Webinar Housekeeping Rules

How do I ask a question?

If you have technical or content-related question, please use the Q&A window. We will address the question as they come in.

Can I view this presentation after the webinar?

Yes, this presentation is being recorded. A link to the recorded presentation will be sent to the email address you used to register.

The key to autonomous AI agents and MCP servers you can trust

Cisco

Julu Panat, Director of Product Management, Outshift

Cindy Qu, Senior Product Manager, Duo

September 2025

Julu Panat

Director of Product Management

Outshift by Cisco

Cindy Qu

Senior Product Manager

Duo Security

Outshift by Cisco is the **incubation** engine delivering what's next and new for Cisco: **Emerging** technologies that target **adjacent** markets and **personas** to build **meaningful** businesses and achieve innovative results.

outshift by cisco

Focused on driving the Internet of Agents revolution

The Internet of Agents is an open[1], interoperable, internet for

quantum-safe | agent-agent collaboration

[1] An open, interoperable Internet of Agents will drive maximum value for all players: infra builders, operators, app developers, consumers

AGNTCY

A Proud Project of THE LINUX FOUNDATION

An open source project for inter-agent collaboration

The AGNTCY is where we are building the Internet of Agents to be: A diverse, collaborative space to innovate, develop, and maintain software components and services for agentic workflows and multi-agent software.

FORMATIVE PARTNERS

Cisco · Google · Dell · Red Hat · Oracle

75+ collaborating organizations

AG2 · Agency · AGENTOVERLAY · aiplotch · Aisera · ANON · anyscale · Arcfleet · arize · aviz AI for Networks Networks for AI · boomi · Browserbase · ciroos · comet · crewai · Dagger · DUO · Dynamiq · Ema · Fabrix.ai · Galileo · glean · Haize Labs · HUMAN · HYPERBOLIC · Infinitus · Infosys · komodor · LangChain · Letta · Lightning AI · LlamaIndex · Lleverage · Lobby · mem0 · MongoDB. · Mozilla.ai · Naptha AI · NURIX · onetrust · OPAQUE · outshift · patternagentic.ai · Pensar · Permit.io · Persistent · PydanticAI · Redis · SciEncephalon AI · SKREENS · Skyfire · SmythOS · snaplogic · softserve · superbo · traceloop · Tyk.io · ushur · vijil · VOAGENTS · voltagent · Wayfound · weaviate · yaLLMa3 · Yōkai · zep

AGNTCY project donated to Linux Foundation

AGNTCY + THE LINUX FOUNDATION

Why does this matter?

- Neutral governance
- Collaborative system
- Alignment with A2A strategies

What are we contributing?

- Discovery
- Identity
- Messaging
- Observability
- Protocol integration

Why do agents change everything?

Need for an Internet of Agents

Agents have **human-like** attributes and communication needs
but operate at machine **speed** and **scale**

1 discover and identify

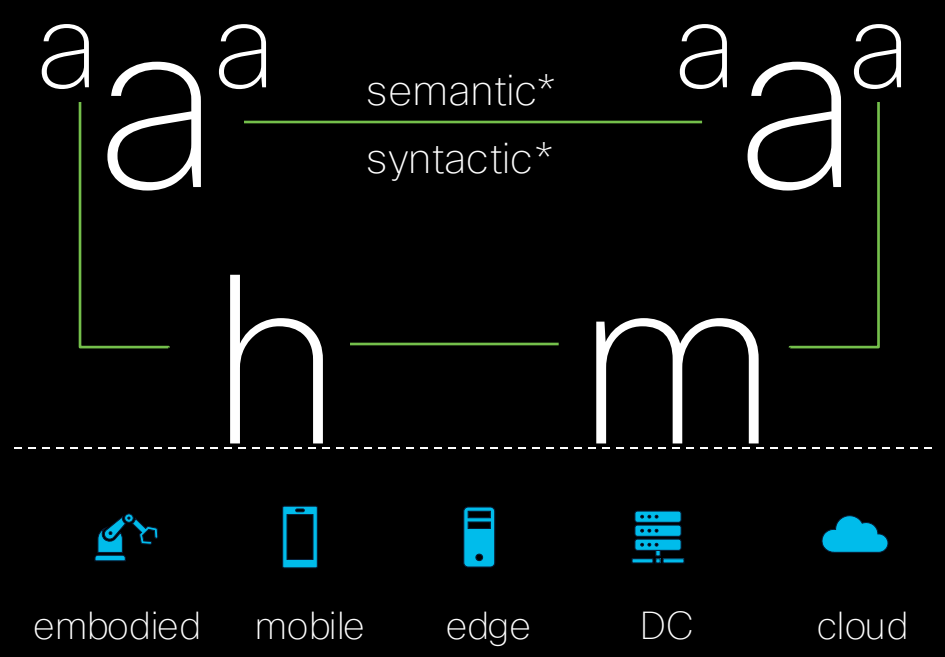
- find agents for specific tasks? are they reputable?
- identify them, give access on my behalf?

2 securely connect

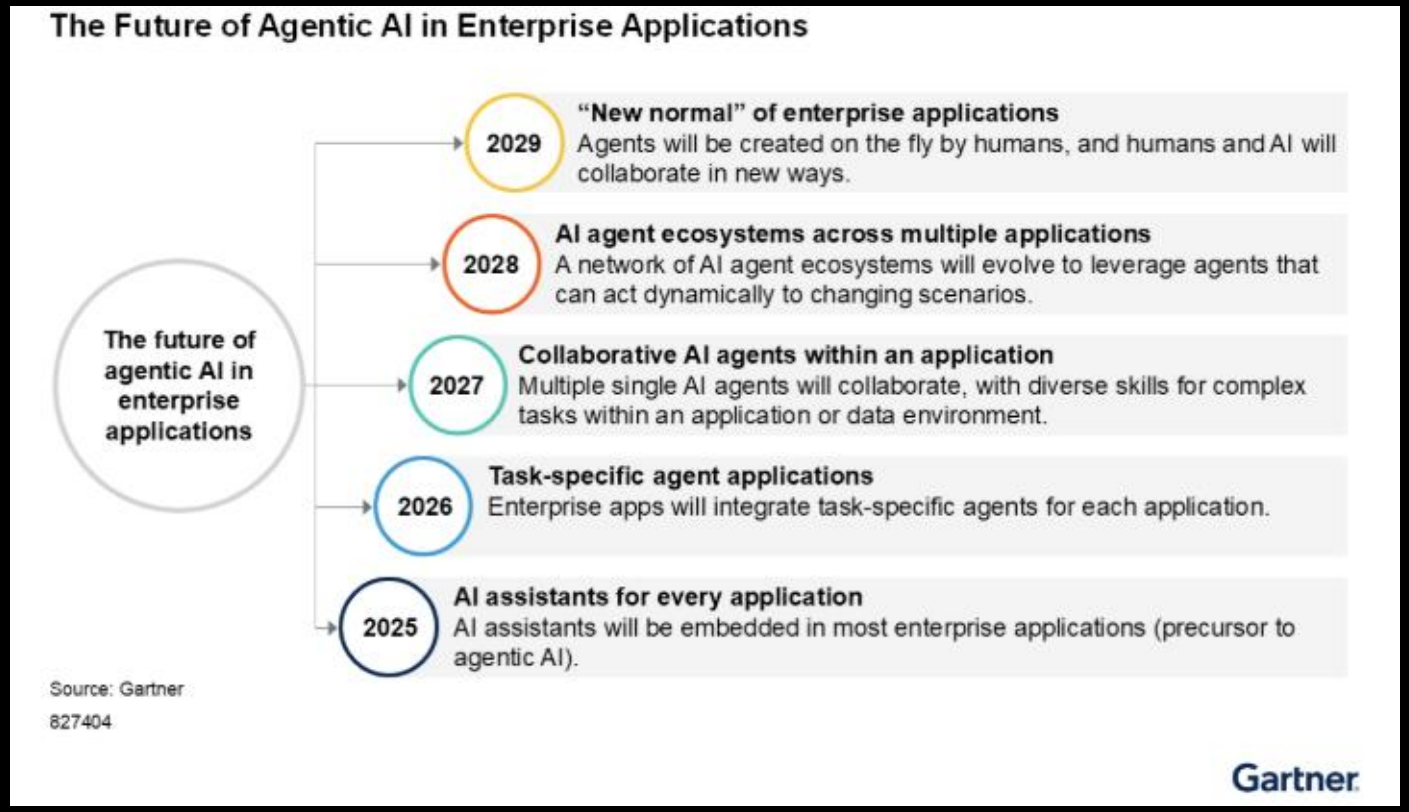
- assemble them to collaborate on the job to be done?
- interpret probabilistic / natural language inputs and outcomes?
- efficiently & securely transfer text-video-image-audio state?

3 observe and evaluate

- doing what they are supposed to do?
- getting into conflicts, loops



Use of task-specific agents projected to grow rapidly



"By 2026, 40% of enterprise apps will be integrated with task-specific agents - up from less than 5%."

– Gartner, *Emerging Tech: The Future of Agentic AI in Enterprise Applications*, 22 July 2025

Where existing Identity and Access Management solutions fall short

Traditional IAM has excelled in human-centric environments

IAM Today is Optimized For:

- Human users and long-running services
- Stable, long-lived credentials
- Organization-bound trust and visibility
- Manual approvals and static roles

But Agents Can Be:

- Ephemeral, autonomous, and fast-spawning
- Tasks span clouds, orgs, and time zones
- Decisions must happen at machine speed
- Identity is no longer just tied to a human

Why RBAC, ABAC, or ReBAC don't work for agentic software

Role-Based Access Control (RBAC)

- ✅ Mirrors organizational structure and hierarchy, intuitive for **humans** and static **services** (e.g., "admin", "viewer")
- ❌ Agents operating with an assigned or inherited role often gain more access than required

Attribute-Based Access Control (ABAC)

- ✅ With more context, the permissions model becomes more flexible and dynamic (e.g., **based on** time, location, **department**)
- ❌ **Complexity** increases with more attributes, making policies harder to manage and audit at agentic scale

Relationship-Based Access Controls (ReBAC)

- ✅ Well-suited for collaborative applications by modeling permissions around **relationships** (e.g., **“Alice is manager of Bob**", "Bob is working with Ted on spreadsheet X")
- ❌ Relies upon a relatively static relationship graph, but agent relationships change with each new assignment

Why traditional IAM approaches have failed with MCP Servers

❓ Lack of Reciprocal Authentication

- In most multi-agent systems, **only clients authenticate** to servers.
- **MCP Servers** lack verifiable, **identities**.
- This creates a **trust asymmetry** in agent-to-agent (A2A) interactions.

🔓 Security Gaps

❌ No proof that an MCP server is legitimate.

❌ No verifiable claim of capabilities or task permissions.

❌ Prone to impersonation or spoofed agent responses.

How can we carry forward the strengths of traditional IAMs to an agentic world?

AGNTCY Agent Identity framework: Overview and demo

Mission for AGNCTY Agent Identity

Evolving Identity and Access Management for agentic services

Agent-native identity with task-, tool-, transaction - based access control (TBAC)

Just-in-Time

Interoperable

Secure

The AGNTCY Identity framework

Trusted identity for secure, accountable, autonomous systems

Assign, verify, and manage cryptographically verifiable identities for **AI Agents (OASF, A2A)**, and **MCP Servers**

Create fine-grained (task-tool based) access control policies

Add human-in-the-loop approvals for sensitive actions

Tap into your trusted Identity Provider – Duo, Okta, Ory, or AGNTCY's built-in decentralized identity provider

Establish trust across **distributed** agentic services

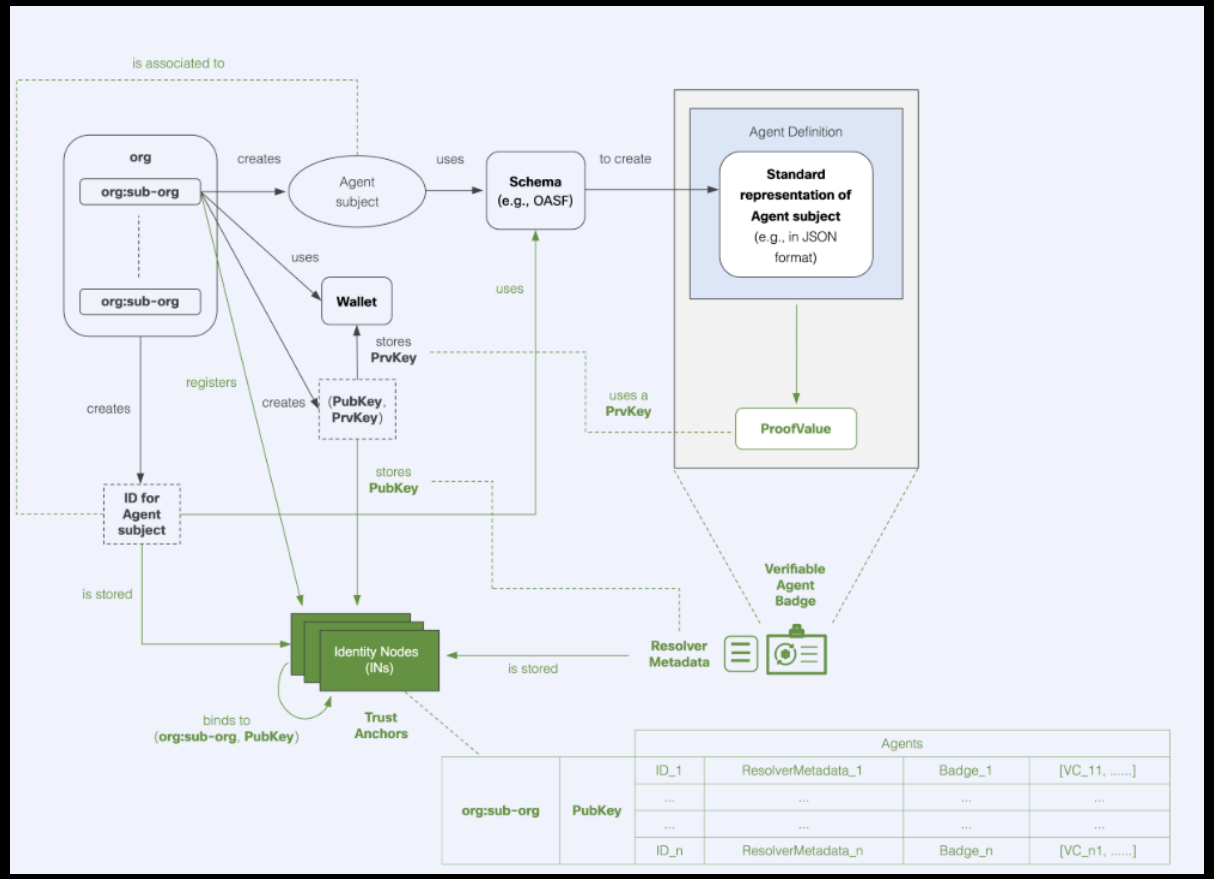
Enforce **fine-grained** access control

Build **interoperable** agentic systems

AGNTCY Identity: The foundation of agent trust

An identity framework that assigns, verifies, and manages credentials for AI agents

1. Assign cryptographically verifiable identity to every agentic service (agent, mas, mcp server)
2. Bind identity to agent registration and MCP onboarding
3. Issue JOSE-signed ID badges with asymmetric key pairs
4. Anchor credentials in a tamper-proof, trusted identity node
5. Enable real-time identity resolution across APIs, clouds, and orgs
6. Support standard IdPs (OIDC supported): Duo, Okta, Microsoft AD, Auth0



TBAC: Granular access controls for agentic software

Evolving RBAC, ABAC, ReBAC in support of AI agents and MCP servers

Tasks

Agents can perform what actions

→ e.g., ability to book a flight

Tools

Agents can access which tools: APIs

e.g., access to book_flight API

Transactions

Agents can execute which specific requests

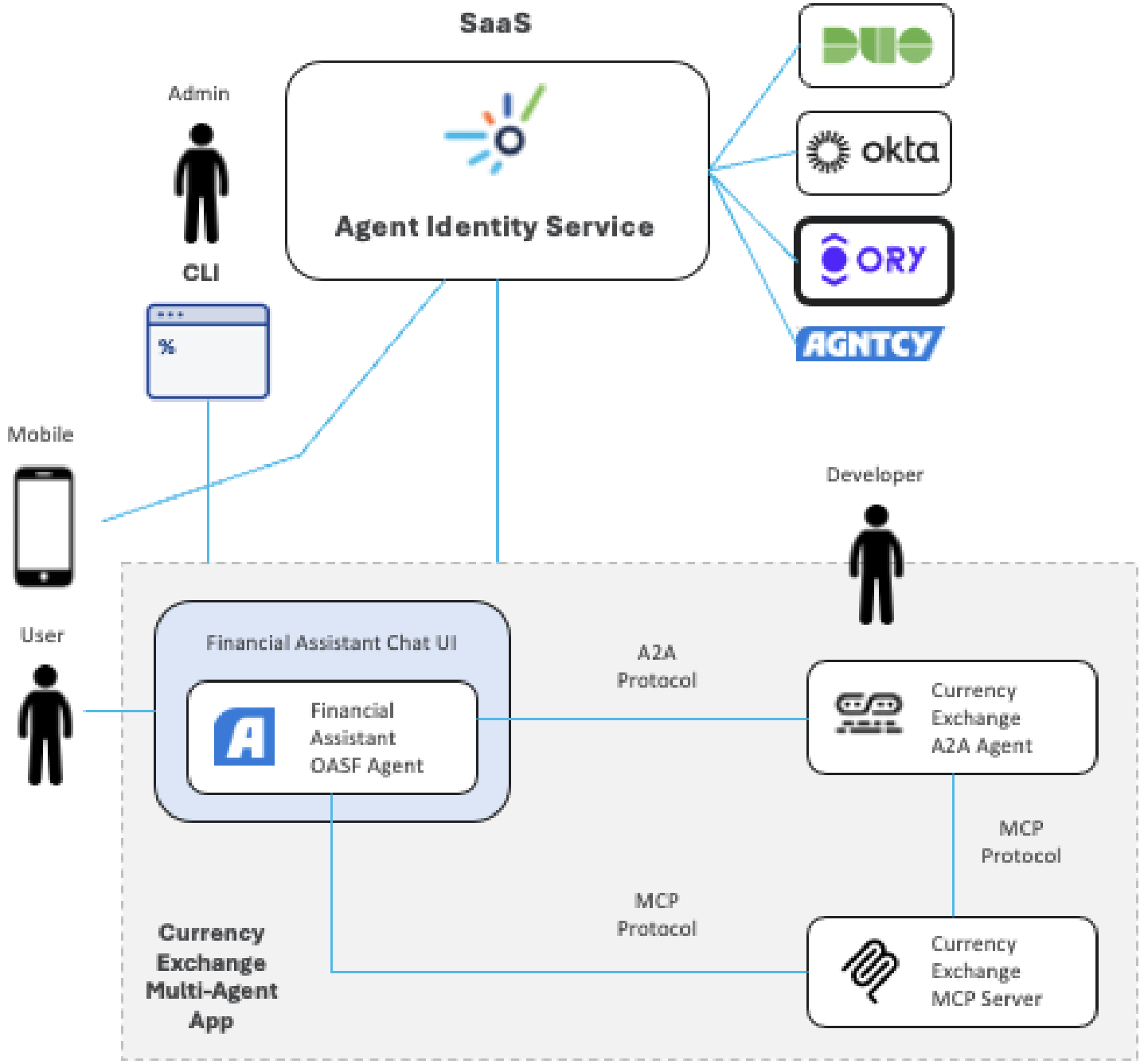
→ e.g., book flight SEA → NYC, 9/11-9/15, <$500

TBAC enables **fine-grained, contextual, and auditable access controls**, ensuring trust, compliance, and security across all AI-driven operations.

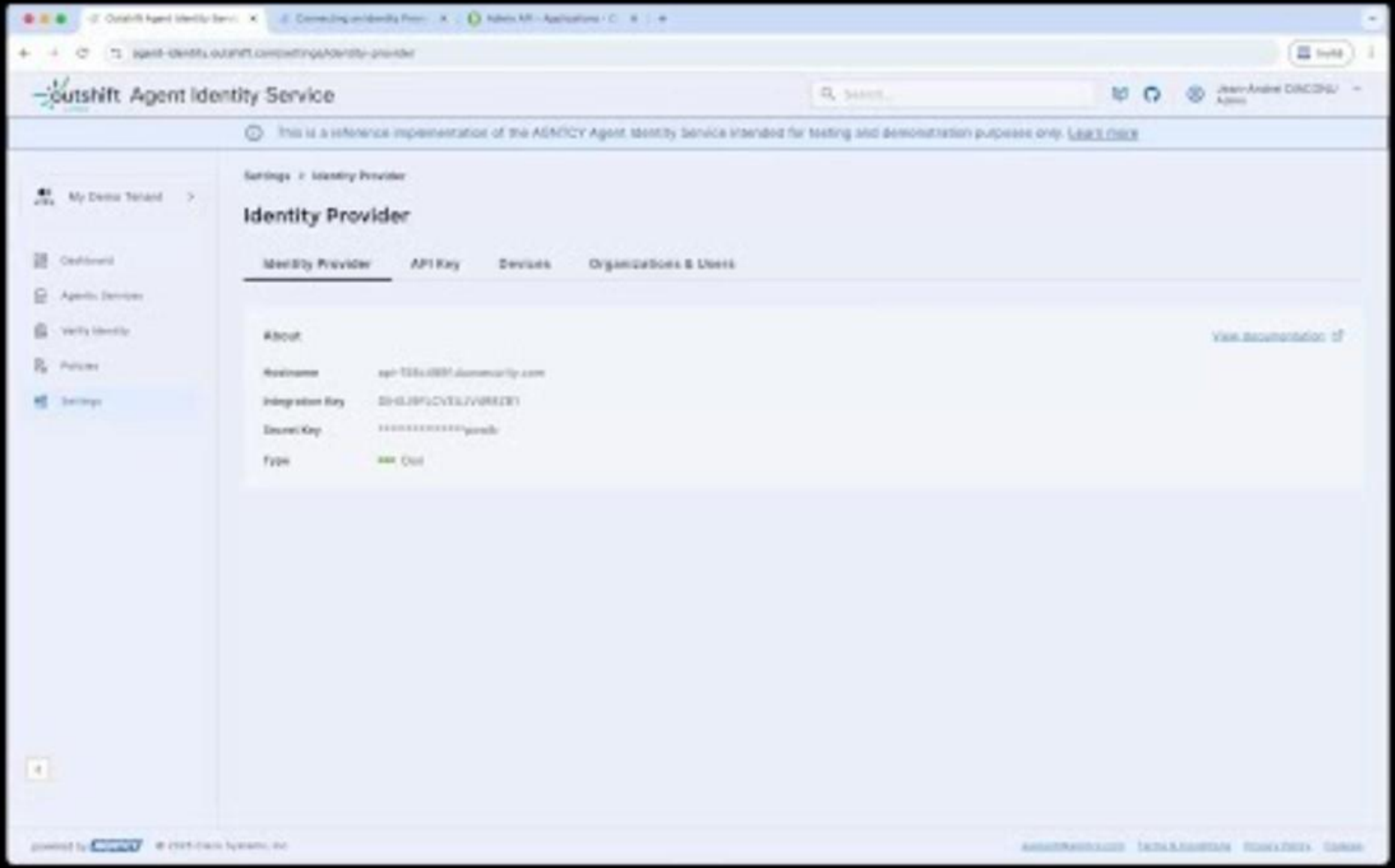
How TBAC addresses traditional IAM challenges

Traditional IAM	TBAC approach
Static and slow	Activated while task is being worked, automatically revoked when task is complete
Organizationally bounded	Identity bound to specific agent instances
Overly permissive	Scoped to minimum necessary tools, limited to specific auditable transactions

Demo Setup



Demo: Configuring an identity provider



Demo: Policy configuration

Demo: Creating policies involving human-in-the-loop

Learn more

Outshift Agent Identity Service

https://agent-identity.outshift.com/welcome

AGNTCY Agent Identity GitHub repository

https://github.com/agntcy/identity

AGNTCY website

https://agntcy.org/

Thank you!

outshift.com ↗ @ outshiftbycisco

outshift.com ↗ @ outshiftbycisco

FAQs

Why SPIFFE/SPIRE Won't Work for Agentic Identity

🧩 **SPIFFE/SPIRE Overview**

- SPIFFE defines workload identity using **X.509 SVIDs**.
- SPIRE issues certs via mutual TLS from a secure workload node.

🚫 **Mismatch with Agentic Needs**

❌ Designed for **infrastructure workloads**, not dynamic agents.
❌ Tied to **trusted control planes and static node environments**.
❌ Doesn't handle **fine-grained, task-level permissions**.

🔍 **Agents Need:**

- **Self-contained, portable identity tokens** (not mTLS chains).
- **Capabilities + policy assertions** (not just who they are).
- **Support for local/ephemeral agents** (not just long-lived services).

Why ANS or X.509 Are Insufficient

❌ ANS (Agent Name Service) Limitations

- ⛔ Provides **discovery**, not **identity attestation**.
- ❌ No support for **task-level permissions or verification**.
- ❌ No built-in authentication or badge structure.

Ref: [OWASP ANS Spec v1.0]

❌ X.509 Certificates Don't Fit

- 📜 Heavy, hierarchical, hard to manage in distributed agent ecosystems.
- ❌ No **task-bound claims or policies** embedded.
- ❌ Poor fit for **short-lived, self-issued identities** (e.g., CLI dev agents).

Why Agents Need Cryptographic Identity — Not Just URLs

✅ Proof > Pointer

- A well-known URL tells you *where* something claims to be.
- A cryptographic identity **proves** *who* or *what* something is, using digital signatures.
- Agents need to **present credentials**, not just show up from a known URL.

✅ Portability

- Autonomous agents may not live at fixed domains — they may run across clouds, edge devices, or org boundaries.
- Cryptographic identity is **location-independent** — an agent can prove its identity anywhere it runs.

. ✅ Tamper-Resistance

- URLs can be spoofed (via DNS poisoning, TLS misconfig, misissued certs).
- A public/private key pair cannot be faked without access to the private key.
- Cryptographic identity gives you **tamper-proof, verifiable bindings** between an agent and its capabilities.

✅ Zero-Trust Security

- Agents often interact without a human in the loop.
- They need to be able to **verify each other directly** — cryptographic identity enables **peer-to-peer authentication** without relying on external DNS or routing.
-

Getting Started

Resources to seed the webinar tab

🔗 Documentation & Dashboard

AGNTCY
- Identity Spec Overview
- Github Repo

Outshift Agent Identity Service (SaaS-UI)
- Agent Identity Web UI
- Docs: Getting Started
- OpenAPI Spec (v1alpha1)
- Currency Exchange Example Video

☕ Explore the CoffeeAGNTCY Reference App

A reference implementation showcasing key Agent Identity features.

CoffeeAGNTCY GitHub Repo

Use the App SDK to experiment or tailor identity flows for your own agents.

App SDK