



Stop Rebuilding Authorisation

Accelerating AI Agent Development

Toby Allen

Principal Solutions Engineer, Okta | Auth0

Autonomous Agents and Authorization challenges

AI Agents as "Autonomous Colleagues"

Integrating Reasoning & Action

Automate non-routine tasks: LLMs interpret, plan (Planning), and dynamically select tools (APIs) to achieve complex goals.

Scaling beyond system boundaries

Seamlessly executing across multiple SaaS platforms and internal systems to bridge functional silos.

Acting as a "Proxy" for the user

Holding goals and privileges delegated by the user, making independent judgments to scale the user's impact.

! The Challenges

Passing user tokens directly

Giving full user privileges to AI creates an "impersonation" state where the AI acts as the user without knowing what actually required for the task.

Structural limits of static scopes

Scopes like *drive.read* cannot distinguish the task's specific purpose.

An "expense settlement" request might grant access to unrelated confidential files because the scope covers the whole drive.

Chain of damage from persistent privileges

Compromised session tokens or long-lived keys become long-term access routes for attackers if the agent platform is breached.

We handle identity so you can ship faster

Beyond chatbots... Enable high-value agent interactions

Users are increasingly interacting directly with AI agents to get things done

Agentic commerce

offers new ways to transact

Old Way

Product search



Product research



User reviews



Pricing & shipping



Checkout



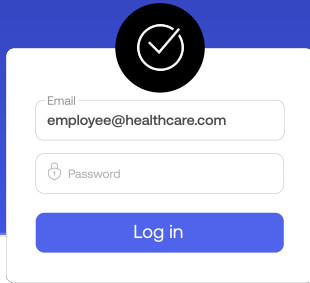
New Way



You need identity to (securely) bring agents to production — **fast**.

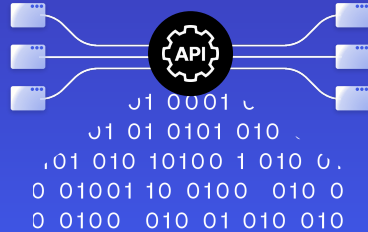
Four auth requirements to build GenAI applications

AI needs to
know who I am



A login form with a black circle containing a white checkmark above it. The form has two input fields: 'Email' with the value 'employee@healthcare.com' and 'Password'. Below the fields is a blue 'Log in' button.

AI needs to
call APIs on
users behalf



AI uses
async interactions



AI data access
must consider
user permissions



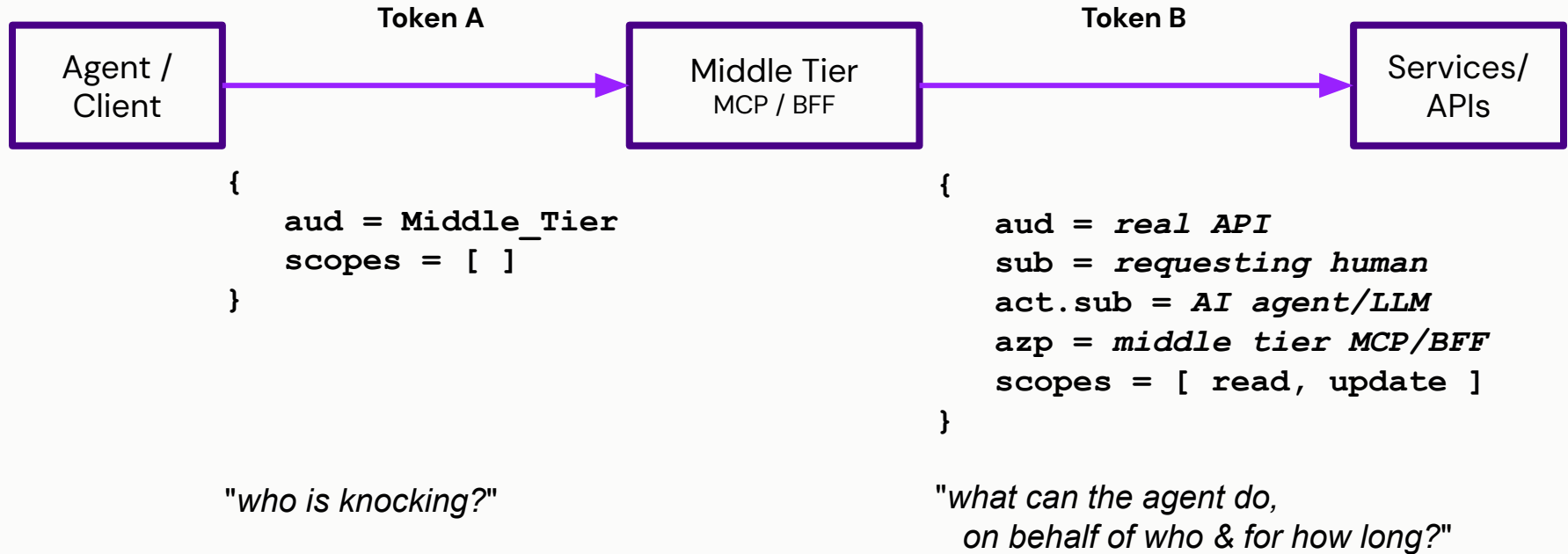
Stop giving agents users' keys

Give them a notarized permission slip (in the form of JWT claims)

Identity	JWT Claim	Question it Answers
The User	sub	Whose data / money is this?
The Agent	act.sub (RFC 8693 actor claim)	Who initiated this action?
The Middle Tier <i>MCP / BFF</i>	azp (authorized party, the issuing client)	Who vouches this exchange is legitimate?

```
{
  "sub":    "auth0|user_abc",           // The human
  "act":    { "sub": "client_external_agent" }, // The calling agent/LLM
  "azp":    "client_mcp_middle_tier",    // The OBO client
  "aud":    "https://.../api/commerce",  // Where
  "scope":  "commerce:write",           // What
  "acr":    "...multi-factor",          // Step up context
  "exp":    1717420800                  // When - for how long
}
```

Agents need **delegated** keys, not borrowed ones



Agentic Commerce

Hifi Online – An agentic shopping experience

