

WSO2con

AFRICA

SEPT 22 - 24, 2026 | NAIROBI, KENYA

Creating Seamless and Secure Authentication Experiences: From Consumers to AI Agents



Dulsara Kumarage

Associate Lead - Sales Engineer II



Omindu Rathnaweera

Head of Product Management - IAM



Ayesha Dissanayaka

Associate Director/Architect - Engineering

Overview

01 Challenges in Securing Consumer Apps

02 Securing a Consumer App

Hands-on

03 Building the IAM Journey

Hands-on

04 Beyond Authentication: VCs & Identity Verification

Hands-on

05 Knowing Your Users: CDS & Identity Analytics

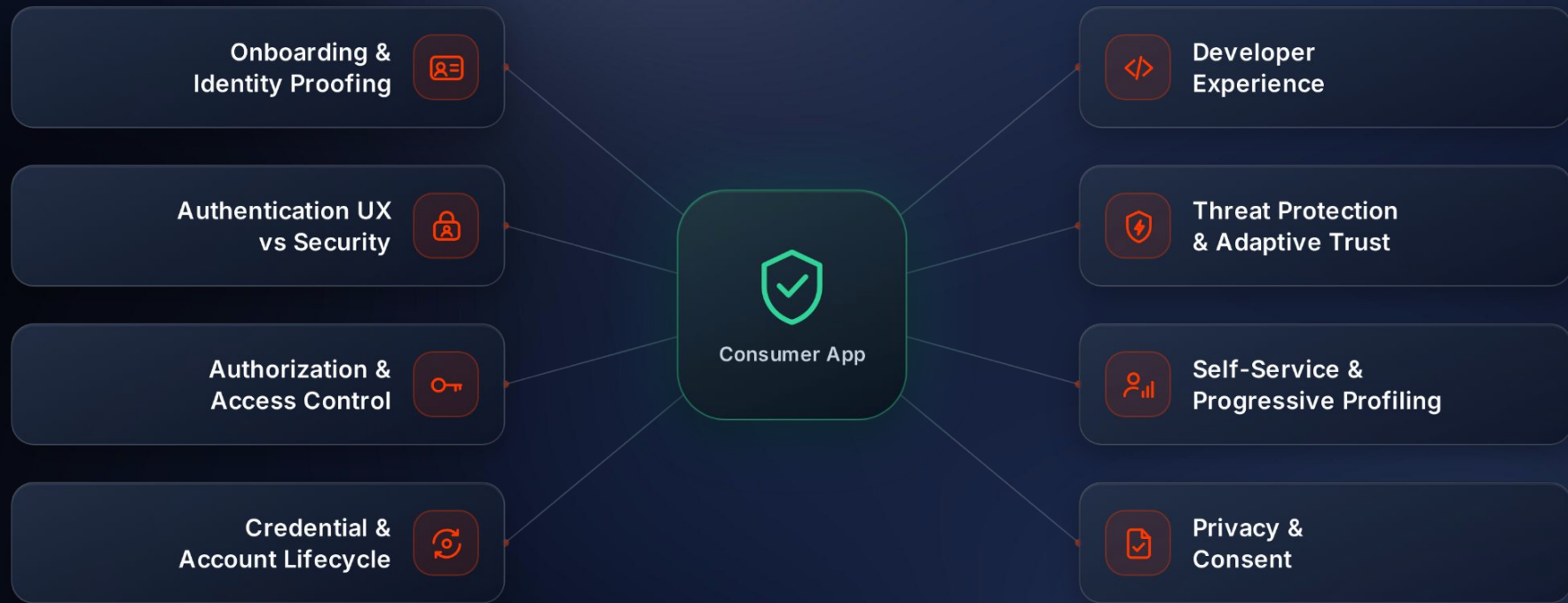
06 Identity for AI Agents

Hands-on



Challenges in Securing Consumer Apps

Challenges in Securing Consumer Applications



The Balancing Act



Security that frustrates users

→ they leave



Friction only when the risk earns it

→ they stay, and you're covered



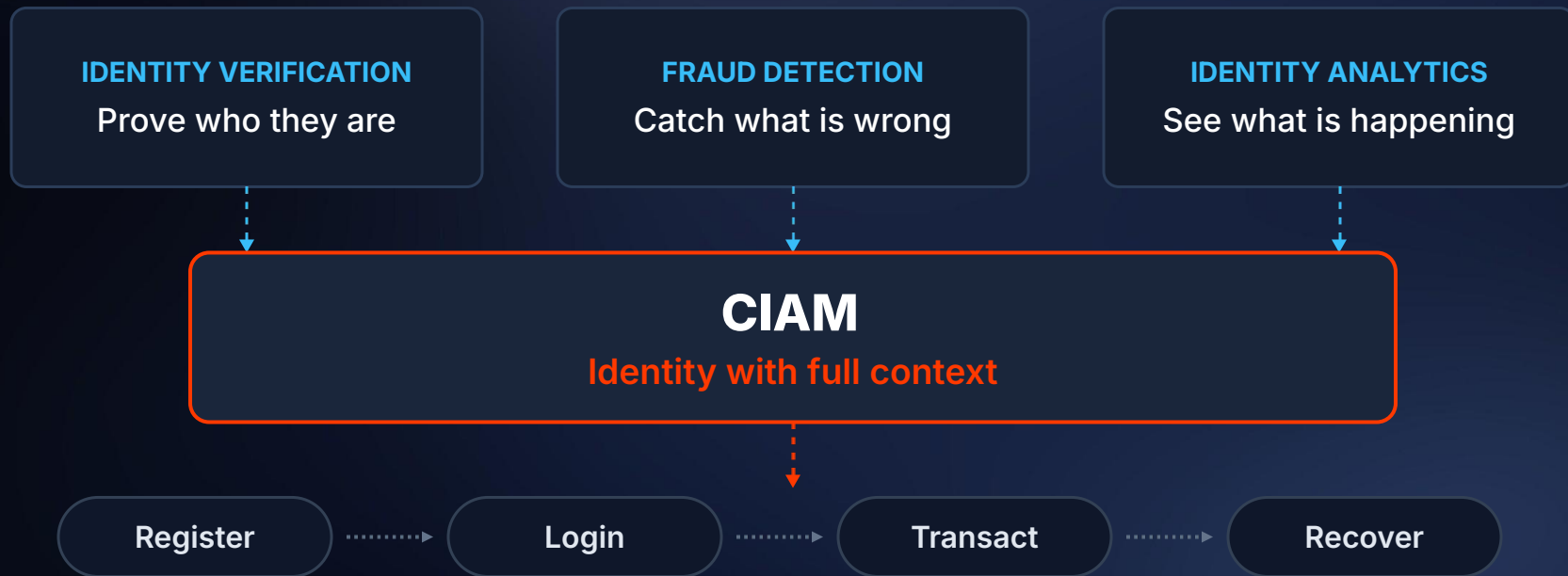
Great UX with weak security

→ you're exposed



Convergence in CIAM

Trusted customer journeys require **verification**, **fraud detection**, and **customer insights** to work together.



AI is Fundamentally Changing Identity Management

A new kind of actor is showing up at the front door: **non-deterministic**, autonomous, and acting on someone else's behalf.

AI for IAM across the identity integration lifecycle.

- Copilot-driven SDKs.
- Natural-language login flows.
- Zero-click MCP setup compress the integration lifecycle.



Blending identity and intelligence with
seamless, secure authentication

<https://wso2.ai>



Build vs Buy

Build from scratch:

- Full control, full burden
- Every evolving threat is your problem
- Auth is never "done", it's a moving target

Use an identity provider:

- Focus on your business logic
- Security, compliance, and standards handled
- New capabilities (passkeys, adaptive auth) on day one



A single **open source solution** powering multiple deployment options

WSO2 IDENTITY SERVER

The Leading Open Source IAM

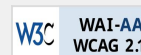
Identity Server is a powerful, modern and highly extensible identity and access management solution for your on-premises or cloud environment

WSO2 **Identity** Platform

SaaS IAM

Identity Platform is a developer-focused IDaaS solution that provides seamless, secure authentication and user management. It is available as a multi-tenant SaaS or private cloud deployment.

Verifiable Security Assurance and Regulatory Trust



Available for purchase via



Securing a Consumer App

Follow Along!

```
git clone https://github.com/wso2con/2026-NBO-iam-tutorial-1
```



Identity Platform Free Sign Up
<https://asgardeo.io/signup>



DEMO

Securing a Consumer App

The **Manual** Mode

DEMO

Securing a Consumer App

The **AI-Assisted** Mode

DEMO

Elevating the IAM experience

CIAM **capabilities** that make the difference

Beyond Authentication: VCs & Identity Verification

DEMO

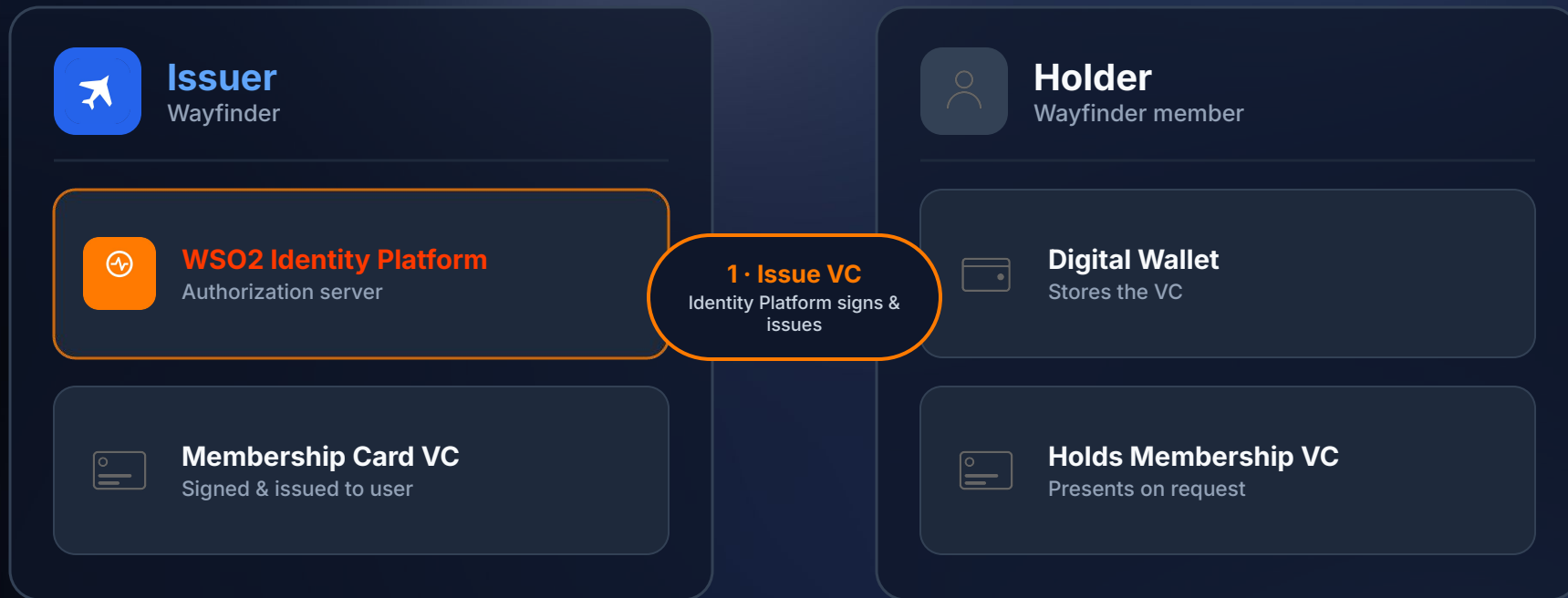
Verifiable Credentials

Empowering portable, user-centric digital identity

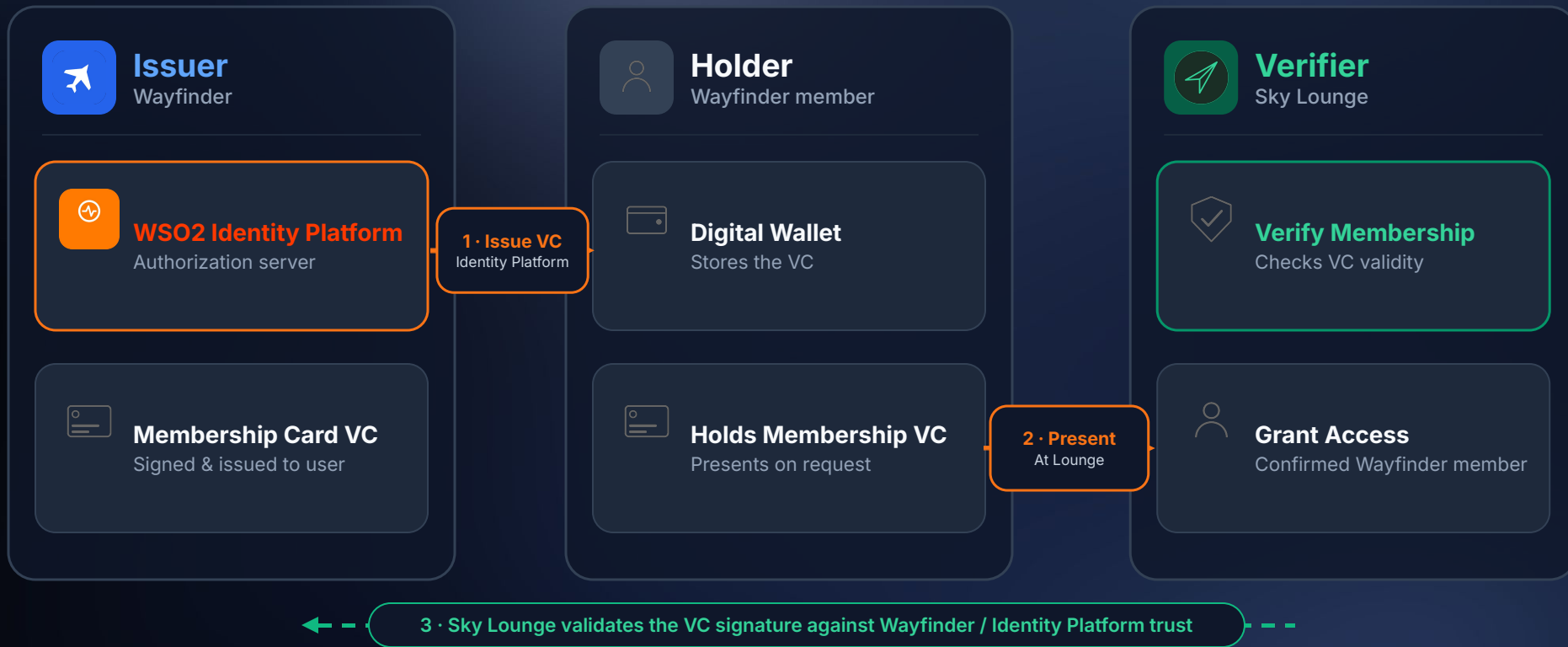
Verifiable Credentials (VC) with WSO2 Identity Platform



Verifiable Credentials (VC) with WSO2 Identity Platform



Verifiable Credentials (VC) with WSO2 Identity Platform Architecture & Flow





Demo

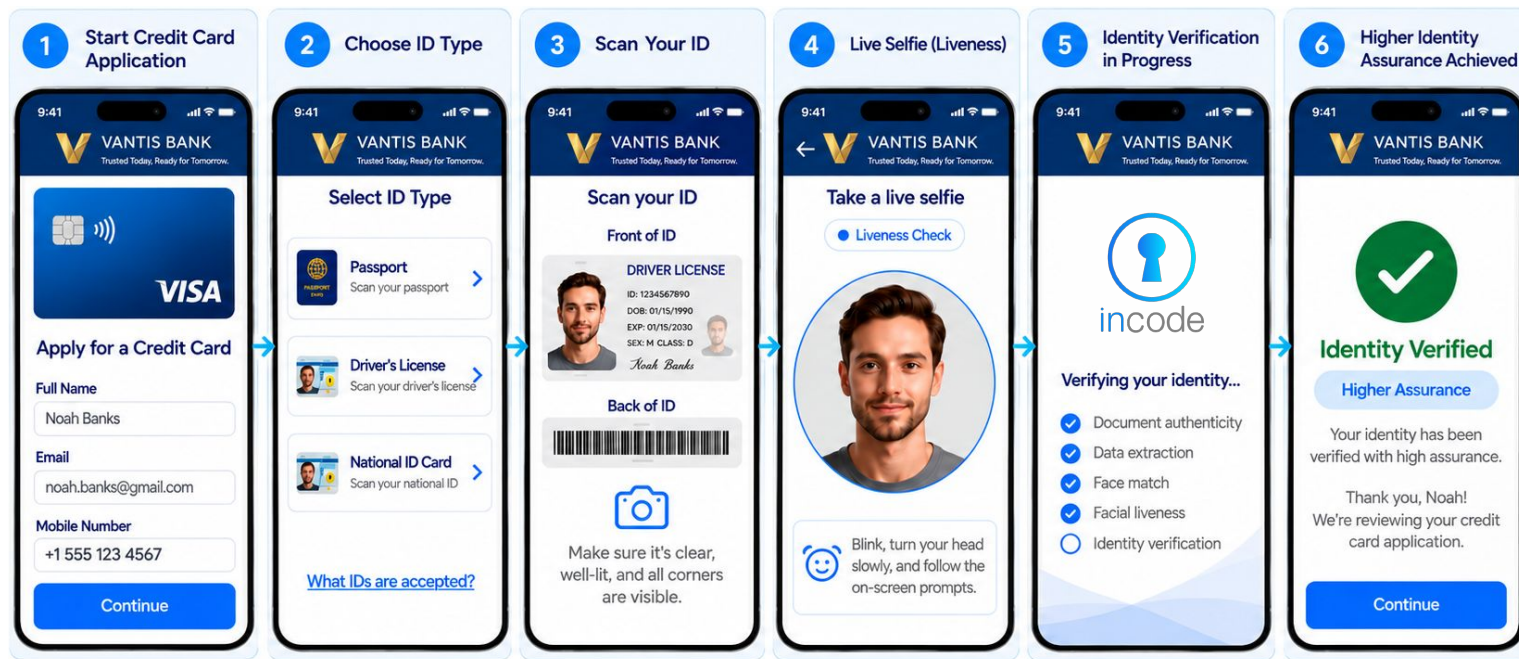
BEYOND AUTHENTICATION

Identity Verification

Know the human behind the account

Identity Verification

High risk actions trigger an automated identity check. A document scan, a facial liveness test, done entirely from home.



Knowing Your Users: CDS & Identity Analytics

DEMO

Customer Data Service

A **golden profile** of every customer

Your customer is one person. Your data says otherwise.

Three gaps stand between businesses and a real understanding of their customers.



Anonymous blind spot

Most of the customer journey happens before login. Those early signals are lost the moment a visitor signs up.



Fragmented systems

CRM, loyalty, booking, support and POS each hold a different slice of the same person, keyed by different identifiers that never meet.



Developer Execution Friction

Even when businesses successfully collect customer data, it gets locked in heavy analytical warehouses. Application developers lack the lightweight, low-latency APIs required to actually inject that data into the live app experience.

The result: Generic experiences for customers a business already knows and no way to act on what it learns.



One golden profile. Every use case flows through it.

Profile Enrichment



Connect & Unify fragmented Data

Break down silos. Ingest and merge customer data from CRM, loyalty and legacy systems. Use pre-built integrations or write powerful integrations.



Advanced progressive profiling

Gather customer details gradually through natural interactions.



Track guest user journeys

Capture guest behavior from the first visit - before signup or login.



Golden profile

The unified, consent-aware single source of truth anchored on Identity.

➔ **Powered by identity resolution**

Rule-based matching stitches every source whether it is anonymous, cross-device, cross-system into one single profile.

Activation



In-app personalization

Deliver real-time tailored experiences and content inside apps.



Consent-aware data access

Every profile read is gated by the customer's consent choices.



Journey orchestration

Feed real-time profile signals into your campaign and engagement tools.



Capabilities



Guest User Tracking

Track anonymous or guest users and seamlessly preserve their data during the sign-up process.



Profile Unification

Unify fragmented, siloed customer profiles into a cohesive single customer view.



Profile Export

Easily export unified profiles to sync downstream systems and target destinations.



API Integration

Invoke powerful APIs to retrieve profile information in-app and deliver highly personalized experiences.



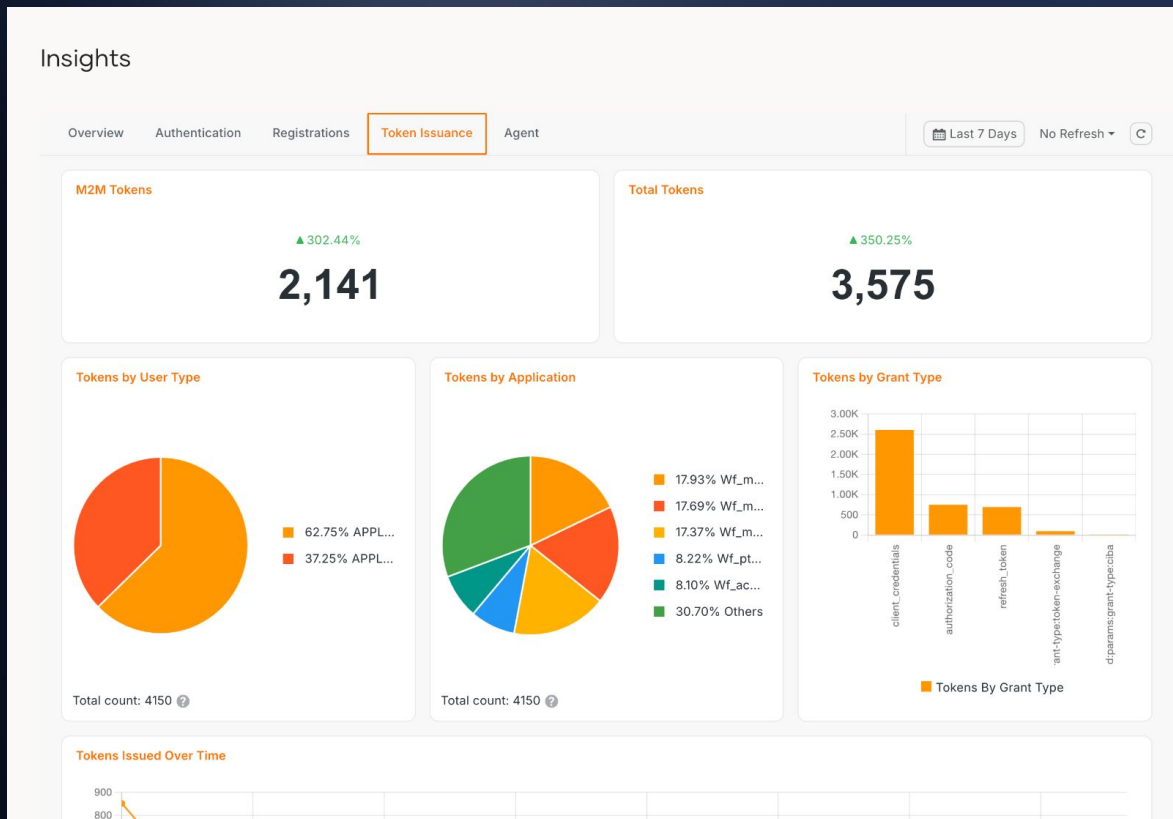


Demo

Identity Analytics

Customer **usage insights**, in Moesif.

Event-Driven Insights: Identity Platform to Moesif





Demo

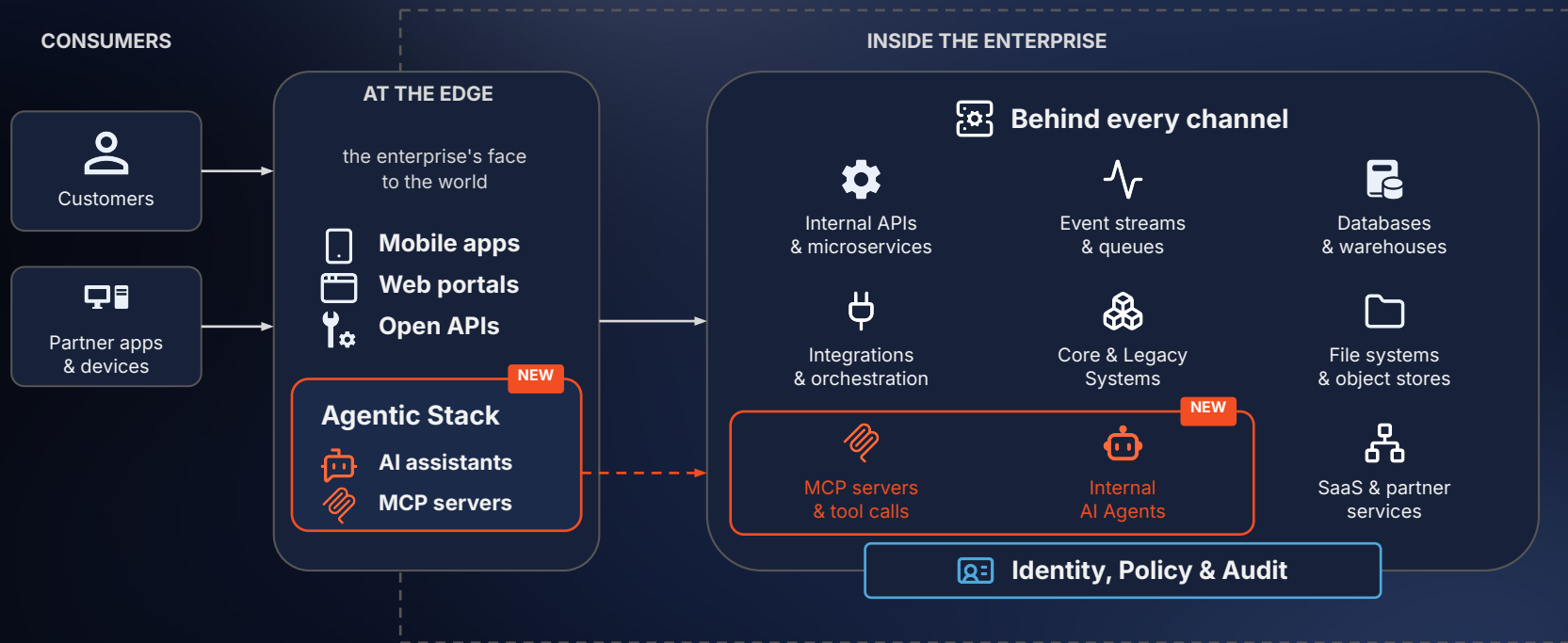
FUTURE OF IDENTITY

Agents as the new frontier for your customers

The identity **journey** continues

The Agent Advantage: Transforming How You Engage Customers

The enterprise already exposes itself to the world. Agents arrive at the same door.



Traditional ChatBot vs. **Agentic AI**

 **Classic Chatbot**

Book me a flight to Nairobi

Here are our Nairobi fares:

 **Nairobi fares & routes**
airline.co.ke/fares

How to book:
1. Open the booking page
2. Choose your dates
3. Enter details and pay

If a better fare comes up, move me to it.

Sorry, I did not understand.
Refer front desk for details.

 **Intelligent Agent**

Book me a flight to Nairobi

 **Done. Here is what I did:**

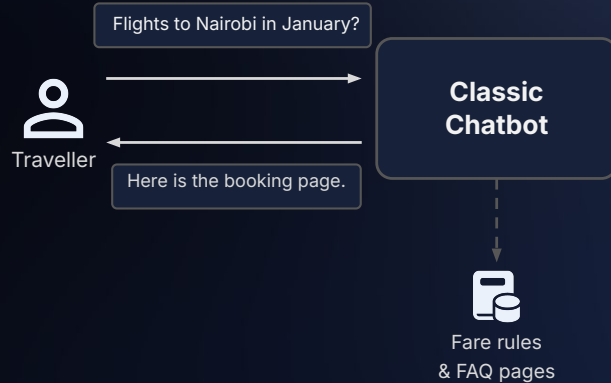
- ✓ Booked KQ 476, 12 June
- ✓ Seat 14A, paid
- ✓ Added to your calendar
- ✓ Itinerary sent

If a better fare comes up, move me to it.

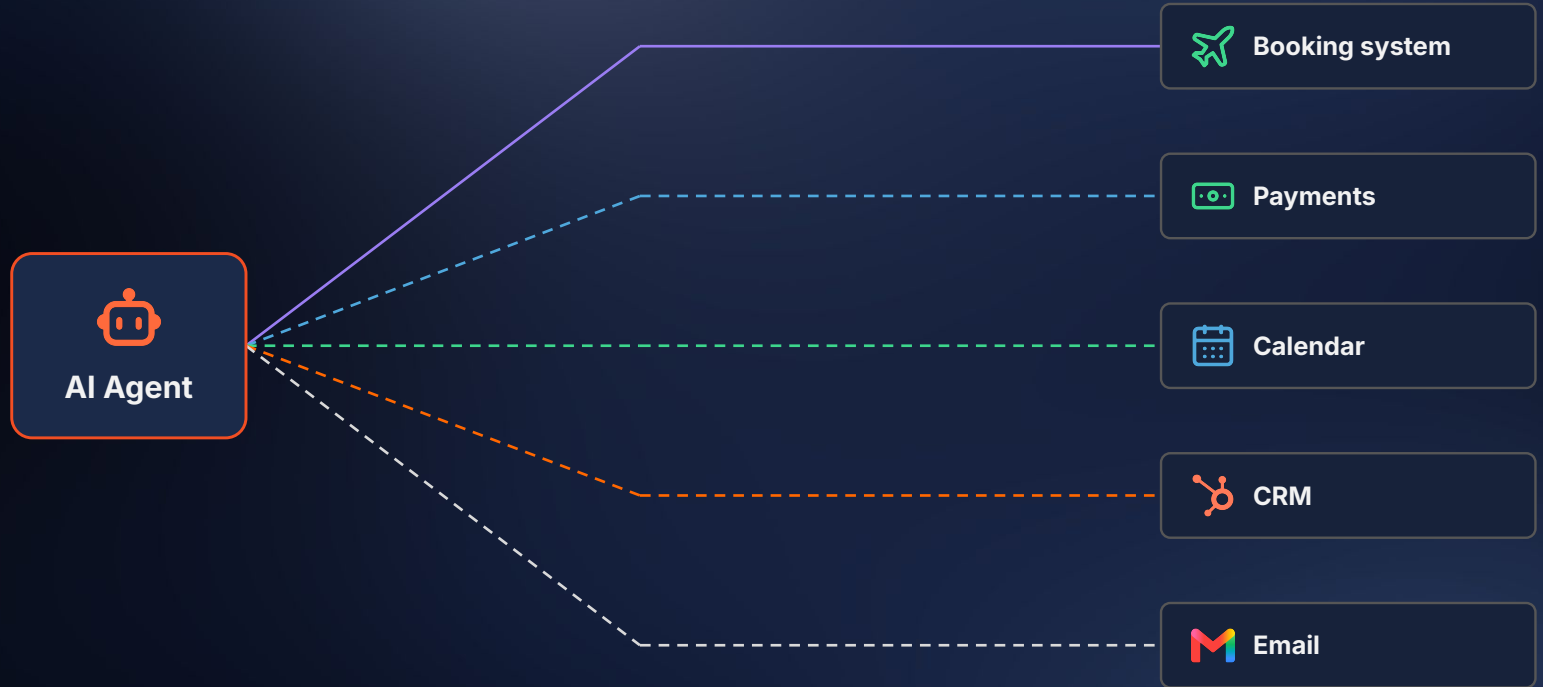
 ●●● watching fares



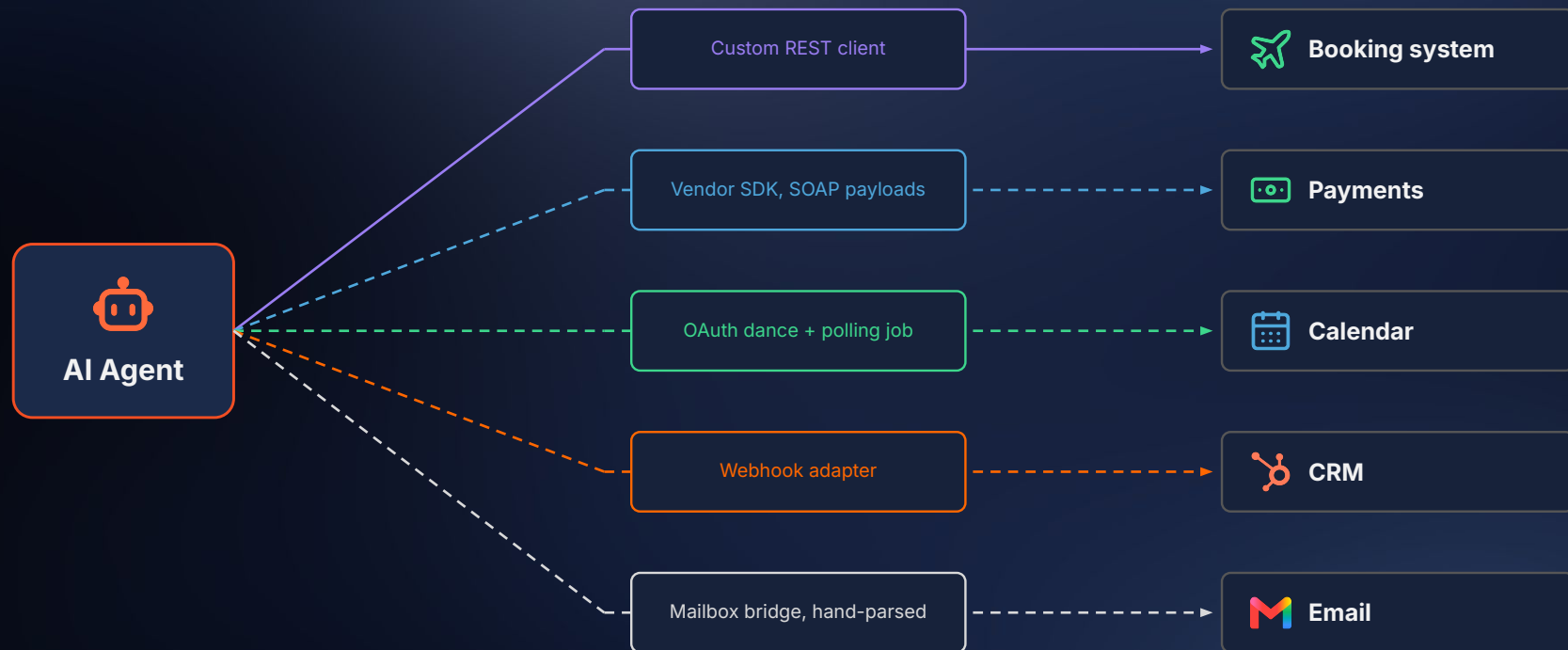
Architecture: Traditional ChatBot vs. Smart Assistance



Tools are what make agents **powerful**



A different integration for every tool: **build it, test it, maintain it**



Model Context Protocol: **the standard way agents see tools**

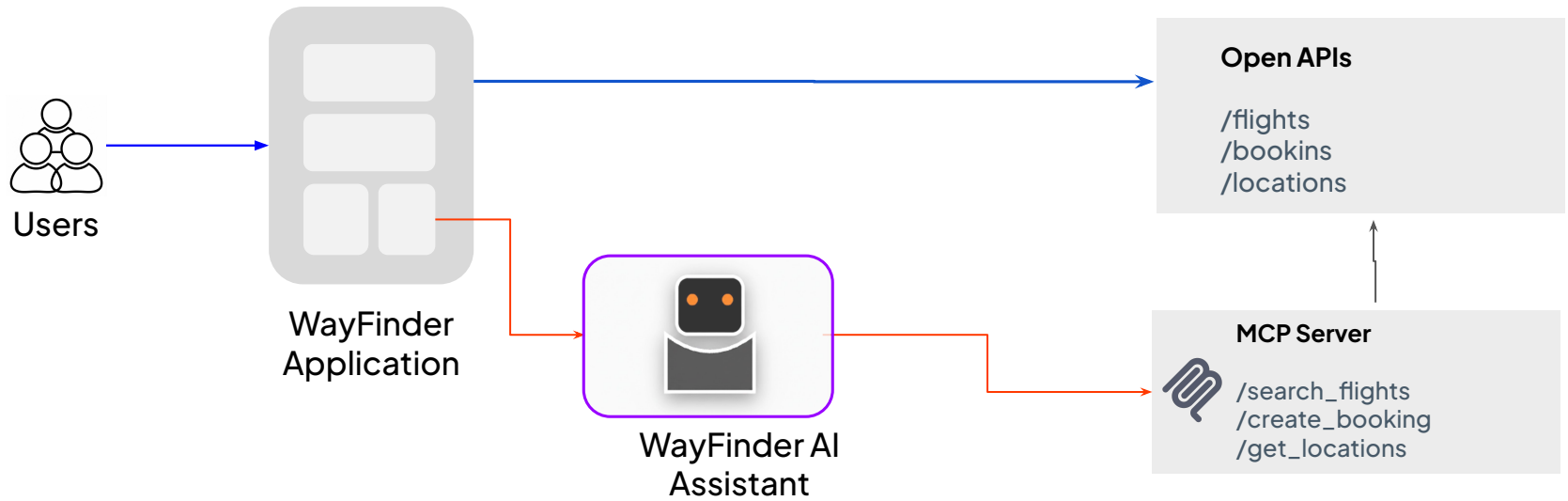
The USB-C port for AI agents: one plug, every tool



Each service describes itself the same way, so the agent needs no code of its own to reach it.



Demo



Scenario 01: Securing MCP Servers & MCP Authorization

1

Register MCP Servers as Resources

2

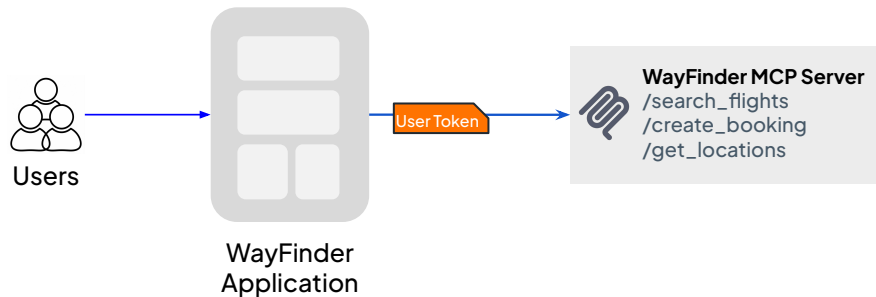
Define permissions for MCP Tools

3

RBAC to MCP

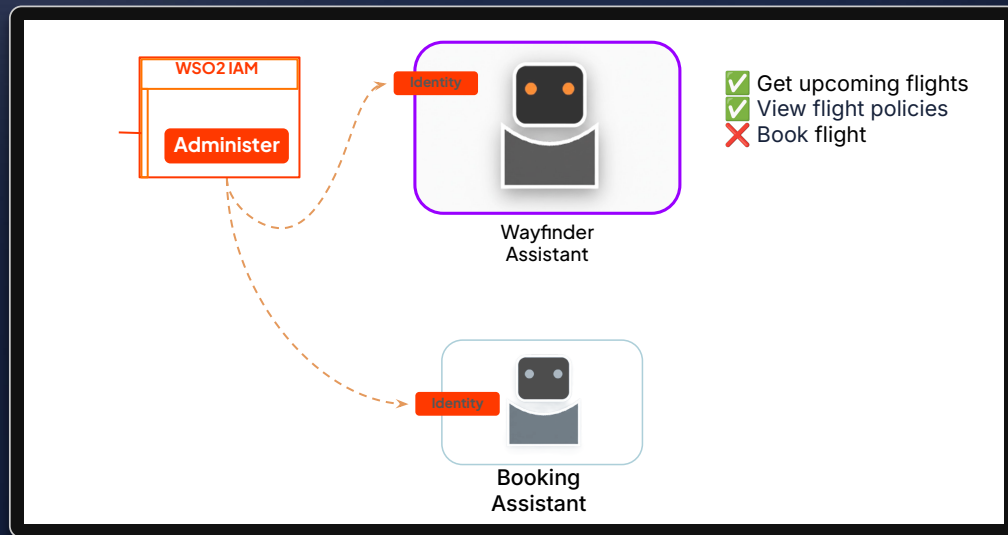
4

Register MCP Client to connect



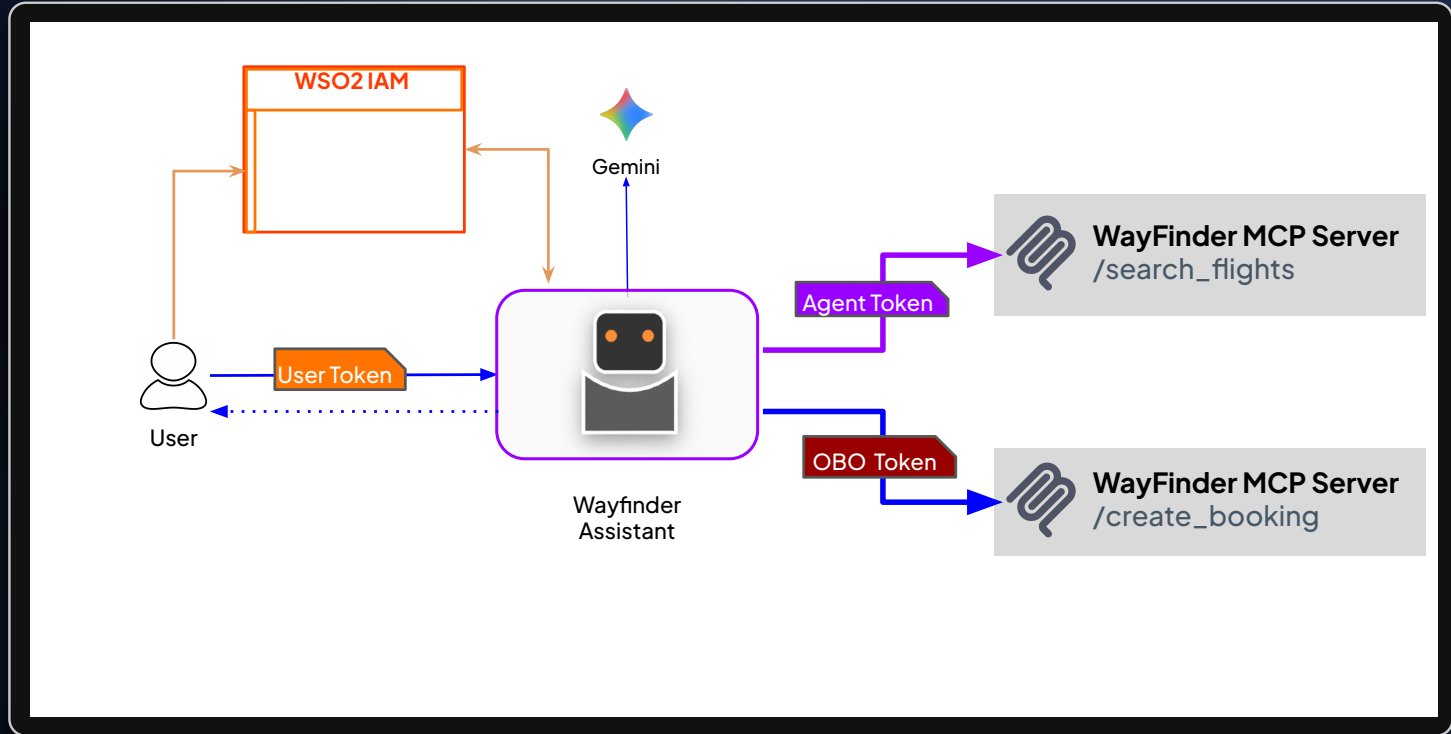
Scenario 02: Agents as your consumers

- 1 Register Agent and obtain credentials
- 2 Manage attributes and states
- 3 Assign Permissions to act on its own



Let's put it to test

Scenario 04: User delegated authorization for Agents



Track agent activities across different systems

● **actor** the agent that acted ● **sub** the user it acted for ● **req** ties the hops together

wayfinder · audit trail · one booking, five systems · ids truncated				
Identity Platform	05:38:12.041Z	TOKEN ISSUED	actor=c85157a8... sub=c98ee690... req=cca4cb38...	
MCP Server	05:38:13.214Z	POST /mcp/tools/create_booking	actor=c85157a8... sub=c98ee690... req=cca4cb38...	
Bookings API	05:38:13.216Z	POST /api/bookings	actor=c85157a8... sub=c98ee690... req=cca4cb38...	201
Flights API	05:38:24.993Z	GET /api/flights	actor=c85157a8... sub=c98ee690... req=cca4cb38...	200
Payments API	05:38:25.104Z	POST /api/payments	actor=c85157a8... sub=c98ee690... req=cca4cb38...	403

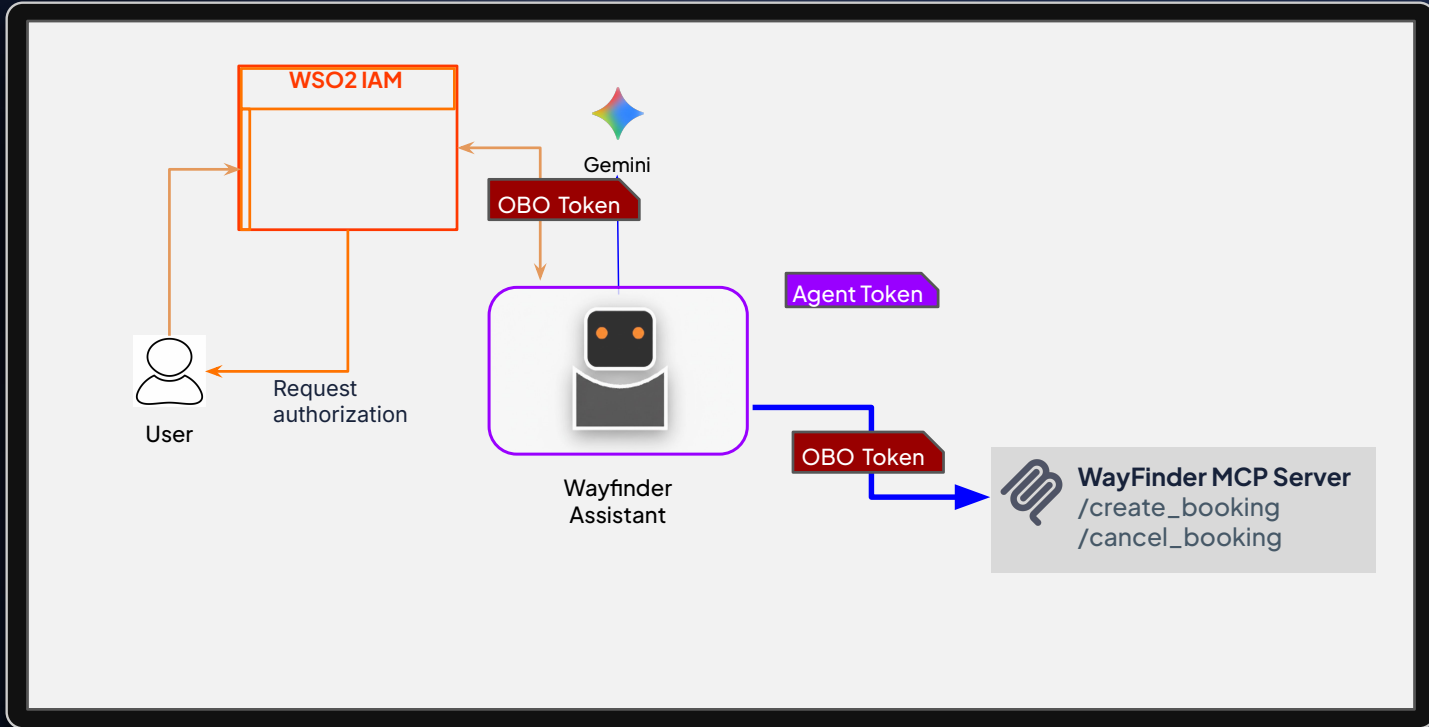
Every hop carries both identities, so you can see what the agent did, for whom, and where it was stopped



Ambient/Background Agents

Scenario 05: Ambient Agents

Dynamic human-in-the loop authorization



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": "medical_appointment",
      "target": [
        "[target resource]"
      ],
      "intent": "Book one driving licence renewal medical...",
      "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.



Ambient Agents Analytics

Overview Authentication Registrations Token Issuance **Agent**

Last 7 Days No Refresh C

Agent Tokens

▲ 45.68%

236

Active Agents

▼ 0.00%

15

New Agents

▲ 200.00%

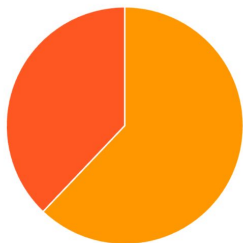
6

Active Agent Sessions

▲ 100.00%

24

Agent Token Distribution

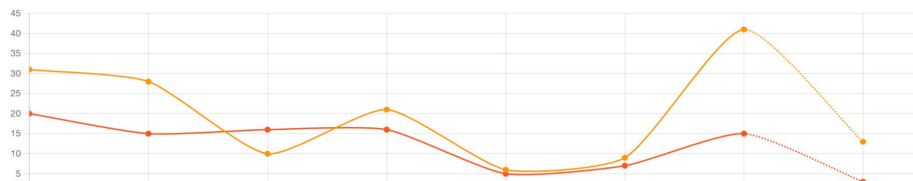


Total count: 256

Agent Usage by Users

- A4c8e00a-88ed-495a-Abd5-412ff4776907
- A46bd41e-452b-4231-8722-E29714b67851
- D0e82c22-Fc70-4f33-A6c9-Ce81dd3d78e9
- D400b93c-6feb-4f2c-887d-8abcca62f645
- Eeef830b-173d-4ace-A239-Dfb75e21cf0c
- 19f3b646-Ba29-47a4-8731-Ebd8500bdb8a
- 588a15dd-Bf8b-45ce-915d-5c5180e7b676
- 13158590-890e-401c-988d-35fd481ee136
- 135e425d-1904-44d7-9eb9-01269dacc963
- F3b50780-5272-4560-85de-Aafef9cd0d19
- 2ff6a3f6-D5a4-4c9f-884f-8e8acc2261b8

Agent Tokens Over Time



Agent Tokens Over Time

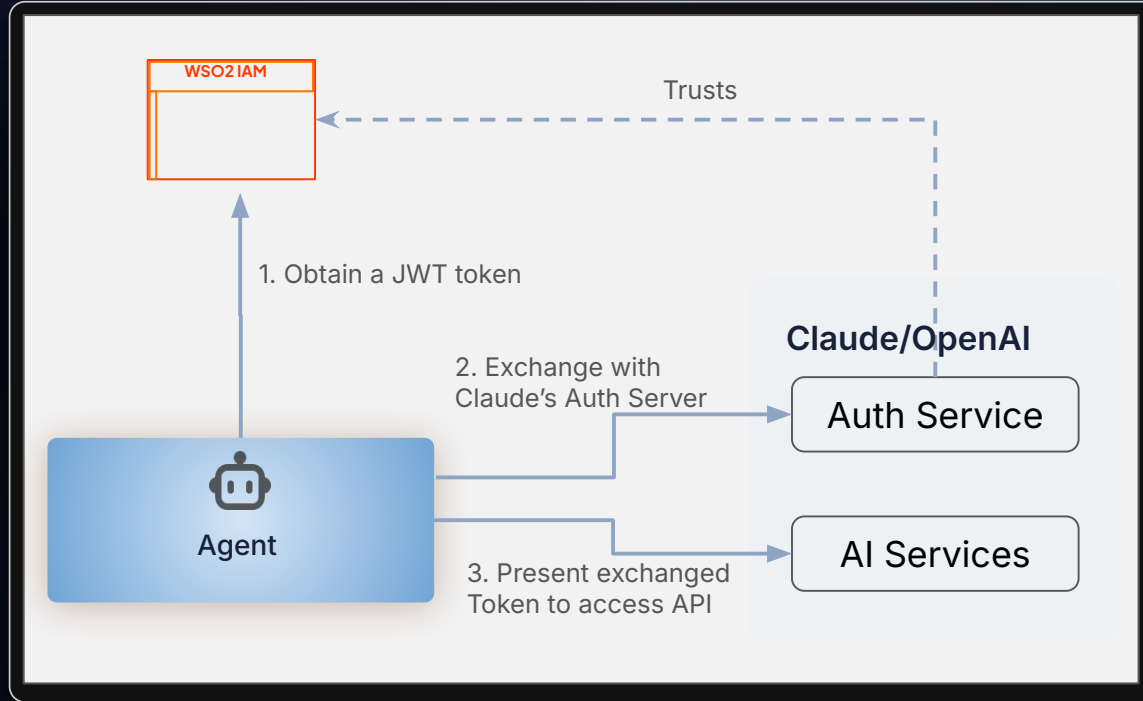


Agent Logins Over Time

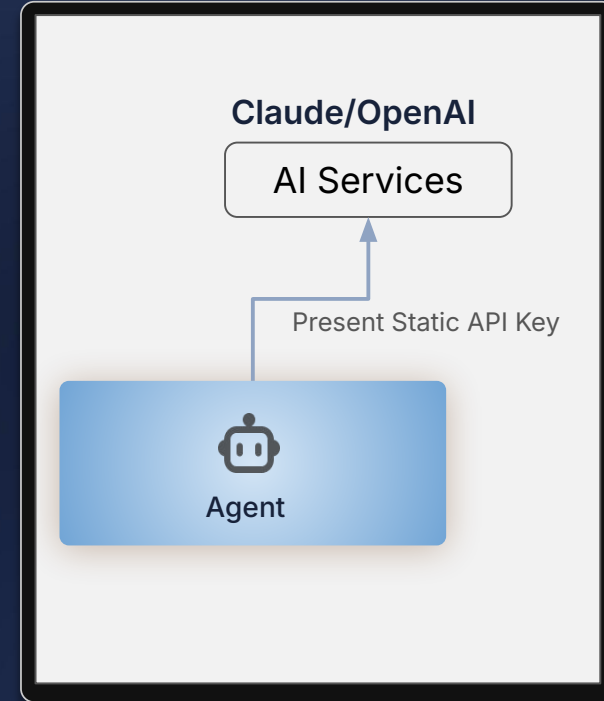


Scenario 06: Model Provider Access with Agent ID

Integrate with Claude/Open AI Workload Identity Federation



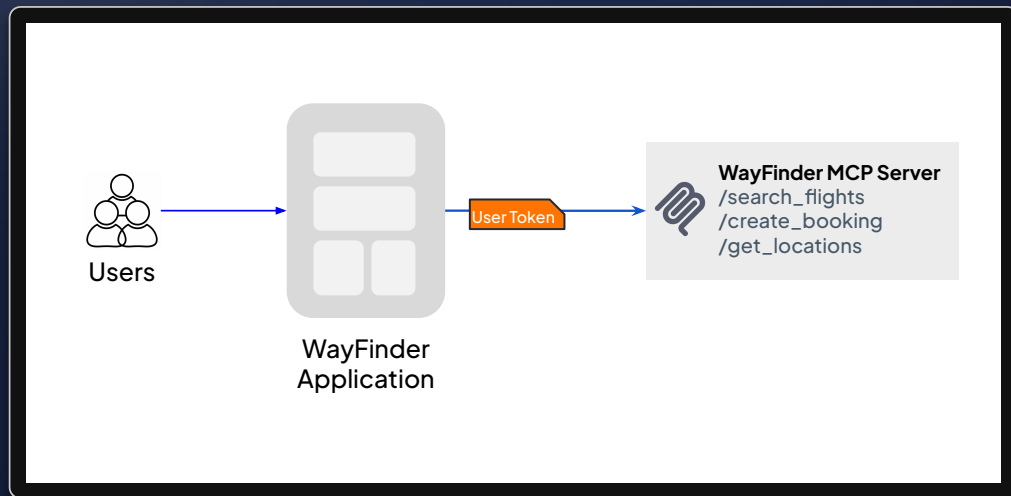
Vs.

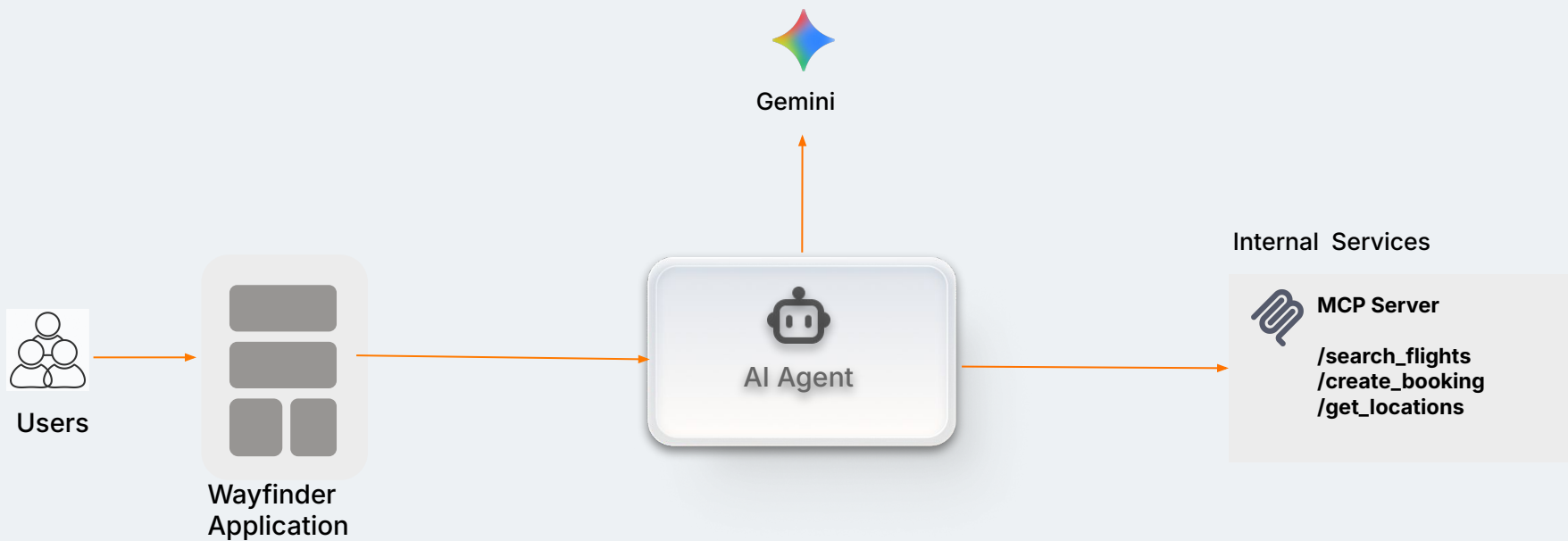


Question Time!

Scenario 01: Securing MCP Servers & MCP Authorization

- 1 Register MCP Servers as Resources
- 2 Define permissions for MCP Tools
- 3 RBAC to MCP
- 4 Register MCP Client to connect





Scenario 02: Agents as your consumers

1

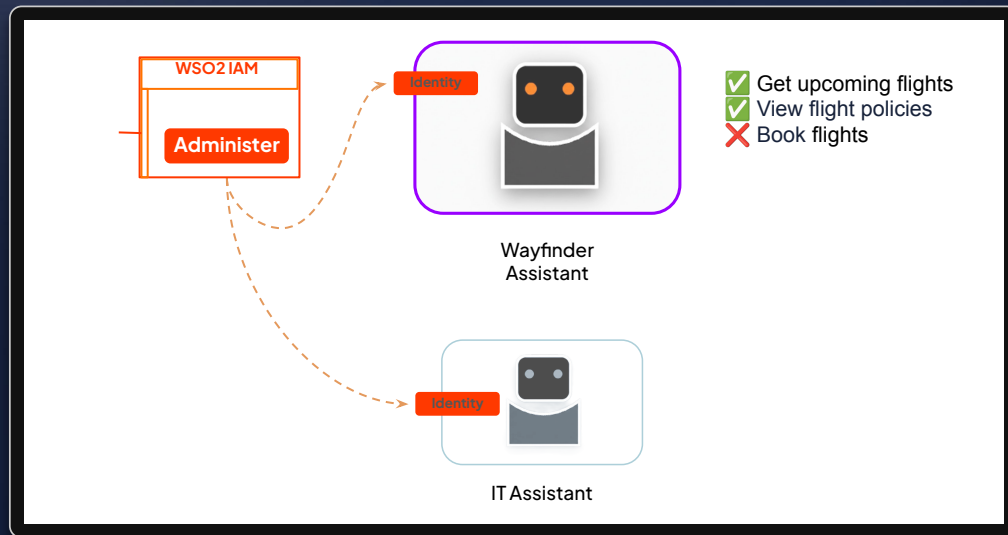
Register Agent and obtain credentials

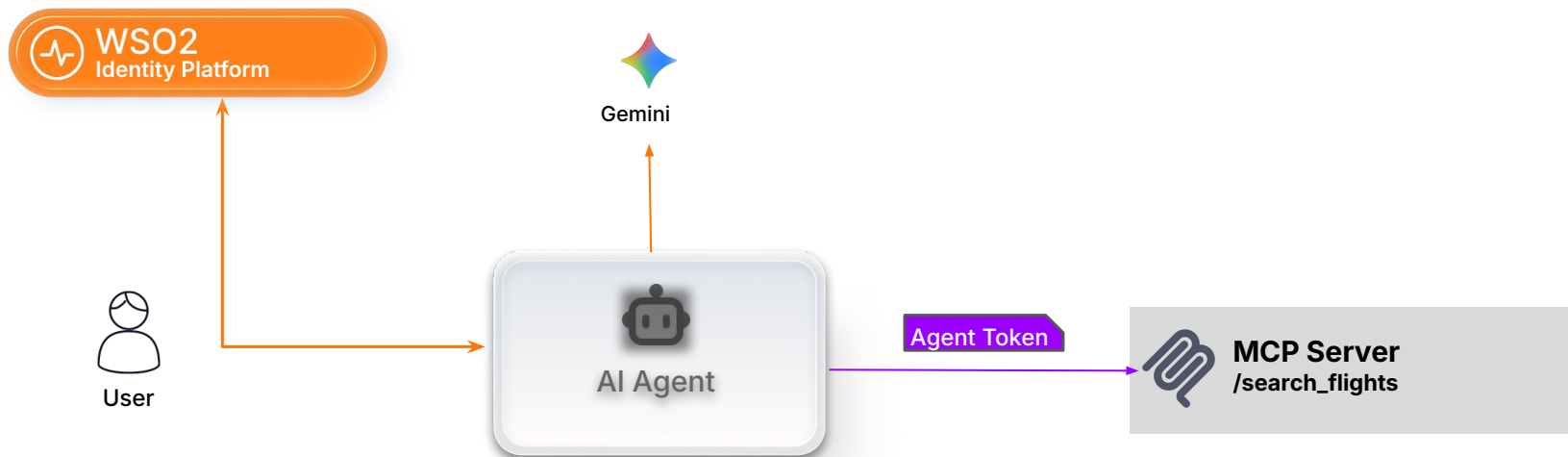
2

Manage attributes and states

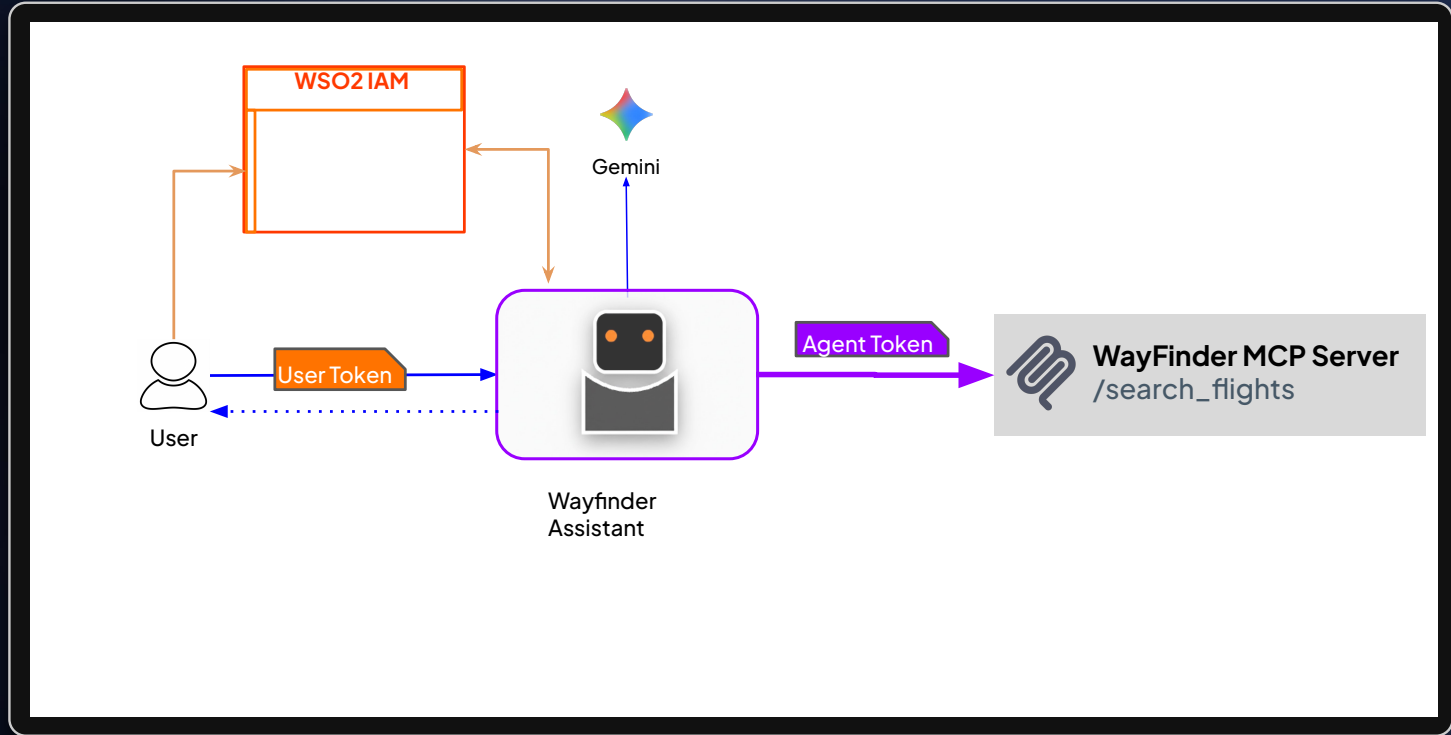
3

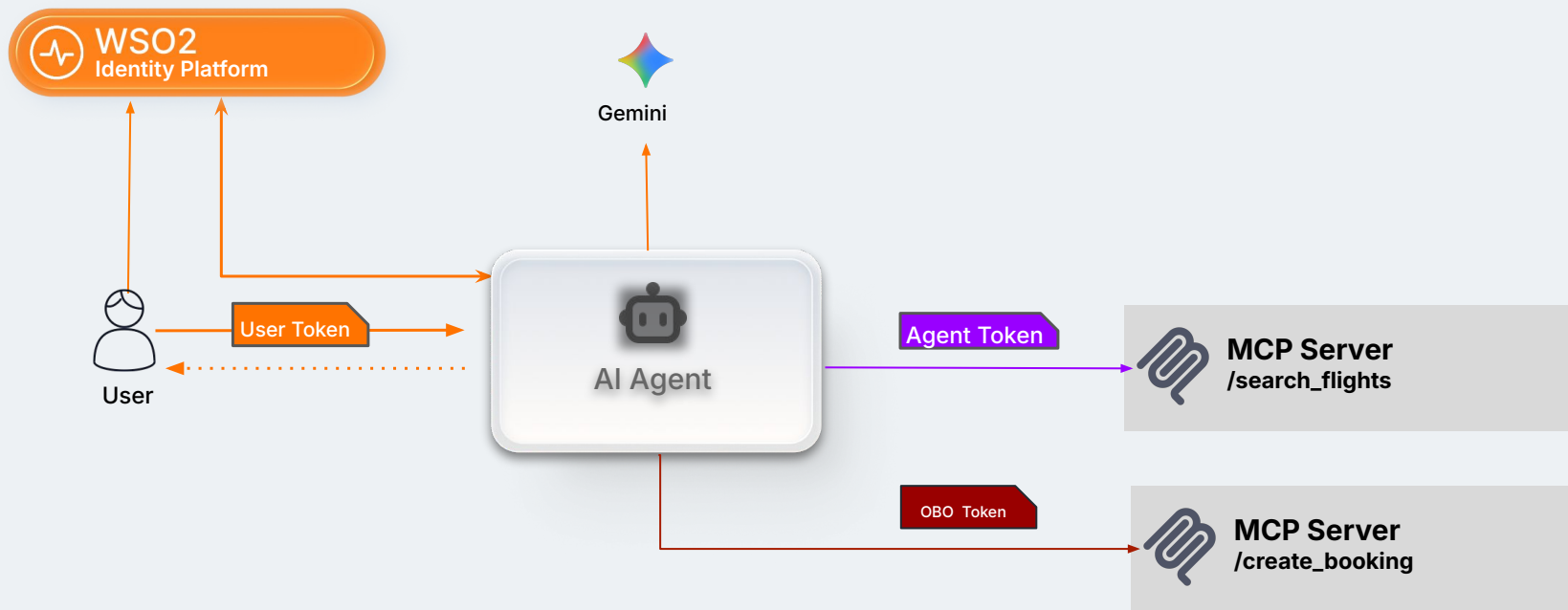
Assign Permissions to act on its own



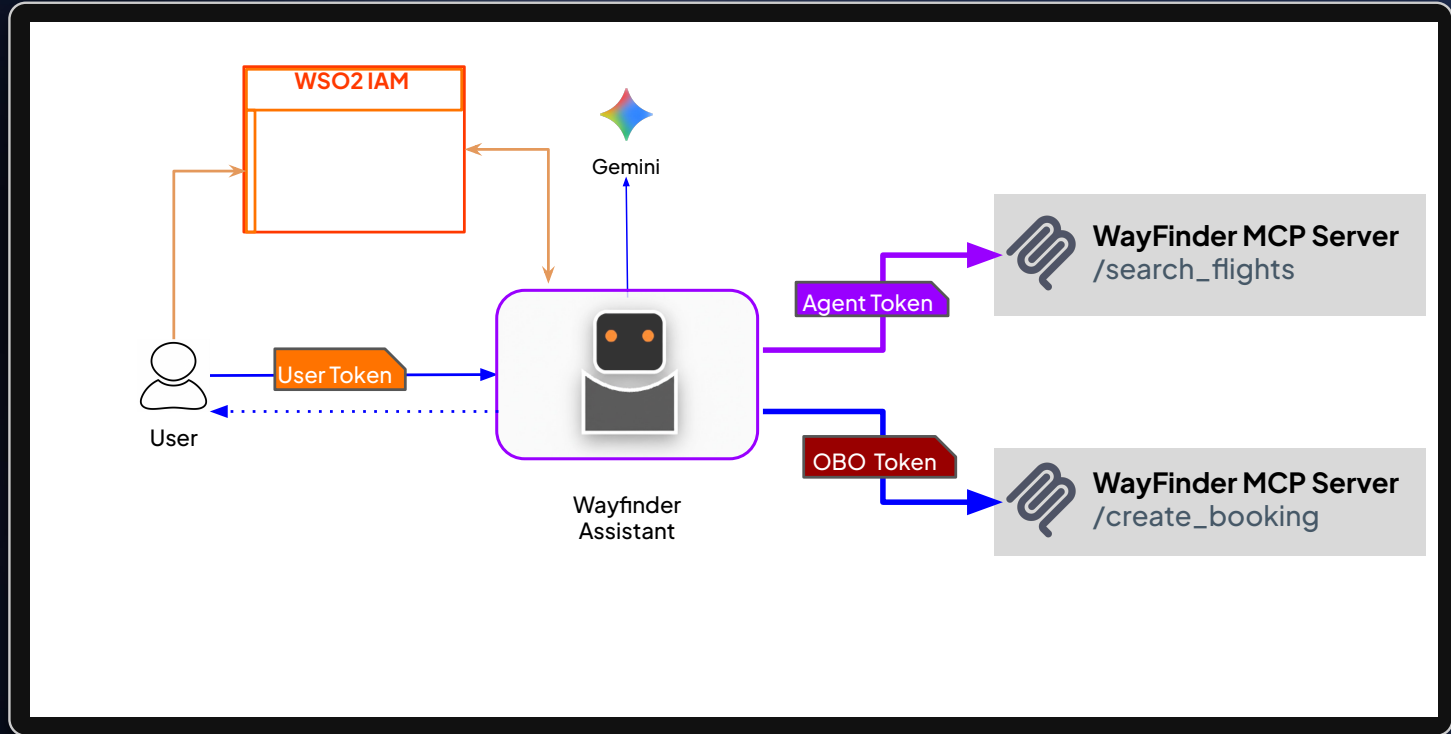


Scenario 03: Agents as your consumers (Interactive Agent)





Scenario 04: User delegated authorization for Agents





Demo

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-2b0d7b3dcb6d",
    "act": {
      "sub": "637653a8-3989-429a-8ba1-3e66cf9235345"
    }
  },
  "azp": "9euHgATTsXbH0EryhnyoEA2r034a",
  "org_id": "f3568aea-64ef-4d70-8527-c90711996d06",
  "scope": "appointment_read appointment_create",
  "authorization_details": [
    {
      "type": "medical_appointment",
      "target": [
        "[target resource]"
      ],
      "intent": "Book one driving licence renewal medical...",
      "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.

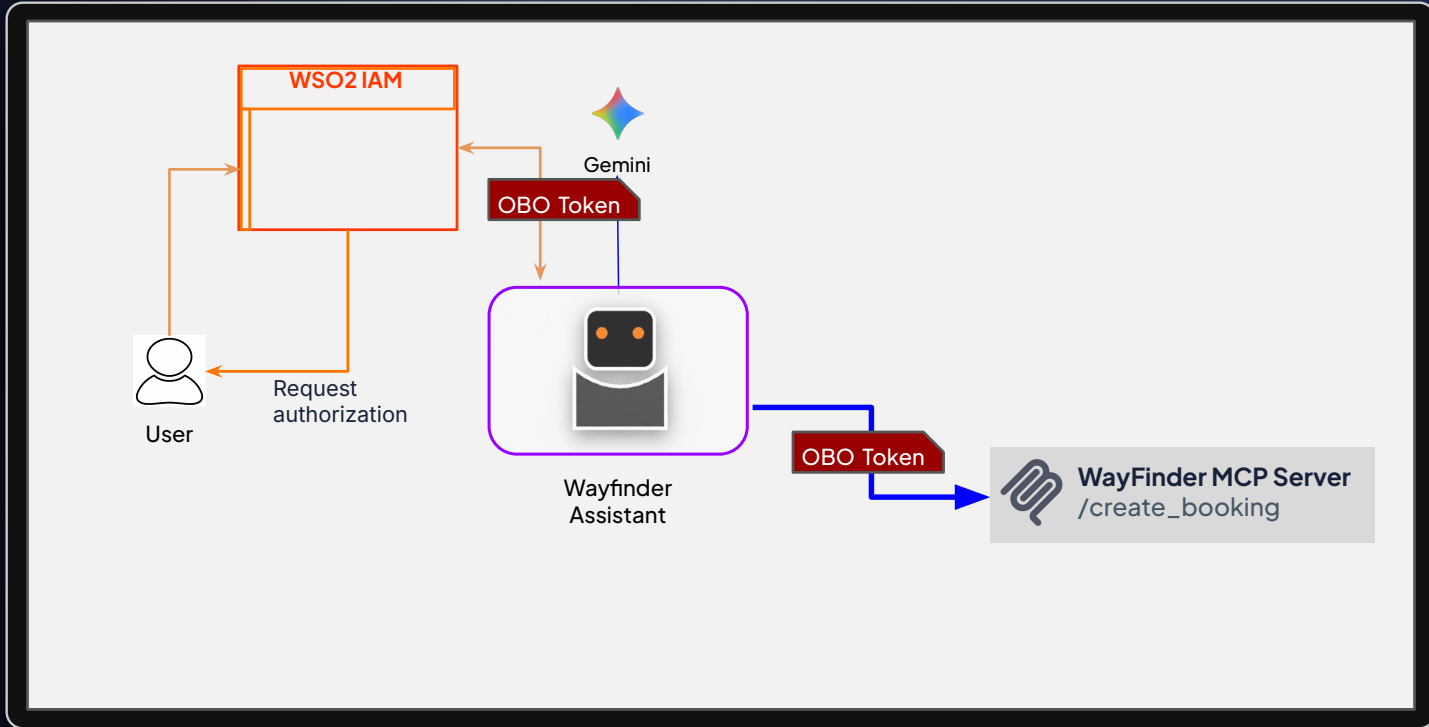


DEMO

Ambient Agents

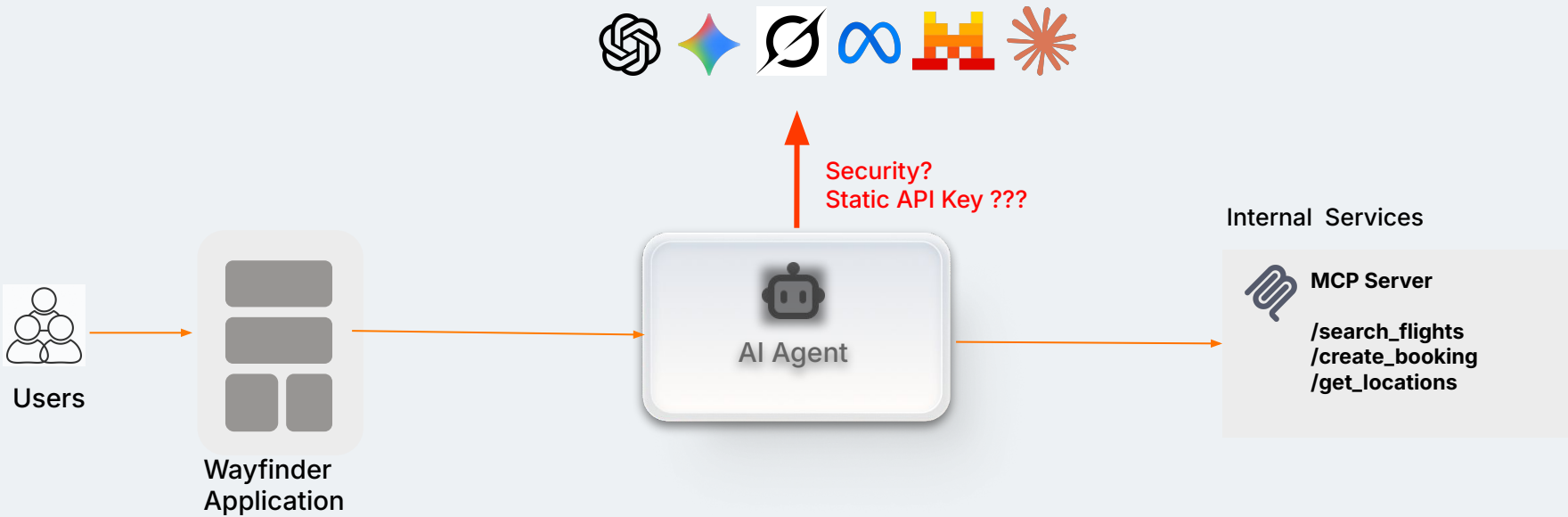
Scenario 05: Ambient Agents

Dynamic human-in-the loop authorization



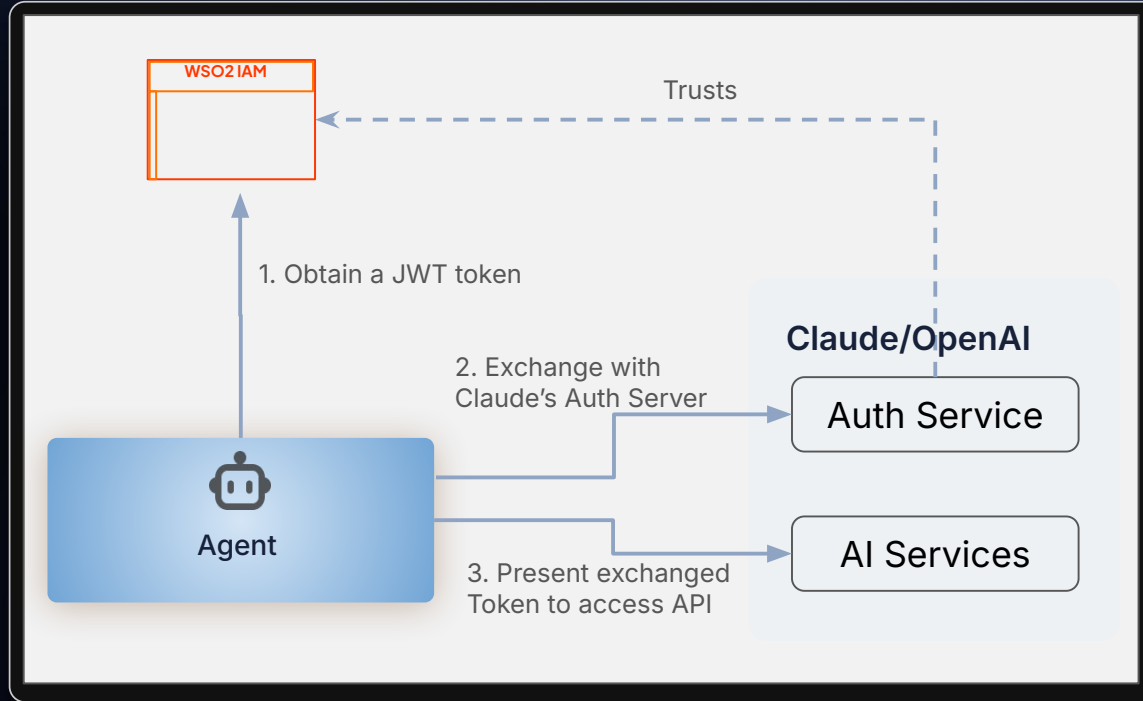


Demo

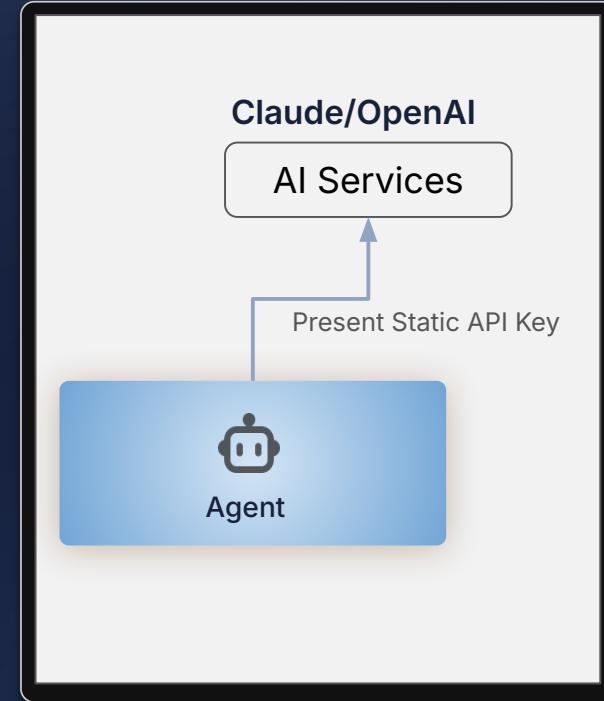


Scenario 06: Model Provider Access with Agent ID

Integrate with Claude/Open AI Workload Identity Federation



Vs.





Demo

Question Time!

WSO2con

AFRICA

SEPT 22 - 24, 2026 | NAIROBI, KENYA

Thank You!



Dulsara Kumarage

Associate Lead - Sales Engineer II



Omindu Rathnaweera

Product Manager - IAM



Ayesha Dissanayaka

Associate Director/Architect - Engineering