Agentic AI: A Rising Realm

A C2PA Ecosystem Perspective

July 2025

Prepared by

Makki Elfatih, Hkdolts

Leonard Rosenthol, Adobe

Karen Kilroy, NYX Code

Content

Why is Agentic AI Unique?

A Forward Looking Definition of Agentic AI

An MIT Media Lab Definition of Agentic AI:

Agentic AI refers to artificial intelligence systems that exhibit autonomous goal-directed behavior, capable of perceiving, reasoning, and acting on behalf of users or organizations within defined boundaries and with varying degrees of delegated authority.

We are shifting quite rapidly beyond a rule-based execution which means..

1 More Autonomy

Seamless performance of activities supported by persistent memory and reasoning (with or without instructions), including self-correction mechanisms

2 Multi-Agent Coordination

More capabilities to deploy teams of agents to collaborate, as well as the ability to deploy super agents to oversee large teams and complex workflows

3 Endless Integrations

And with possibilities to execute API Driven actions where agents can manipulate tools (e.g., databases, browsers and SaaS apps) to execute tasks.

How Does Emerging Communication Protocols Augment Agentic AI?

Interoperability with Agentic AI Communication Protocols

To achieve the desired scalability in process and task automation, Agentic AI need to interoperate with communication protocols that can at a minimum:

- **Act as a Reliable Plug:** Connecting Agents with platforms, to fetch needed assertions, perform actions, and collate and exchange required information between Agents
- **Enable Secure Navigation:** Of tools, programs and interfaces by ensuring robust cryptographic mechanisms are embraced in the communication and exchange processes
- **Supply Audit Trails:** To provide the necessary level of assurance to concerned stakeholders that due process has been exercised and actions are being monitored against adopted frameworks (for e.g. NIST AI RMF) and regulatory requirements (for e.g. California AI Transparency Act SB 942), if any
- **Present Feedback and Reporting:** Combined with timely analytics and calls to action, especially in case of vulnerabilities, including pentretation threats to data and content

Agentic AI Communication Enabling Protocols

There are a number of prominent and rapidly emerging communication protocols with varying mandates and capabilities to enable the operation of **Agentic AI systems** or the "**Internet of Agents**", including:

- **Model Context Protocol (MCP):** Leverages JSON-RPC* 2.0 message format to deliver rapid data retrieval; acts as an interface between Agentic AI systems, including LLMs, and other systems, and platforms in exchanging and communicating messages and executing actions.

- **Agent to Agent Protocol (A2A):** is designed to standardize communication between AI agents, particularly for those which are deployed in external systems. Previously, such protocols were established for Tools called Model Context Protocol (MCP) which is an emerging standard to connect LLMs with data and resources, as documented by Google Codelabs

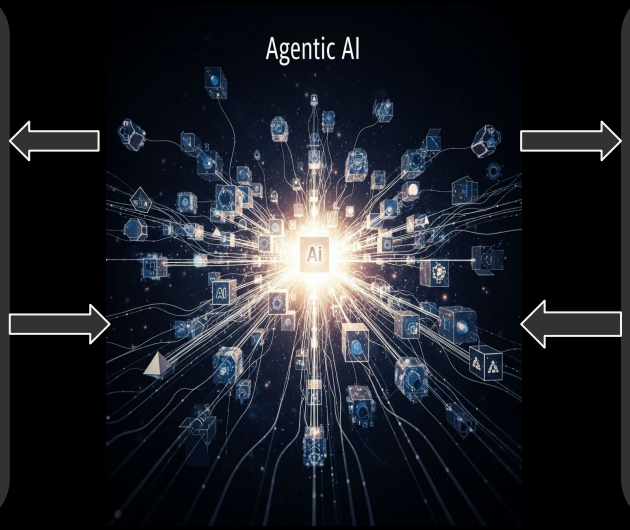
**** A Remote Procedure Call (RPC) is a request-response protocol. An RPC is initiated by the client, which sends a request message to a known remote server to execute a specified procedure with supplied parameters. The remote server sends a response to the client, and the application continues its process.***

MCP, Agentic AI and A2A Protocol in Action

Agentic AI operates as a system comprising of many Individual Agents who can operate asynchronously to execute upon the objectives they were programmed and recruited for. MCP operates as an interface with data retrieval and action fulfillment capabilities for Individual Agents requests. The A2A Protocol, on the other hand, supports two way communication and cross-Agentic AI system teaming and collaboration.

MCP

1. **Initiate / Schedule Request:** using an LLM **(**e.g., Claude) to a remote MCP server (e.g., data retrieval)
2. **Send Request:** the LLM (as MCP client) sends a JSON-RPC request to the MCP server.
3. **Return Results:** MCP processes the task and returns results
4. **Use Results:** to complete the task or make further requests



A2A Protocol

1. **Agent Discovery:** Agents find each other.
2. **Negotiation:** Agents agree on modalities/tasks.
3. **Black Box Communication:** Agents communicate directly, keeping internals private.
4. **Collaboration:** Agents work together on complex tasks.

Who is Currently Advancing Agentic AI Specifications?

A Glimpse into Some of the Leading Agentic AI Specifications

Communications & IPC

- MCP
- ACP
- ANP
- ACP (AGTNCY)
- ACP (IBM)

Authentication

- Of the Agent:
  - Web-bot-auth (IETF, from Cloudflare)
  - Agent Protocol (W3C CG)
- On behalf of (OBO)...users & other agents

Authorization*

- AAuth - Agentic Authorization OAuth 2.1 Extension
- OAuth2.0 Extention for AI Agent: Authorization on Target
- OAuth 2.0 Extension: On-Behalf-Of User Authorization for AI Agents
- Agent Protocol (W3C CG)

*** For further considerations on AI Agent Authentication and Authorization:** https://datatracker.ietf.org/doc/draft-yao-agent-auth-considerations/

*** Other Key Aspects:**

- Data and Process Access Rights
- Financial Authority on Purchasing and Payments Processing Activities
- Limits of Delegation of Authority

A Glimpse into Some of the Leading Agentic AI Specifications

Identity

- **Of the agent/workflow**
  - **Agent Protocol (W3C CG)**
  - **SPIFFE (open source)**
- **Networked Agents And Decentralized AI (NANDA):**
  - Unlocks possibilities for **Internet of AI Agents**
  - **Provides Critical infrastructure** for distributed agent intelligence at scale

Where Can Agentic AI meet the C2PA Ecosystem, including CAWG?

Where can Agentic AI meet the C2PA Ecosystem, including CAWG?

The C2PA develops and promotes open standards for digital content provenance to ensure authenticity, transparency, and global adoption across media and platforms. By defining best practices while maintaining content accessibility, it enables new possibilities to interoperate with Agentic AI, including the following:

Action Tracking

Agents can validate modifications to verified action records to the C2PA manifest, ensuring end-to-end traceability.

Agent Cards

Embedded in a medium an Agentic Card can be used to declare its scope & that it won't alter semantic content or violate C2PA integrity.

Rights & Restrictions*

A publishing agent denies re-upload of an article on a commercial platform if the manifest restricts commercial reuse

Micro Payments*

A user reposting licensed content triggers a payment to the rights holder, with the action logged into the content's updated manifest

**** Potential area for collaboration between C2PA and JPEG Trust***

Where can Agentic AI meet the C2PA Ecosystem, including CAWG?

The CAWG builds on the C2PA's foundation by defining enriched assertions for **individual and organizational** creators to express intent and authorship. As Agentic AI evolves, it must also define Agentic Identity to support AI agents acting on behalf of creators. These use cases are proposed to reflect this need:

Of the Agent...

An instance where an AI Agent represents a human in asserting identity claims under a delegated authority construct

Of the "OBO" Actor

Of the "OBO" Actor relates to cases where an Agent asserts identity claims OBO of an Agent's Agent i.e. the Agent's Agent is a Principal

Integrity Inspector

Agentic AI reviews identity and creator assertions after publication and flags anomalies, mismatches, or missing identity elements

Context Recommender

When viewing or developing content, Agentic AI suggests contextual metadata about creators based on prior public assertions

Now how did we come to Agentic AI?

Human aspiration and ingenuity to create innovative tools and methods to advance the way work activities and consumer products and services are created and delivered is really what brought us here today.

Thank you