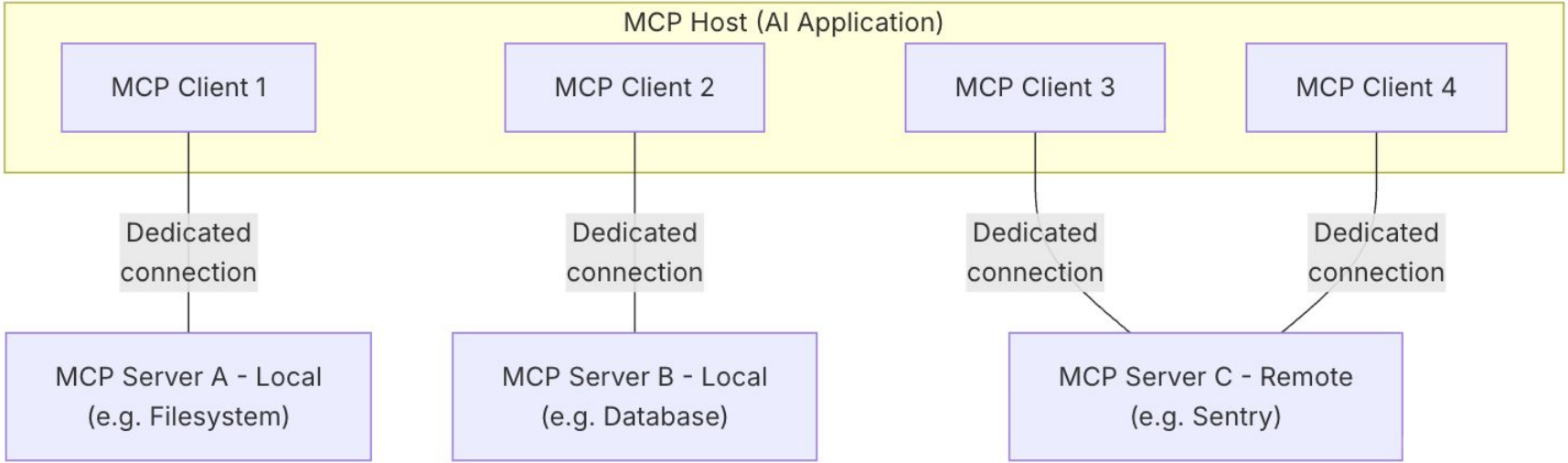
Bringing Identity to MCP Host

Ayesha Dissanayaka

Associate Director / Architect

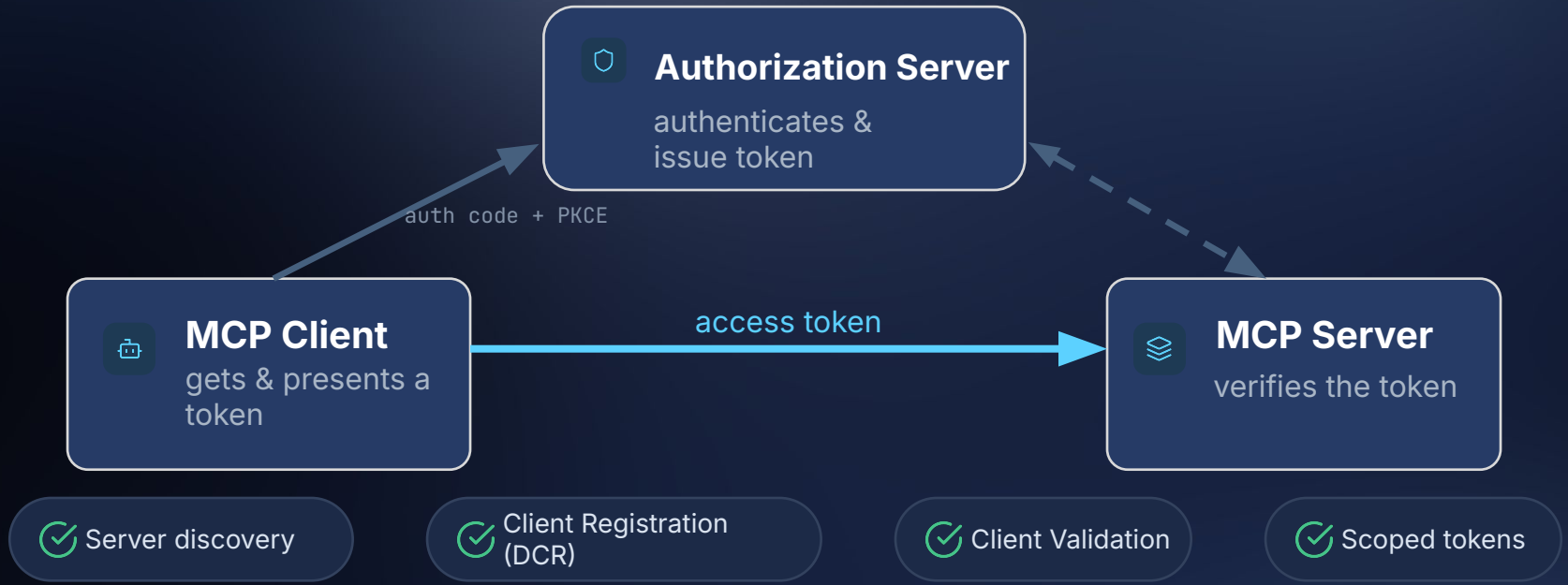
WSO2

MCP Architecture



https://modelcontextprotocol.io/docs/learn/architecture

Where spec focus - A clean OAuth 2.1 story



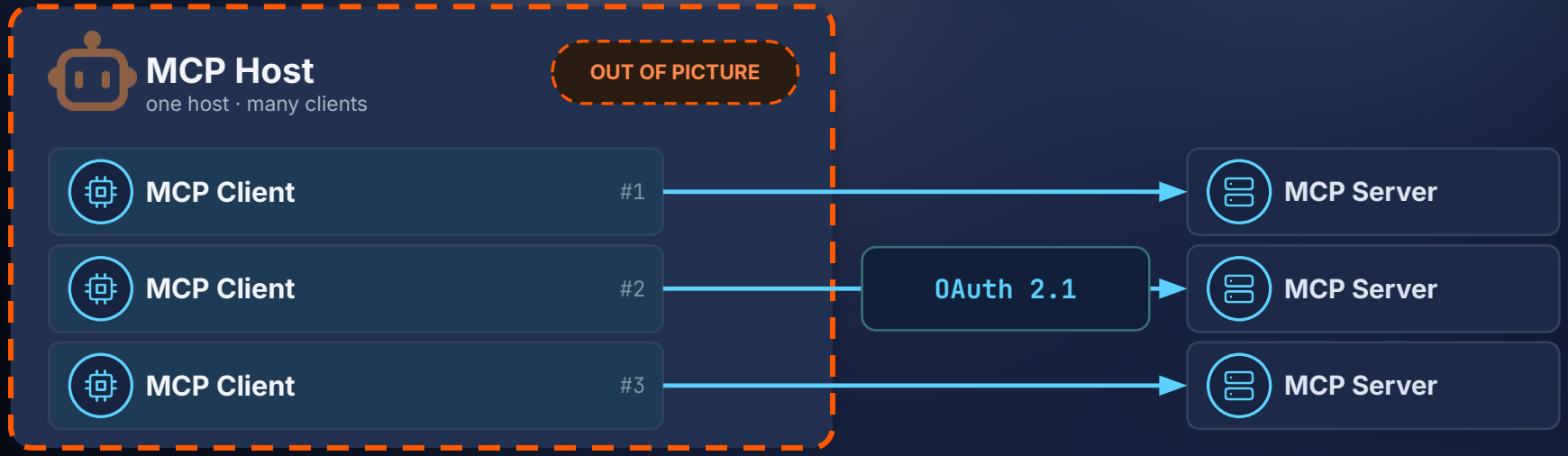
For the client–server edge, this is genuinely solved. Now notice what's in this picture — and what isn't.

Where spec focus today

- Server discovery
- Client Registration (DCR)
- Client Validation
- Scoped tokens

For the client–server edge, this is genuinely solved. Now notice what's in this picture — and what isn't.

The host is the control center



That’s where enterprise deployments quietly break.

The agents enterprises will build

Same MCP plumbing — different functional modes, and very different access patterns.

ON USER'S BEHALF

ON ITS OWN PERMISSIONS

Delegated copilots

IDE coding copilot · IT-helpdesk assistant · CRM email drafting

Async assistants

Overnight inbox triage · 6am morning brief · auto-filed expenses

Shared service agents

Public support assistants · KB Q&A · procurement desk

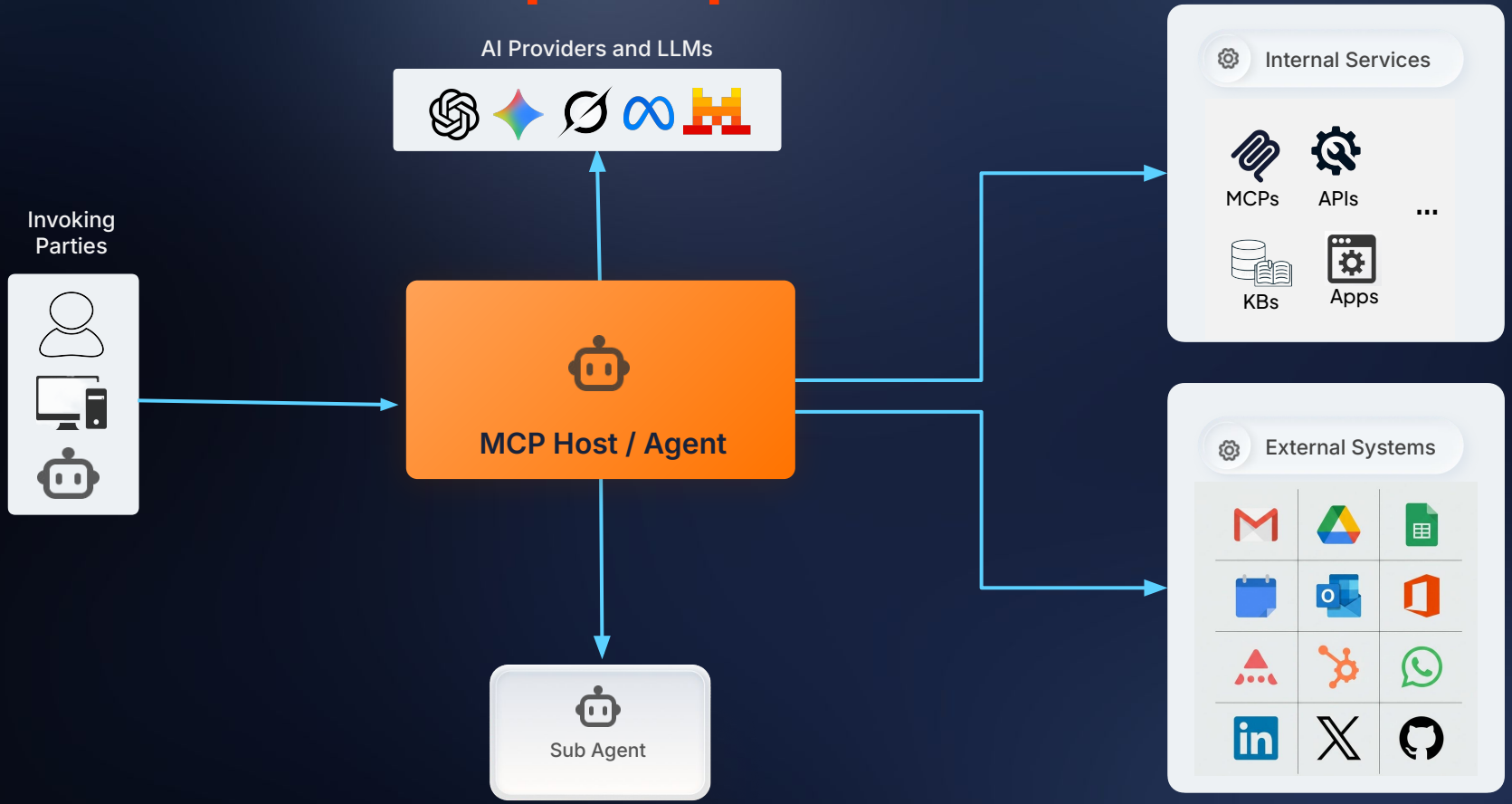
Autonomous workloads

SRE remediation · security response · ETL pipelines

INTERACTIVE
human in the loop

NON-INTERACTIVE
ambient · headless. autonomous

And it is an active principle



The agents enterprises will build

Same MCP plumbing — different functional modes, and very different access patterns.

ON USER'S BEHALF

ON ITS OWN PERMISSIONS

Delegated copilots

IDE coding copilot · IT-helpdesk assistant · CRM email drafting

Async assistants

Overnight inbox triage · 6am morning brief · auto-filed expenses

Shared service agents

Public support assistants · KB Q&A · procurement desk

Autonomous workloads

SRE remediation · security response · ETL pipelines

INTERACTIVE
human in the loop

NON-INTERACTIVE
scheduled · autonomous

The security many starts with: Long-Lived API Keys

What Teams Do

1. Generate a personal access token, or get a API key
2. Grant the broadest scopes "to be safe"
3. Set expiry to 1 year (or never)
4. Paste it into an env variable

The Risk

- Massively over-privileged
- Long-lived — a standing liability
- No per-action audit trail
- Violates principle of least privilege

Your Agent X

An ordinary enterprise AI agent — the one you shipped last quarter, or the one you're about to.

01. Do you even exist?

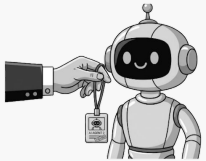
02. Who do we know it’s you?

03. What are you allowed to do?

04. Can you prove what you did?

The Four A's : The Pillars of Agent Identity to address AI Agent Challenges

ADMINISTER



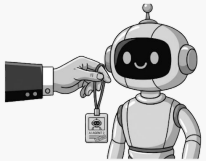
AUTHENTICATE

AUTHORIZE

AUDIT

The Four A's : The Pillars of Agent Identity to address AI Agent Challenges

ADMINISTER



Define and manage agent identities

- Registration
- Lifecycle
- Deprovision
- Ownership
- Suspension
- Visibility

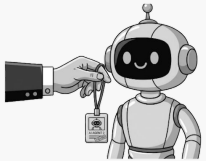
AUTHENTICATE

AUTHORIZE

AUDIT

The Four A's : The Pillars of Agent Identity to address AI Agent Challenges

ADMINISTER



Define and manage agent identities

- Registration
- Lifecycle
- Deprovision
- Ownership
- Suspension
- Visibility

AUTHENTICATE

Secure credentials for agent access

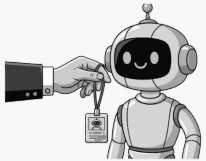
- Attestation
- Zero-trust
- Short Lived tokens
- Credential Rotation, Revocation
- WID integrations

AUTHORIZE

AUDIT

The Four A's : The Pillars of Agent Identity to address AI Agent Challenges

ADMINISTER



Define and manage agent identities

- Registration
- Lifecycle
- Deprovision
- Ownership
- Suspension
- Visibility

AUTHENTICATE

Secure credentials for agent access

- Attestation
- Zero-trust
- Short Lived tokens
- Credential Rotation, Revocation
- WID integrations

AUTHORIZE

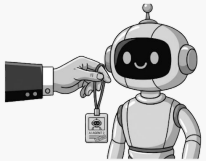
Enforce policies for agent actions and tool access

- Least privilege
- Just-in-Time
- Tool level grain
- Autonomous vs. H-I-L approval
- Delegation / on-behalf-of

AUDIT

The Four A's : The Pillars of Agent Identity to address AI Agent Challenges

ADMINISTER



Define and manage agent identities

- Registration
- Lifecycle
- Deprovision
- Ownership
- Suspension
- Visibility

AUTHENTICATE

Secure credentials for agent access

- Attestation
- Zero-trust
- Short Lived tokens
- Credential Rotation, Revocation
- WID integrations

AUTHORIZE

Enforce policies for agent actions and tool access

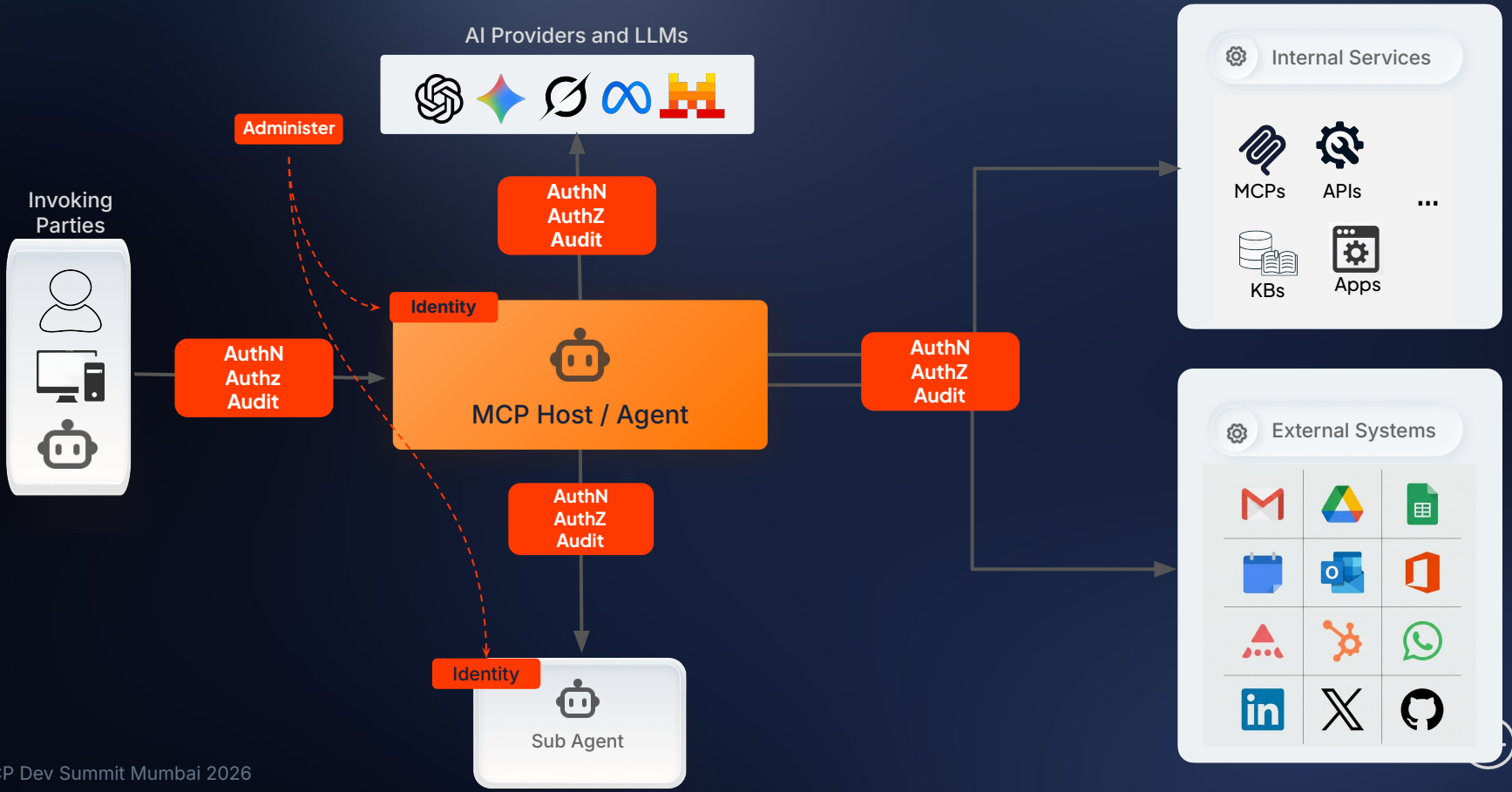
- Least privilege
- Just-in-Time
- Tool level grain
- Autonomous vs. H-I-L approval, on-behalf-of
- Delegation / chaining

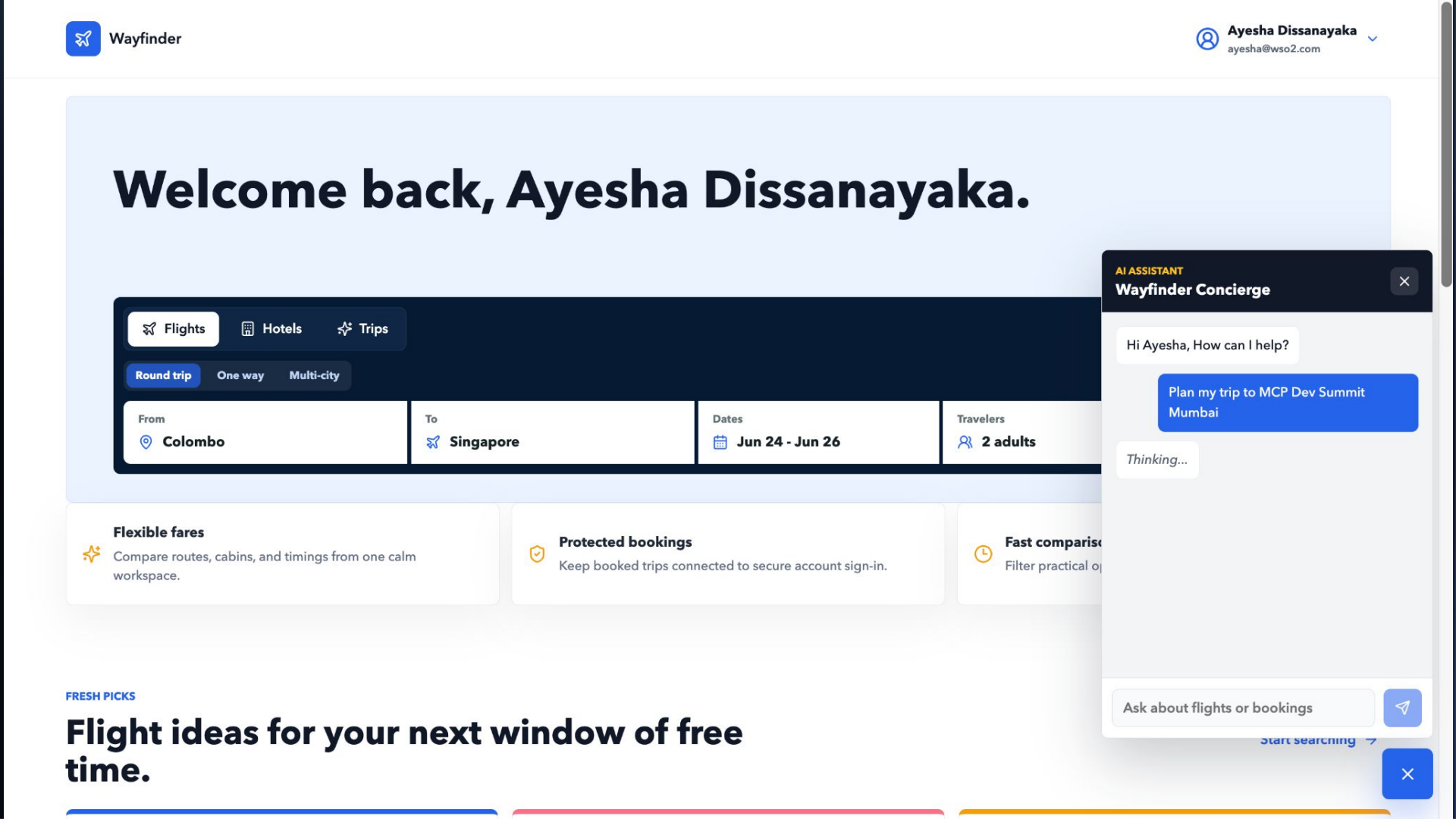
AUDIT

Enable tracking agent activity for accountability

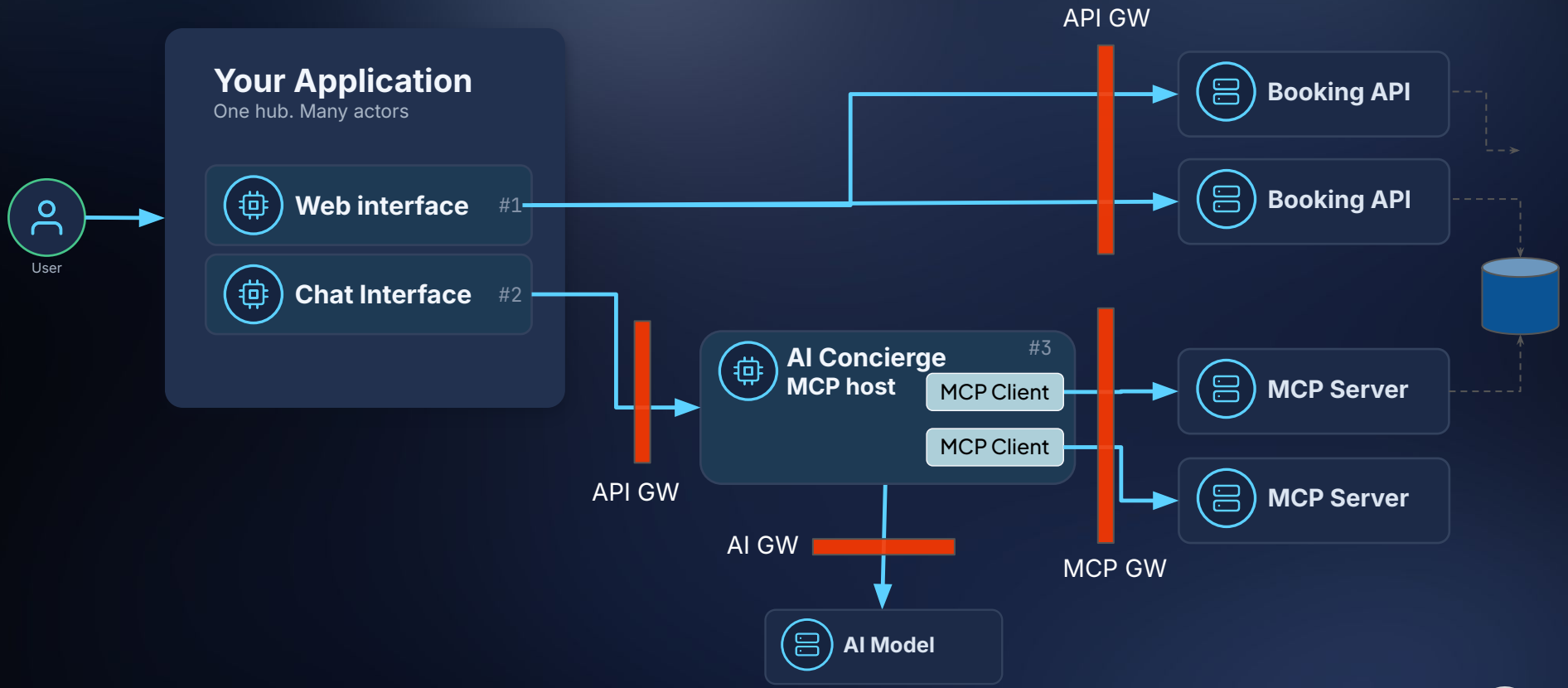
- Audit trail
- Compliance evidence
- Decision provenance
- Anomaly detection
- Forensic replay

Host ID enables the 4A's for each interaction




Wayfinder
Ayesha Dissanayaka
ayesha@wso2.com
Welcome back, Ayesha Dissanayaka.
Flights
Hotels
Trips
Round trip
One way
Multi-city
From
Colombo
To
Singapore
Dates
Jun 24 - Jun 26
Travelers
2 adults
Flexible fares
Compare routes, cabins, and timings from one calm workspace.
Protected bookings
Keep booked trips connected to secure account sign-in.
AI ASSISTANT
Wayfinder Concierge
Hi Ayesha, How can I help?
Plan my trip to MCP Dev Summit Mumbai
Thinking...
Ask about flights or bookings
FRESH PICKS
Flight ideas for your next window of free time.
Start searching

Real world scenario in enterprises



Delegation: On-Behalf-Of(OBO) Token

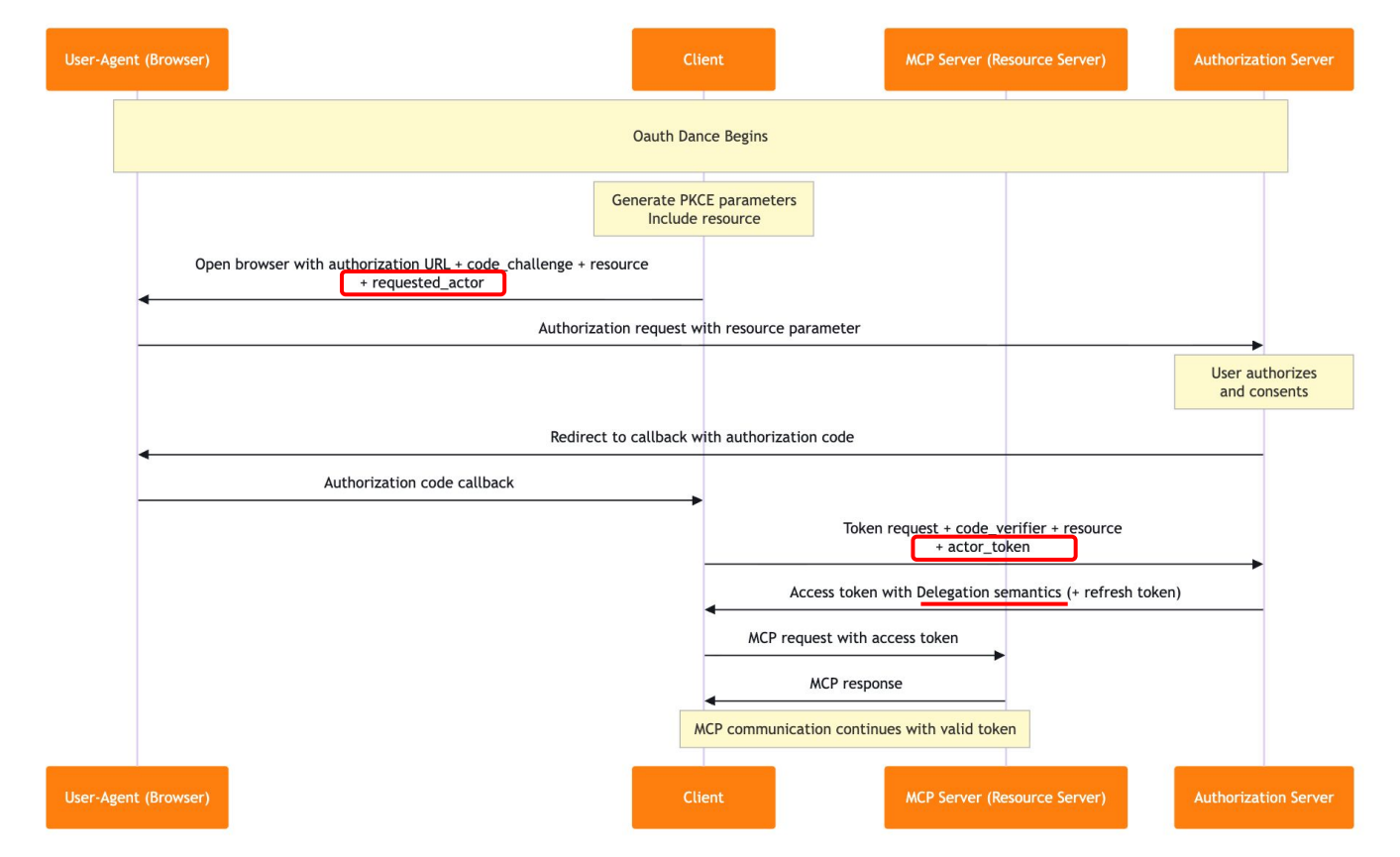
User/Subject Token

+

Agent/Actor Token

Exchange

User Consented OBO Token



https://datatracker.ietf.org/doc/draft-oauth-ai-agents-on-behalf-of-user/01/

Where the ecosystem is converging

OAuth Token Exchange

RFC 8693 + actor claims

Workload Identity

SPIFFE / SVID & attestation

On-Behalf-Of Flows

multi-hop agent chains

Back channel Auth

ambient . background . long running

MCP for Enterprise

extending the spec upward

Least Privilege

by default · scopes from the task

The building blocks exist — they're just not yet assembled into the MCP host story. Let's assemble them before ad-hoc workarounds calcify.

So - who’s calling?

Make the MCP host an identity you can name, scope, and hold accountable.

Thank you!

MCP Dev Summit Bengaluru

WSO2

https://www.linkedin.com/in/ayeshadissanayaka/

Ayesha Dissanayaka

Associate Director / Architect