



SEPT 22 - 24, 2026 | NAIROBI, KENYA

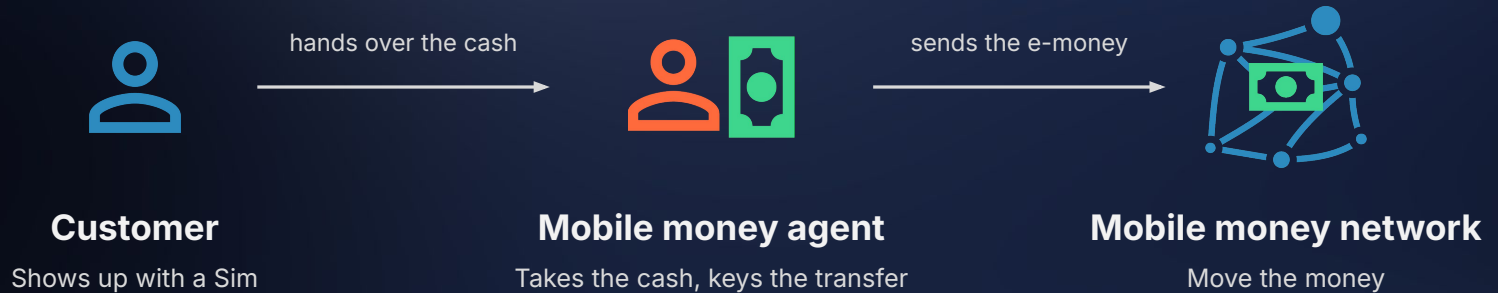
Identity, Delegation, and Access Governance for AI Agents



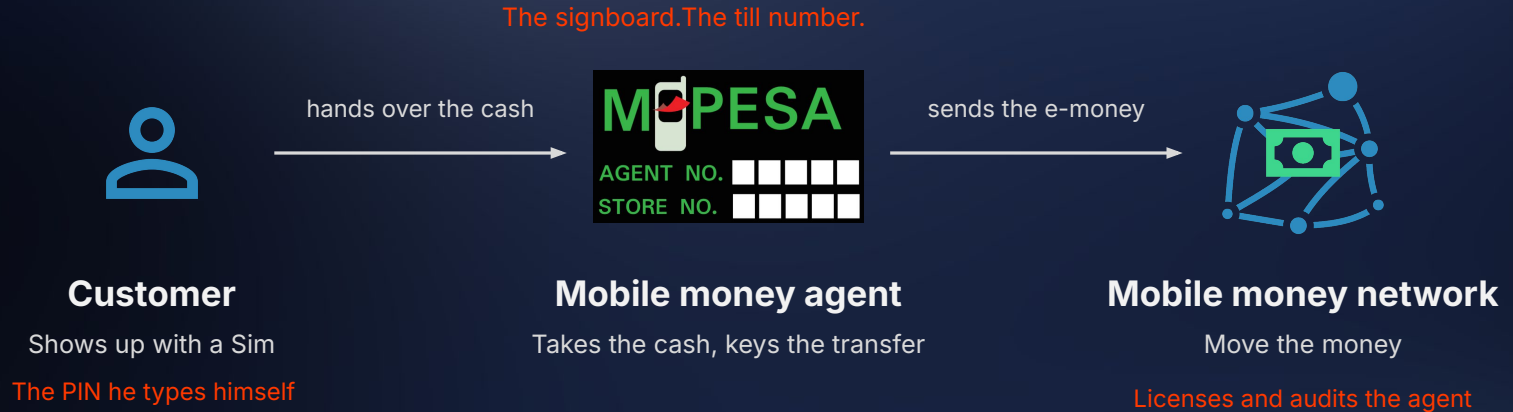
Ayesha Dissanayaka

Associate Director/ Architect
AAIF Ambassador

How Traditional Agent Networks Work



How Traditional Agent Networks Work



None of it is trust, all of it is infrastructure

Identity makes the handoff safe



Traditional IAM was built around **humans**, **Agents** are **not** humans. **Nor standard services.**



No Script

Goal-oriented rather than executing predefined, static steps.



Type vs. Instance

Spans dynamically across models, context, runtimes, and vendors.



Speed

Runs on megahertz.
Rapidly evolving tool catalogs outpace static lists.

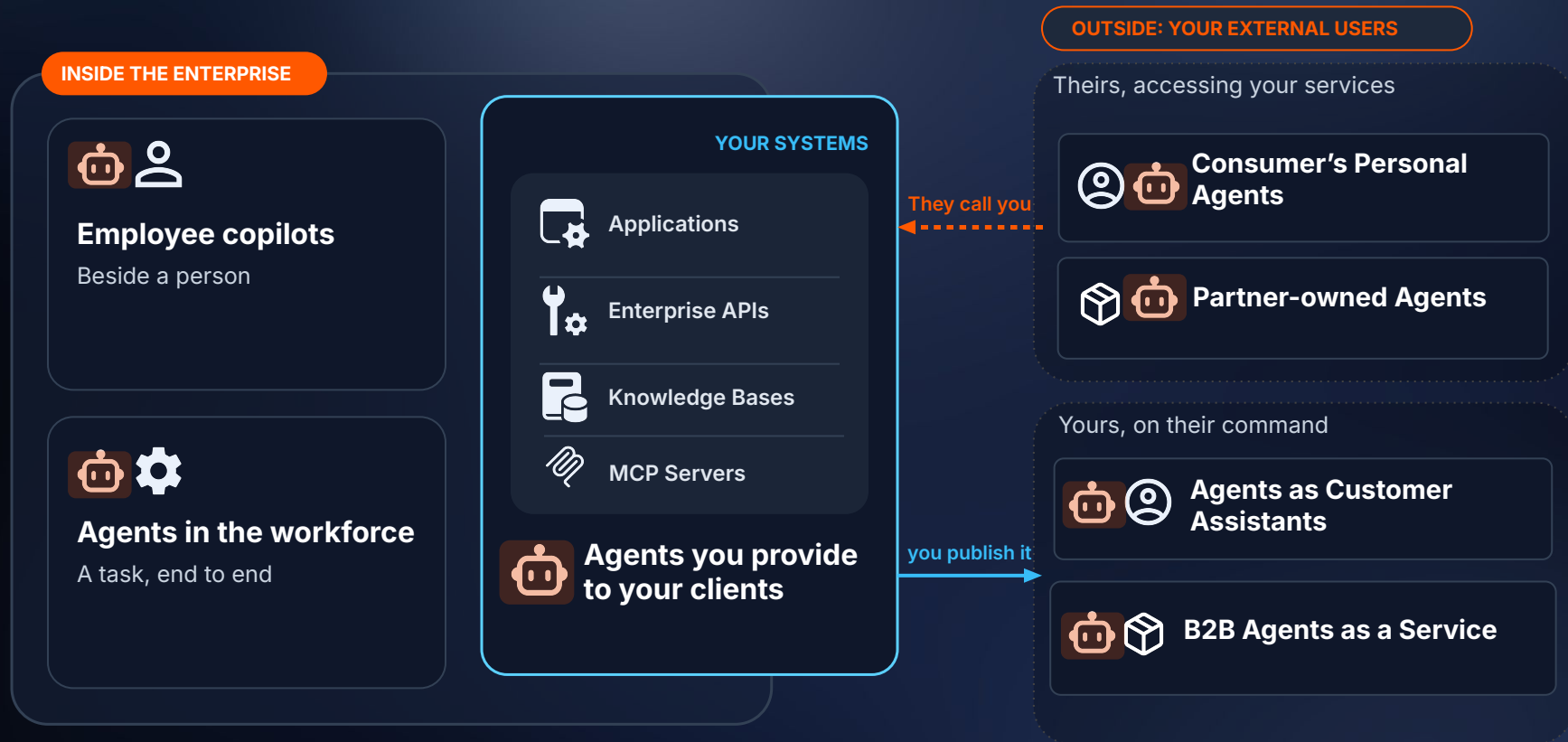


Cost of Borrowing

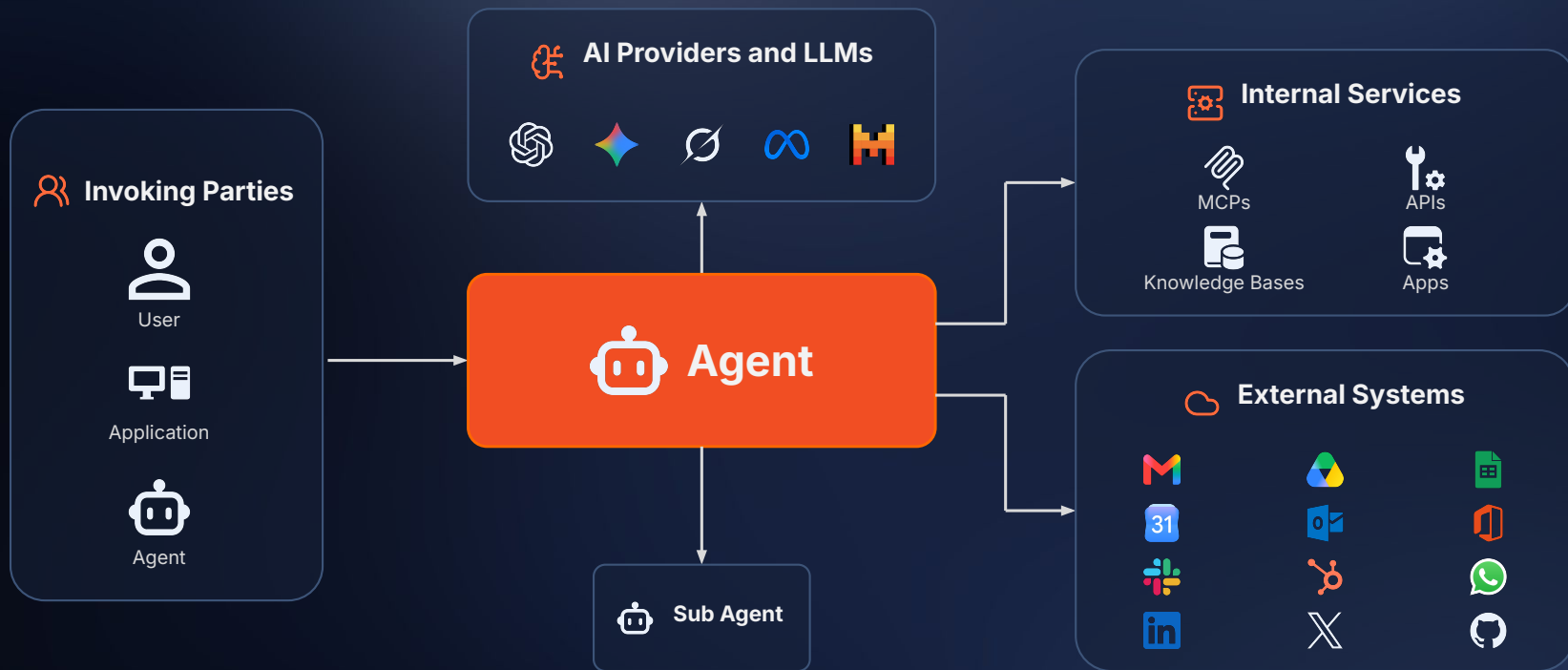
Auditability is destroyed as agents operate silently in the shadows.



Different types of AI Agents an enterprise will deal with



Agents reach across the stack



Four A's for Agent Identity & Access Management

The four things Agent ID does for every agent it governs.



Administer

Register every agent with its own identity, owner, state and lifecycle.



Authenticate

Agent-friendly credentials the agent proves itself with, never a borrowed user secret.



Authorize

What the agent may do on its own, and what it may do on behalf of a user.



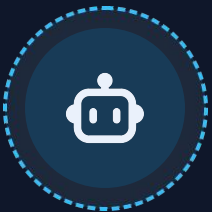
Audit

Every action traceable to the agent, the user it acted for, and the intent.



Start with governed **Agent ID** with an accountable owner

AGENT ID BAHARI FREIGHT, MOMBASA



Clearance Agent
UUID: f3568aea-64ef

● **ACTIVE**

First-Class Identity Entity
Autonomous & Delegated Execution



IDENTITY

agent://bahari/clearance



OWNER

Peter Kariuki, Operations Lead



CREDENTIAL

private_key_jwt (its own, not Asha's)

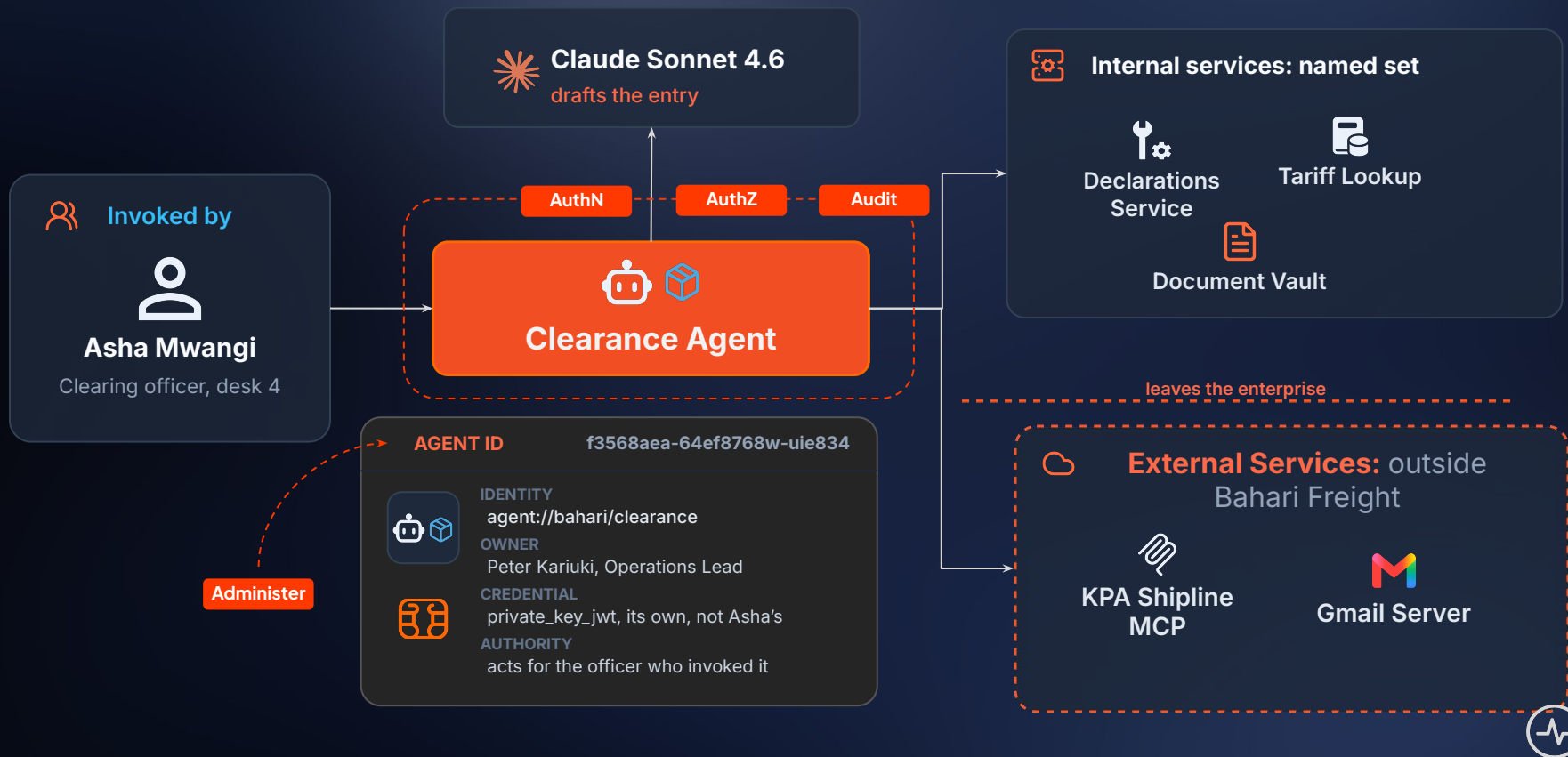


AUTHORITY

Acts for the officer who invoked it, under their delegated authorization

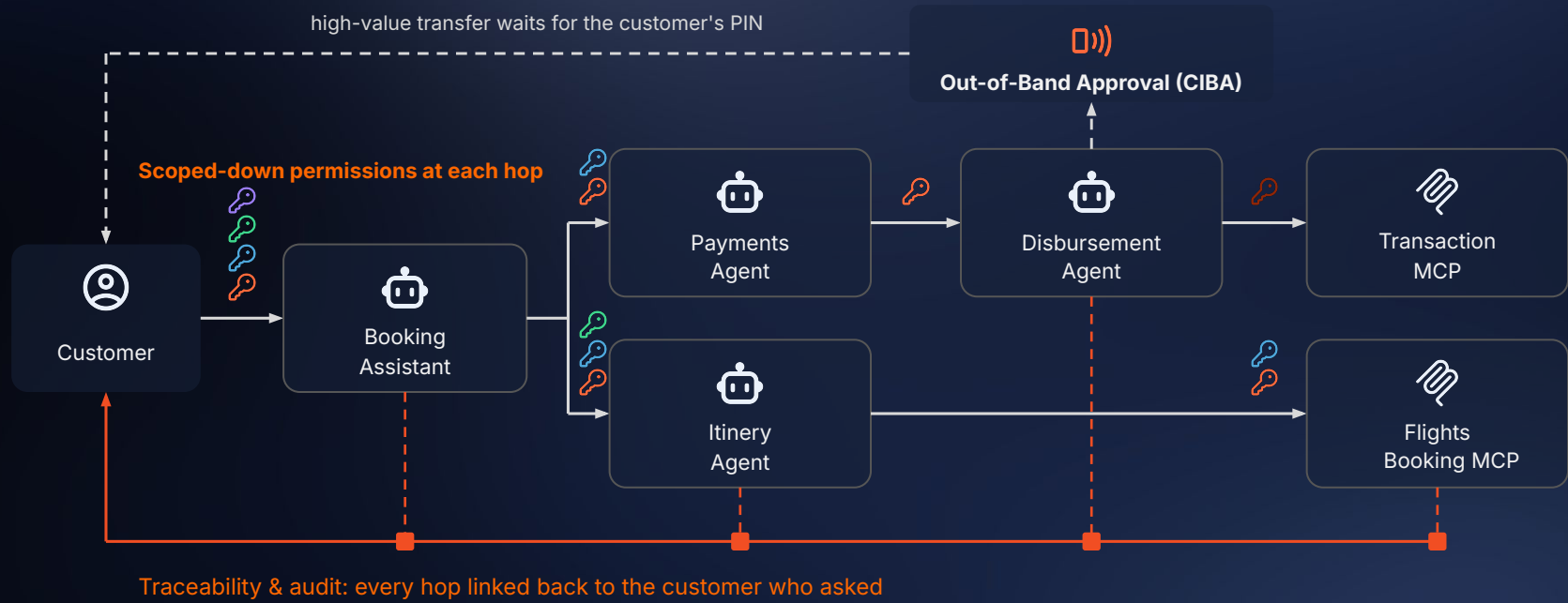


Agent ID enables the 4A's for every Agent



Agent to Agent, Delegation Down the Chain

One customer request, fanned out across agents and back.



Authorization & Audit with delegation chains and Intent

```
{
  "sub": "591c2a1c-2d08-4b1f-b8ff-cbfa46a0061e",
  "aut": "APPLICATION_USER",
  "iss": "https://idp.wso2/oauth2/token",
  "client_id": "9euHgATTsXbH0EryhnyoEA2r034a",
  "aud": "[target audience/mcp/resource server]",
  "nbf": 1757486458,
  "act": {
    "sub": "9b1deb4d-3b7d-4bad-9bdd-2b0d7b3dc6d",
    "act": {
      "sub": "637653a8-3989-429a-8ba1-3e66cf9235345"
    }
  },
  "azp": "9euHgATTsXbH0EryhnyoEA2r034a",
  "org_id": "f3568aea-64ef-4d70-8527-c90711996d06",
  "scope": "appointment_read appointment_create",
  "authorization_details": [
    {
      "type": "flight_booking",
      "target": [
        "[target resource]"
      ],
      "intent": "Cancel Nairobi to Dubai for better deal...",
      "constraints": {
        "max_invocations": 1
      }
    }
  ]
}
```

sub User / Resource Owner

Identifies the end-user who owns the data or resource.

client_id OAuth Client / MCP Client

Identifies the client application requesting access.

act → **sub** Agent/MCP Host Acting on Behalf of User

Represents delegated actor/AI agent executing actions. Chained in multi-agent scenarios.

scope Granted / Delegated Permissions

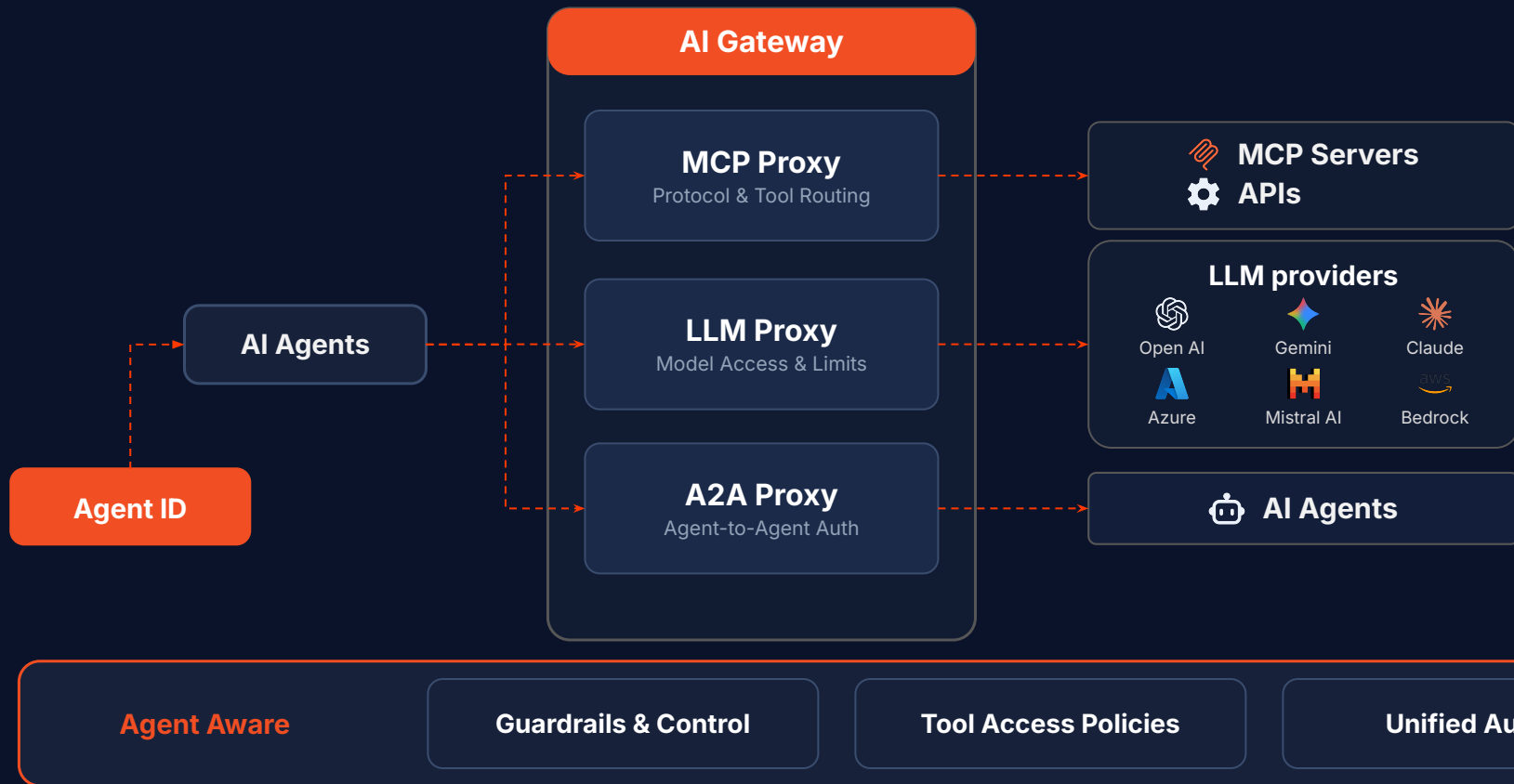
Permissions assigned to the request scope.

authorization_details Authorized Intent (RAR)

Rich authorization context with target and constraints.



Runtime Governance with **Agent Identity and AI Gateway** together



Welcome back, Ayesha Dissanayaka.

✈ Flights

🏠 Hotels

✳ Trips

Round trip

One way

Multi-city

From	To	Dates	Travelers
📍 Colombo	✈ Singapore	📅 Jun 24 - Jun 26	👤 2 adults



Flexible fares

Compare routes, cabins, and timings from one cabin workspace.



Protected bookings

Keep booked trips connected to secure account sign-in.



Fast comparison

Filter practical options

FRESH PICKS

Flight ideas for your next window of free time.

AI ASSISTANT

Wayfinder Concierge

Hi Ayesha, How can I help?

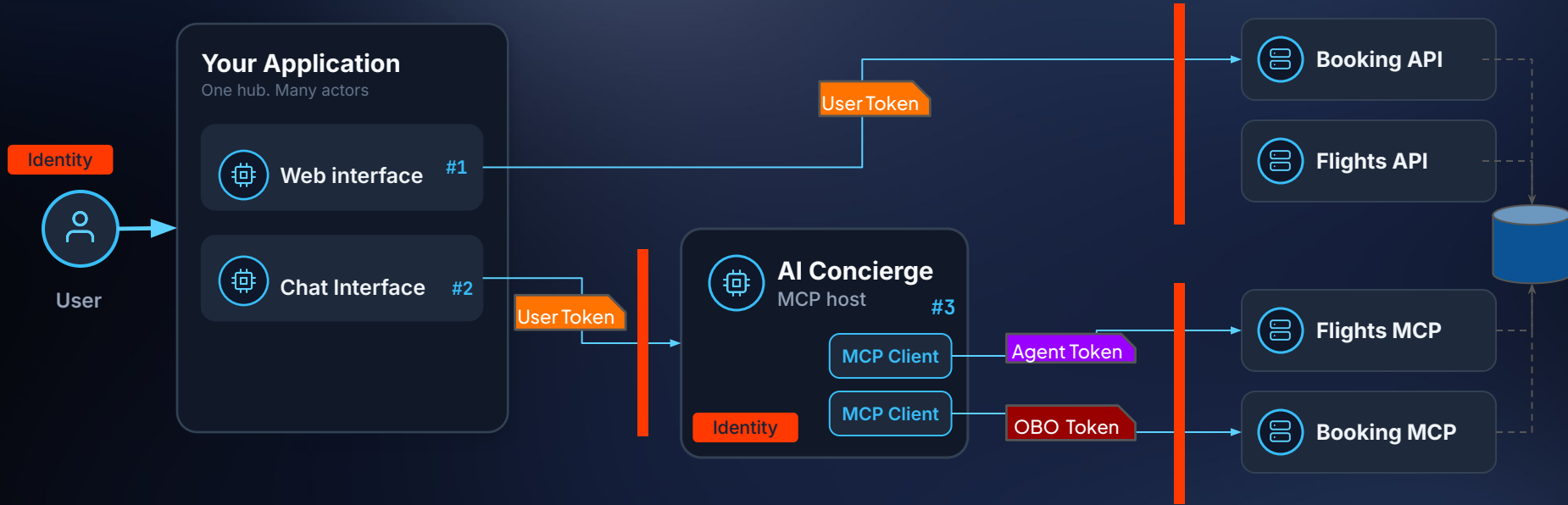
Plan my trip to MCP Dev Summit
Nairobi

Thinking...

Ask about flights or bookings

Start searching

Real world scenario in enterprises



Your Back-to-Office Checklist.

- 01** Not every AI agents touching your systems are built or controlled by you
- 02** Agents need **first-class identities**, not shared API keys, or borrowed credentials.
- 03** Apply the **4A Framework** to govern agent access
- 04** **Agent ID with AI Gateway** for complete oversight and transaction control
- 05** Start now. **Crawl, walk, run**. And build a foundation to scale safely





SEPT 22 - 24, 2026 | NAIROBI, KENYA

Thank You!



Ayesha Dissanayaka

Associate Director/ Architect
AAIF Ambassador

Delegation: On-Behalf-Of(OBO) Token

User/Subject
Token

+

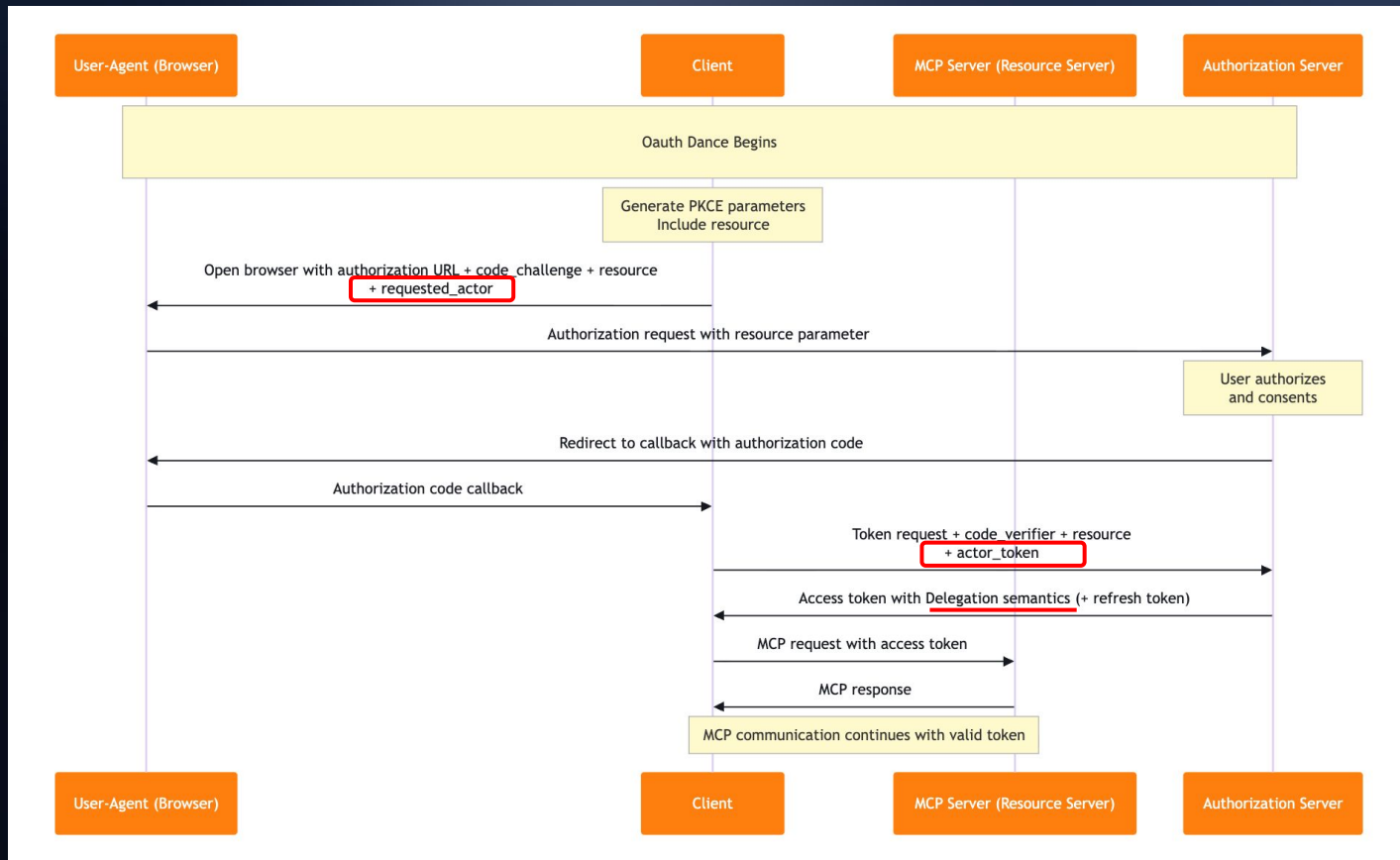
Agent/Actor
Token

Exchange

```
{
  "sub": "7a6f7b26-f9ea-48ea-9012-87d6b54f4055", ← user identifier
  "aut": "APPLICATION_USER",
  "iss": "https://localhost:9443/oauth2/token",
  "client_id": "7KafXIoqkfzS6TugWBBtby9A7FYa", ← Oauth/MCP Client identifier
  "aud": "http://localhost:8000/mcp",
  "nbf": 1762978120,
  "act": {
    "sub": "91bb155e-b23c-4a34-94e5-77478691f4bd" ← agent/MCP Host identifier
  },
  "azp": "7KafXIoqkfzS6TugWBBtby9A7FYa",
  "org_id": "10084a8d-113f-4211-a0d5-efe36b082211",
  "exp": 1762981720,
  "org_name": "Super",
  "iat": 1762978120,
  "jti": "f692e5cc-6906-4935-862d-bdab3a18623c",
  "org_handle": "carbon.super"
}
```



User Consented OBO Token



B2B Agents as a Service: **Your Org-aware Agents**



You already have users, now you have Agents

Both sides are already managed independently. Nothing yet connects them.



Your users

In an existing identity provider(s)

- ✓ Profiles and attributes
- ✓ Entitlements and group memberships
- ✓ Authentication and lifecycle



Your agents

In WSO2 Agent ID

- 🔑 Agent identities and credentials
- 🔧 Permissions, roles and entitlements
- ↔ Ownership, state and lifecycle



An agent acting on-behalf-of a user needs both sides at once.



Govern centrally, and let agents act on-behalf-of your consumers

Agent ID has never seen the user, and still decides what the travel assistant agent may do for her.



1 Federate

User authenticates at the provider and arrives with her attributes. (Federation, token exchange, ID-Jag)

2 Govern the agent

Agent ID registers the Travel Assistant, credentials it and issues its tokens.

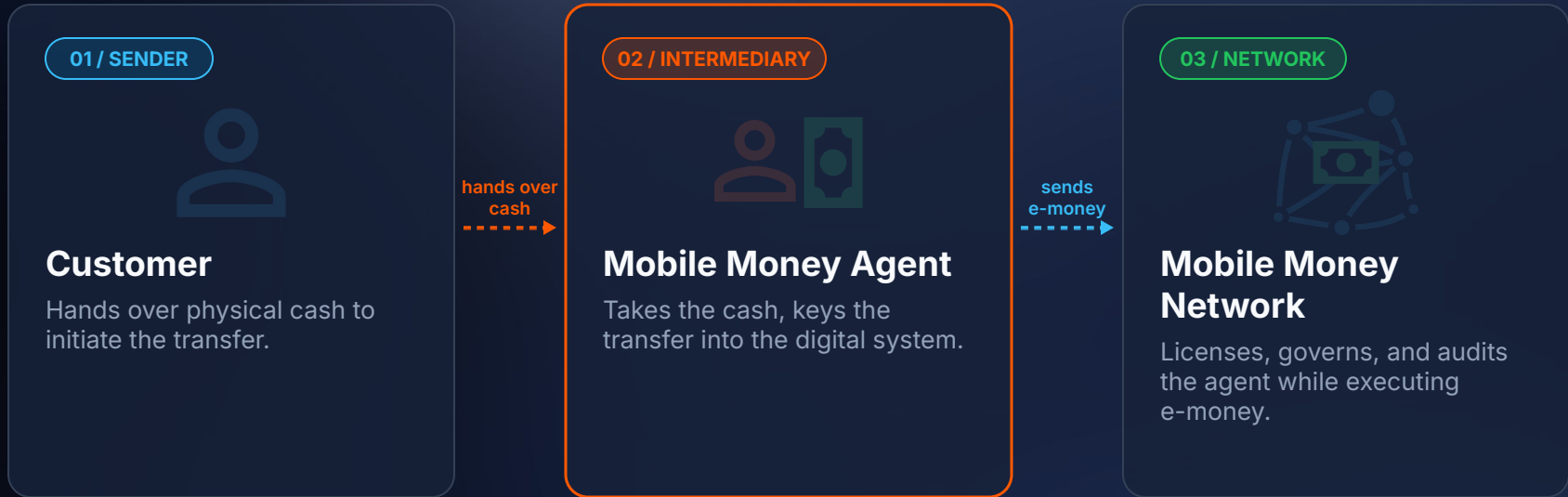
3 Call on her behalf

The agent reaches Booking Services with a token naming both it and Maya.



How Traditional Agent Networks Work

A physical-to-digital value flow built on explicit handoffs and infrastructure.



Infrastructure, Not Pure Trust: Physical verification at the counter makes the digital handoff safe.



"Agents" are already in Africa's operating system

THIS MORNING

Human agents

One deal at a time



Shipping agent



Mobile money agent



Safari agent

delegates the boring half

BY NEXT YEAR

The agent's own agents

Thousands per agent



always on



Clearance agent

Files paperwork for 10,000 containers



Reconciliation agent

Matches 2 million transfers overnight



Itinerary agent

Calls 200 lodges when a flight drops

Now they run at the speed of code.



Start with a governed identity and an accountable owner



First-Class Identity

Registered, rotated, revocable



Streamlined Provisioning

Admin or self-service, by agent type



Explicit Ownership

One accountable human, always



Machine-Ready Credentials

Its own, never a borrowed secret



Emergency Suspension

One switch, no users affected



Agent ID enables the 4A's for every Agent



Deploy and run with controlled inbound and outbound access

When invoked: who may call it



**Authenticate
the Caller**



**Authorize
Exposures**



**Step-Up
Assurance**



**Time/Intent-Bound
Consent**

When reaching out: what it may invoke



Model Interaction



Internal Services



External Integration

