KNOW YOUR AGENT

Your agent has an identity, just as you do.

Oathera

Every part of what Oathera knows about your agent has a counterpart in how you already know a person. Recorded once, at enrollment, and checked every time the agent acts.

YOUR AGENT — What Oathera records and checks		A PERSON — The same pieces, for someone you know
Identity and role — The person who answers for it, from your identity provider: name, email, groups — *Ada Okafor, engineering*	1	**Name, email, organization, groups** — Who you are and the teams you belong to — *ada@company.com*
Credentials — Its identifier, made from a key created on its own host; its model and version — *Ed25519, version 1.0.0*	2	**Professional credentials and skills** — Your qualifications and what you are trained in — *Software engineer*
Capabilities — What it says it does, and the access it asks for — *report-generation, data-analysis*	3	**What you can do** — Your permissions and responsibilities — *Write code, manage projects*
AI and platform — Its model, AI providers and AI models, platform and operating system — *Linux*	4	**Your device and software** — The laptop and applications you work with — *MacBook Pro, macOS*
Host — The machine it runs on: hostname, CPU, memory, network cards, held as one digest — *host digest MYQAQXgb9kC3hqXx*	5	**Your device and location** — Where you sign in from, and on what — *Home Wi-Fi, New York*
Process and runtime — The running agent, its user and its code, seen from the operating system by the Oathera Witness	6	**Your activity and session** — What you are doing, and since when — *Signed in at 10:24*
Code integrity — Hashes of the code it runs, so a change is noticed	7	**Identity documents and checks** — The documents that prove you are who you say — *Driver's license, background check*
Container and infrastructure — Docker, Kubernetes or Podman, when it runs in one	8	**Workplace** — The office or site where you work — *Office, remote*
Cloud and hosting — Its cloud and instance, with a signed platform attestation where the cloud gives one	9	**Where you live** — Your address and the laws you live under — *California, US*
Organization and sponsorship — The organization behind it: legal name, entity type, jurisdiction	10	**Your employer or sponsor** — The company that vouches for you — *Acme Corp*
Risk and trust — Findings about its host, how confident Oathera is, and whether it is revoked — *host confidence 3, unattested host*	11	**Credit, security and compliance** — Your record, your clearance, your standing — *Security clearance*
One of a kind — Key and host together: its fingerprint on every call. A copy elsewhere leaves a different one.	12	**Biometrics** — Your face and your fingerprints: no one else has them

Oathera Agent Enrollment
On your MCP server. Records the agent once, with the person who answers for it.

Oathera Identity Service
Oathera's cloud. Holds the record, and checks the host at every token.

Oathera Agent Enforcement
On your MCP server. Checks the fingerprint on every call.

Oathera Witness
On the agent's host. Vouches for what runs there.

Examples are from an Oathera demo agent; Ada Okafor is a demo user.

Oathera. Every AI agent, sworn in.