

Jun 30, 2025

Model Context Protocol (MCP)

DOI

<https://dx.doi.org/10.17504/protocols.io.3byl46ebzgo5/v1>

Paola Di Maio¹

¹CSKRNS

Human Cell Atlas Metho...

Bio Neuromod



Paola Di Maio

CSKRNS

Create & collaborate more with a free account

Edit and publish protocols, collaborate in communities, share insights through comments, and track progress with run records.

Create free account

OPEN  ACCESS



DOI: <https://dx.doi.org/10.17504/protocols.io.3byl46ebzgo5/v1>

Protocol Citation: Paola Di Maio 2025. Model Context Protocol (MCP) . protocols.io

<https://dx.doi.org/10.17504/protocols.io.3byl46ebzgo5/v1>

License: This is an open access protocol distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited



Protocol status: Working

We use this protocol and it's working

Created: June 30, 2025

Last Modified: June 30, 2025

Protocol Integer ID: 221289

Keywords: AI, agents, protocols, model context protocol, mcp, protocol, standardized open protocol, managing context, secure interaction, context across session, secure interaction between ai model, model

Abstract

The Model Context Protocol (MCP) is a standardized open protocol designed to enable seamless, secure interaction between AI models and external tools, resources, and systems by managing context across sessions.

Guidelines

Review and test on a case by case basis

- 1 Server Creation Phase ○ Establish MCP servers that expose Tools (functions callable by AI models), Resources (data endpoints), and Prompts (templates guiding tool usage). ○ Register these components with standardized metadata to enable discovery and invocation by clients. ○ Set up secure communication channels and authentication mechanisms to protect resources. (This phase initializes the MCP server lifecycle and prepares it for operation) .
- 2 Client-Server Communication and Session Establishment ● MCP clients (embedded within AI applications or hosts) initiate connections to MCP servers using a defined client-server architecture. ● Clients negotiate capabilities and maintain stateful sessions to preserve context across multiple interactions. ● Communication uses structured JSON-RPC messages over secure transport protocols, ensuring integrity and confidentiality .
- 3 Authentication and Authorization ● Implement user authentication to verify human users (e.g., via OAuth 2.1 with PKCE). ● Authorize AI clients to access specific tools/resources on behalf of users, enforcing fine-grained access control. ● Use well-defined OAuth endpoints (/authorize, /token, and discovery URLs) to manage secure token exchange and session validation .
- 4 Tool Invocation and Context Management ● AI models invoke registered tools via JSON-RPC calls, passing relevant context and parameters. ● MCP servers execute the requested tools and return structured results or error messages. ● Context is managed incrementally, allowing persistent memory and continuity across agent actions, addressing the “disconnected models” problem in AI systems .
- 5 Server Operation and Update Phase ● MCP servers continuously operate, handling multiple client requests, managing sessions, and monitoring security. ● Servers support dynamic updates, including adding/removing tools, updating prompts, and refining security policies without disrupting ongoing sessions. ● Security and privacy risks are actively mitigated through monitoring and protocol enhancements .
- 6 Ecosystem Integration and Extension ● MCP supports integration with diverse AI models, multi-agent systems, and external platforms, enabling interoperability and scalability. ● Extensions include support for streaming responses, multi-modal data, and advanced coordination among agents



Protocol references

Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025). Model Context Protocol (MCP): Landscape, Security Threats, and Future Research Directions. arXiv preprint arXiv:2503.23278. <https://doi.org/10.48550/arXiv.2503.23278>

Krishnan, N. (2025). Advancing Multi-Agent Systems Through Model Context Protocol: Architecture, Implementation, and Applications. arXiv preprint arXiv:2504.21030.

Philschmid. (2025, April 3). Model Context Protocol (MCP) an overview. <https://www.philschmid.de/mcp-introduction>

●oecc, A. (2025, May 20). Model Context Protocol: Landscape, Security Threats, and Future. LinkedIn. <https://www.linkedin.com/pulse/model-context-protocol-landscape-security-threats-6-amit-yoecc>