

Agent Tools & Interoperability with MCP

Authors: Mike Styer, Kanchana Patlolla,
Madhuranjan Mohan, and Sal Diaz



Acknowledgements

Content contributors

Antony Arul

Ruben Gonzalez

Che Liu

Kimberly Milam

Anant Nawalgaria

Geir Sjurseth

Curators and editors

Anant Nawalgaria

Kanchana Patlolla

Designer

Michael Lanning



Table of contents

Introduction: Models, Tools and Agents	7
Tools and tool calling	8
What do we mean by a tool?	8
Types of tools	10
Built-in tools	11
Agent Tools	13
Best Practices	15
Documentation is important	15
Describe actions, not implementations	17
Publish tasks, not API calls	18
Make tools as granular as possible	18
Design for concise output	19
Use validation effectively	19
Understanding the Model Context Protocol	20
The "N x M" Integration Problem and the need for Standardization	20



Table of contents

Core Architectural Components: Hosts, Clients, and Servers	21
The Communication Layer: JSON-RPC, Transports, and Message Types	22
Key Primitives: Tools and others	24
Tool Definition	26
Tool Results	28
Structured Content	29
Error Handling	29
Other Capabilities	31
Resources	31
Prompts	31
Sampling	32
Elicitation	33
Roots	33
Model Context Protocol: For and Against	34
Capabilities and Strategic Advantages	34
Accelerating Development and Fostering a Reusable Ecosystem	34

Table of contents

Architectural Flexibility and Future-Proofing.....	35
Foundations for Governance and Control.....	36
Critical Risks and Challenges.....	36
Enterprise Readiness Gaps.....	38
Security in MCP.....	39
New threat landscape.....	39
Risks and Mitigations.....	40
Tool Shadowing.....	42
Malicious Tool Definitions and Consumed Contents.....	44
Sensitive information Leaks.....	45
No support for limiting the scope of access.....	46
Conclusion.....	48
Appendix.....	49
Confused Deputy problem.....	49
The Scenario: A Corporate Code Repository.....	49
The Attack.....	50