

The Agentic Standards *Landscape*

AI agents are software that can take actions for a person (booking, buying, filing, scheduling), not just answer questions. For that to work efficiently and safely, agents need shared rules for how they **find each other**, **prove who they are**, **talk to one another**, and **pay**. This is a plain-language map of who is writing those rules: standards development organizations, the major companies, and the U.S. government. It is a starting point, not a complete list.

01 — THE SHARED FOUNDATION

The Linux Foundation & the *AAIF*

The **Linux Foundation**, the long-standing nonprofit that hosts neutral, shared technology like Linux itself, has become the common home for the building blocks of AI agents. In December 2025 it created the **Agentic AI Foundation (AAIF)** to keep these owned by no single company. Founded by **Anthropic, Block, and OpenAI**, with Amazon, Bloomberg, Cloudflare, Google, and Microsoft also at the top tier. Membership has grown to roughly **190 organizations**, now including government agencies and universities. The four building blocks it stewards:

MCP	Anthropic's standard for letting an agent plug into outside tools and data (a calendar, a database, a service), like a universal adapter. The most widely adopted piece.
A2A	Google-created standard for letting agents from different companies talk to and hand off work to each other. Now at version 1.0; IBM folded its rival effort into it.
AGENTS.md	An OpenAI-contributed, plain-text way to give coding agents consistent instructions for a project.
goose	A free, open starter kit from Block (the Square/Cash App company) for building working agents.

02 OPEN TECHNICAL STANDARDS GROUPS

W3C — AI Agent Protocol Group VOLUNTEER-LED ACTIVE

The W3C sets the open standards behind the web. This volunteer group (~180 participants from industry and academia) is drafting shared rules for how agents find and safely work with one another online. Early drafts since Aug 2025. w3.org/community/agentprotocol

W3C — WebMCP GOOGLE + MICROSOFT EARLY TESTING

A proposed web standard, led by Google and Microsoft, that lets an ordinary website offer an agent a safe, structured way to act on it (e.g. "book this appointment") instead of the agent clicking around blindly. In early testing in Google Chrome.
github.com/webmachinelearning/webmcp

IETF — Agent Identity Work IETF DRAFT

The IETF writes the core plumbing standards of the internet. Its working drafts tackle the hard question of giving each agent a verifiable identity and limiting what it's allowed to do on a person's behalf. Contributors include Amazon, OpenAI, and security firms. datatracker.ietf.org · [agent identity draft](#)

OpenID Foundation — AI Identity Group OPENID FOUNDATION ACTIVE

The group behind the "Sign in with..." login standards used across the web. It is working to extend proven identity and permission rules to AI agents, so the same trusted login plumbing covers agents acting for users. openid.net · [AI Identity group](#)

03 U.S. GOVERNMENT

NIST — AI Agent Standards Initiative NIST / CAISI FEDERAL

Launched Feb 17, 2026 by NIST's Center for AI Standards and Innovation, among the first U.S. efforts focused on agents working together safely. Three aims: support industry-led standards and U.S. leadership abroad, back the open building blocks above, and research agent identity and security. nist.gov/caisi/ai-agent-standards-initiative

CAISI — Request for Input on Agent Security NIST / CAISI

CLOSED MAR 9
A formal call for industry comment on keeping agent systems secure (comments closed Mar 9, 2026), alongside listening sessions in finance, healthcare, and education. *AFI filed a response.*

NIST NCCoE — Agent Identity Project NIST / NCCOE CLOSED APR 2

A hands-on NIST lab effort (comments closed Apr 2, 2026) on how to verify an agent's identity and control its permissions, the most concrete, build-it-and-test-it government work so far.

04 INDUSTRY CONVENERS

Advanced AI Society INDUSTRY GROUP CONVENING

A neutral group that gathers the various technical teams to compare notes and agree on shared priorities (agent identity, how agents discover each other, and trustworthy payments) so efforts don't fragment. luma.com · [standards convening](#)

MCP / Agent Dev Summits AAIF RECURRING

The recurring industry conferences where the people building these standards meet. Run under the AAIF, with events across North America and Europe through 2026.

05 SHOPPING & PAYMENTS — THE FASTEST-MOVING AREA

LETTING AGENTS SHOP & CHECK OUT

ACP — Agentic Commerce Protocol

From OpenAI and Stripe. Powers buying inside ChatGPT. Used by Etsy, Shopify, PayPal, Salesforce. OpenAI has since shifted focus from in-chat checkout toward product discovery and merchant-controlled purchasing.

UCP — Universal Commerce Protocol

Google's version, for agents to browse store catalogs and check out. Partners include Walmart, Target, Shopify, and Etsy.

MAKING AGENT PAYMENTS TRUSTWORTHY

AP2 — Agent Payments Protocol

Google-led, works with any payment type. Creates a tamper-proof record proving the agent had the user's OK to buy. Backed by Mastercard, PayPal, and American Express.

Visa — Intelligent Commerce

Visa's program to let agents pay safely, with spending limits and fraud checks built for purchases a person isn't clicking through themselves. Includes its "Trusted Agent" rules (Oct 2025).

Mastercard — Agent Pay

Mastercard's equivalent (launched Apr 2025): verified agents, set spending limits, and proof the user consented. Live in several countries.

STORES, WALLETS & "KNOW YOUR AGENT"

x402

An open standard for agent payments on the web. Started by Coinbase, now governed by the Linux Foundation.

Retailers' own agents

Walmart's *Sparky* now appears inside ChatGPT and Gemini; Amazon and Instacart have their own. Big stores increasingly want shoppers using *their* agent, not a platform's checkout.

Underneath all of this sits "*Know Your Agent*": verifying an agent is legitimate and authorized, the way banks verify customers. This is the layer most directly tied to AFI's policy work.

06 THE BIG PICTURE

These pieces fit together rather than compete. An agent uses **MCP** to reach tools and data, **A2A** to coordinate with other agents, **identity standards** (IETF, OpenID, "Know Your Agent") to prove who it is and what it's allowed to do, and the **shopping and payment standards** to buy on a person's behalf. The **Linux Foundation / AAIF, W3C, IETF, and OpenID** keep the rules open and shared, while **NIST** anchors the U.S. government's role. The central policy questions (identity, consent, security, accountability) cut across every layer.