Model Context Protocol

A universal connection standard for AI systems interacting with tools, data, and workflows

Yusuf Ozuysal

Why MCP?

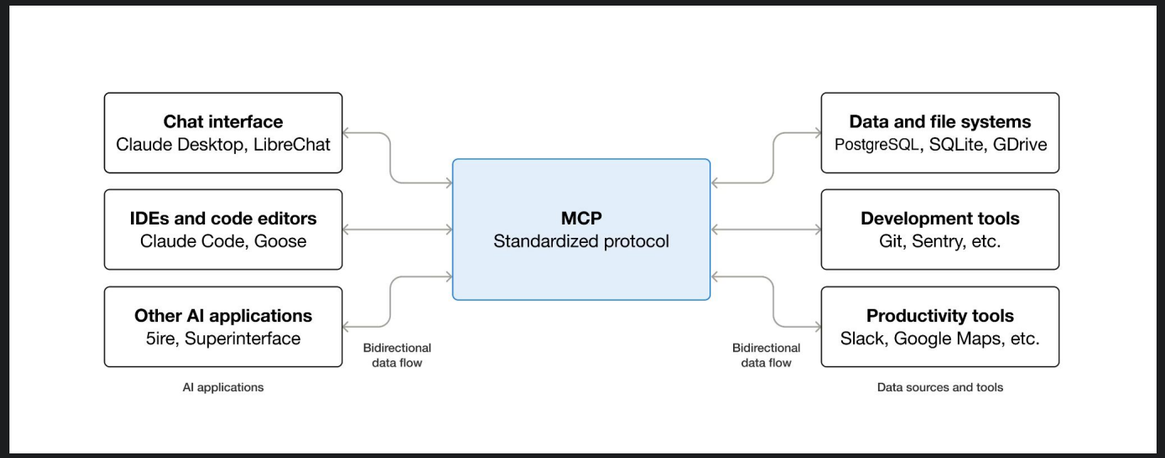
Tool calling expands application surface

Best AI applications utilize tools as experts.

o3 with search, Claude Code with planning, bash, file access, ChatGPT Agent with browser-use...

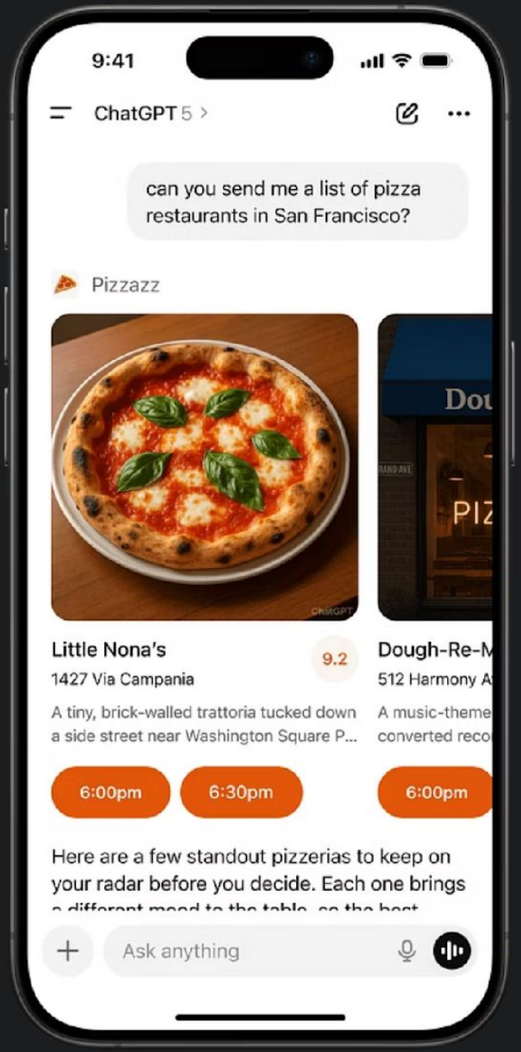
AI harness and tools expertise are different

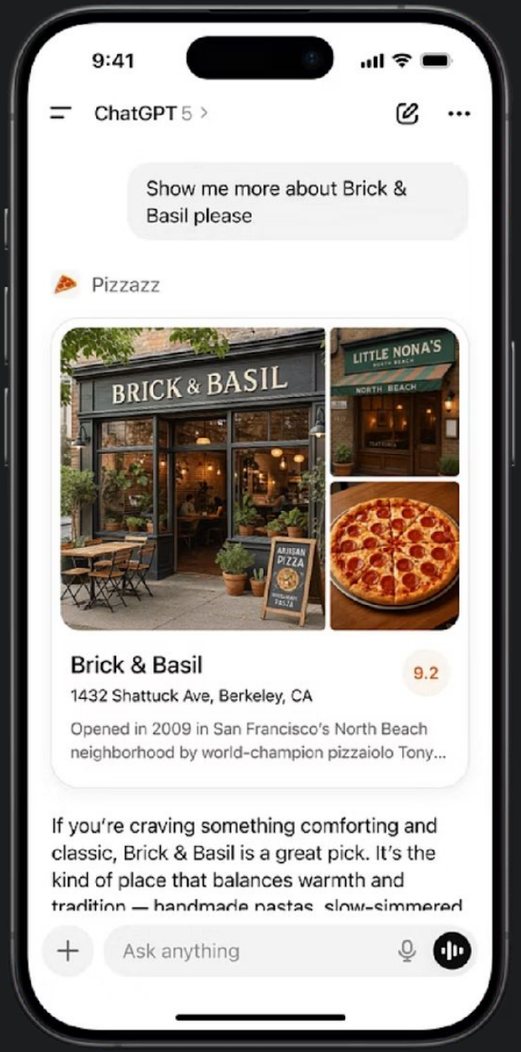
AI models, harnesses are built by frontier labs, tools will be better built by vertical specific enterprises.

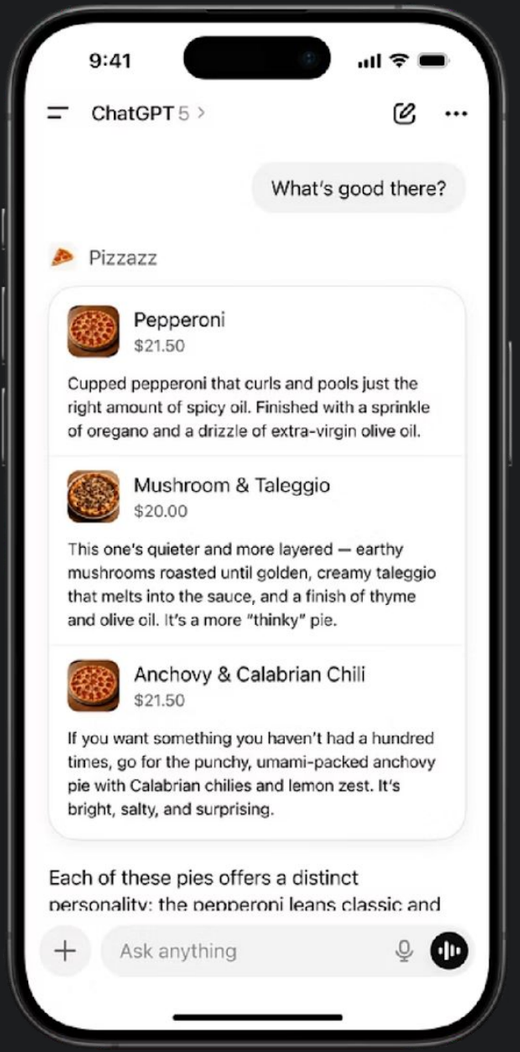


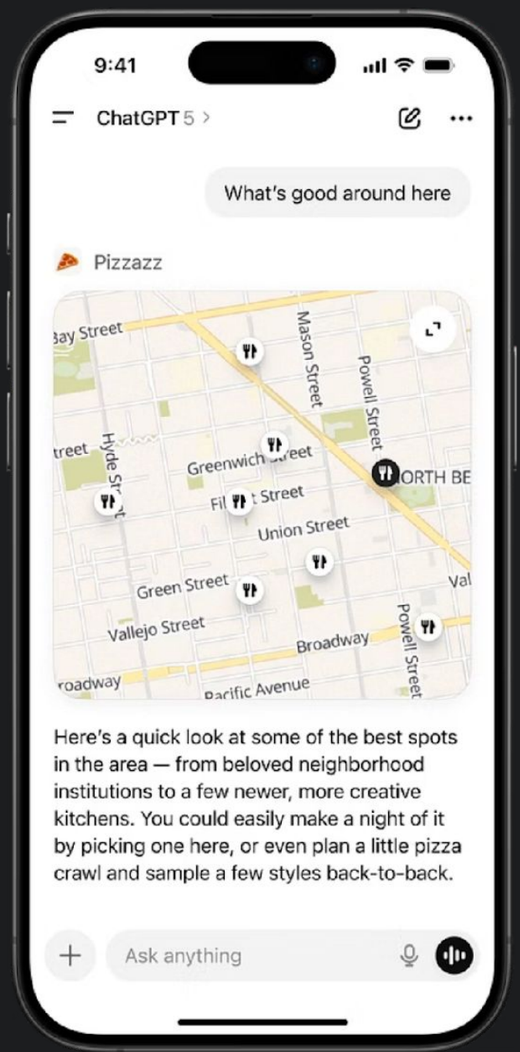
How do we build toolkits/resources that can plug-in to any harness?

Or even a foundation for the new App Store?









openai/**openai-apps-sdk-examples**

Example apps for the Apps SDK

4 17 1k 193

What is MCP?

Universal Standard

Think "USB-C for AI applications" — a common interface enabling seamless connections

Open Protocol

Connects LLMs to tools, data sources, and workflows. Built on stateful, bidirectional communication.

Client-Server Architecture

Hosts (AI apps) use MCP Clients to connect to MCP servers (context providers) via JSON-RPC 2.0

Latest spec: 2025-06-18 includes OAuth 2.1, elicitation capabilities, and enhanced security features with active development ongoing.

Core Primitives

Server-Side Capabilities

Tools: Executable functions like web search and database queries

Resources: Structured data sources including files, logs, and documents

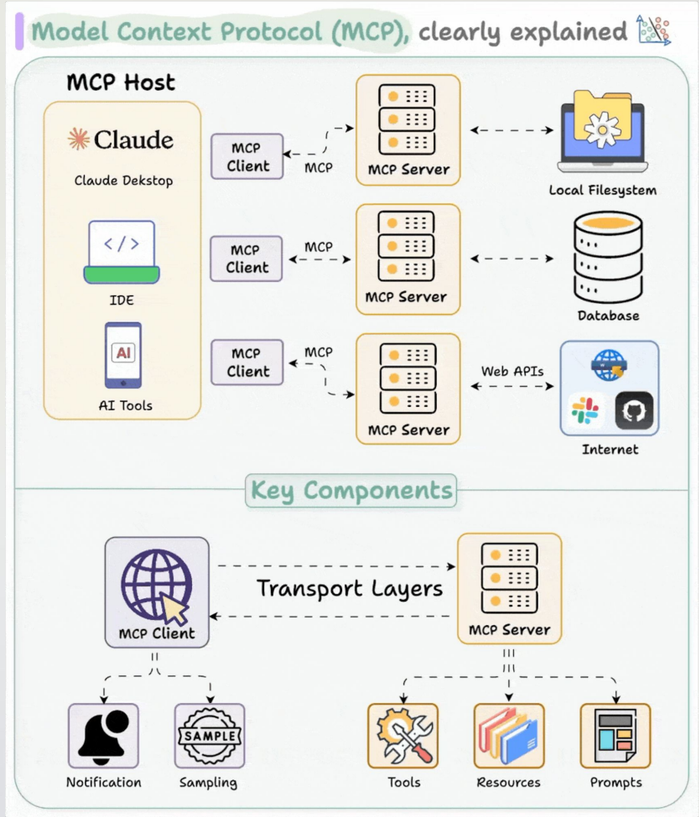
Prompts: Reusable interaction templates for consistent workflows

Client-Side Capabilities

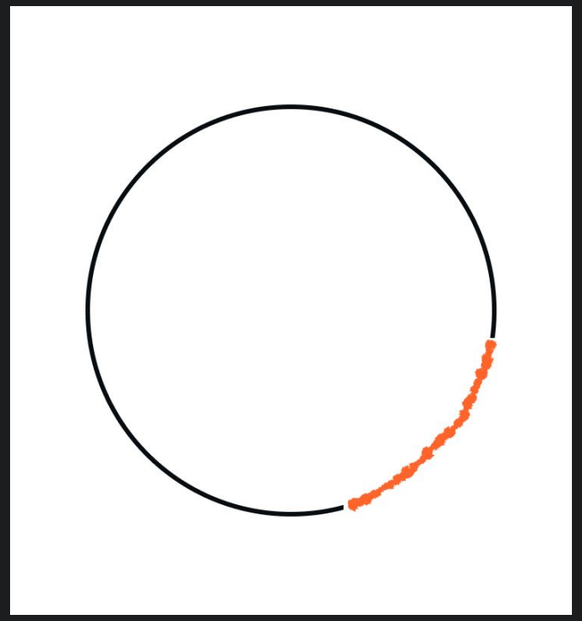
Sampling: Servers request LLM completions from clients

Elicitation: Request structured user input with validation schemas

Notifications: Real-time updates for resource changes and progress

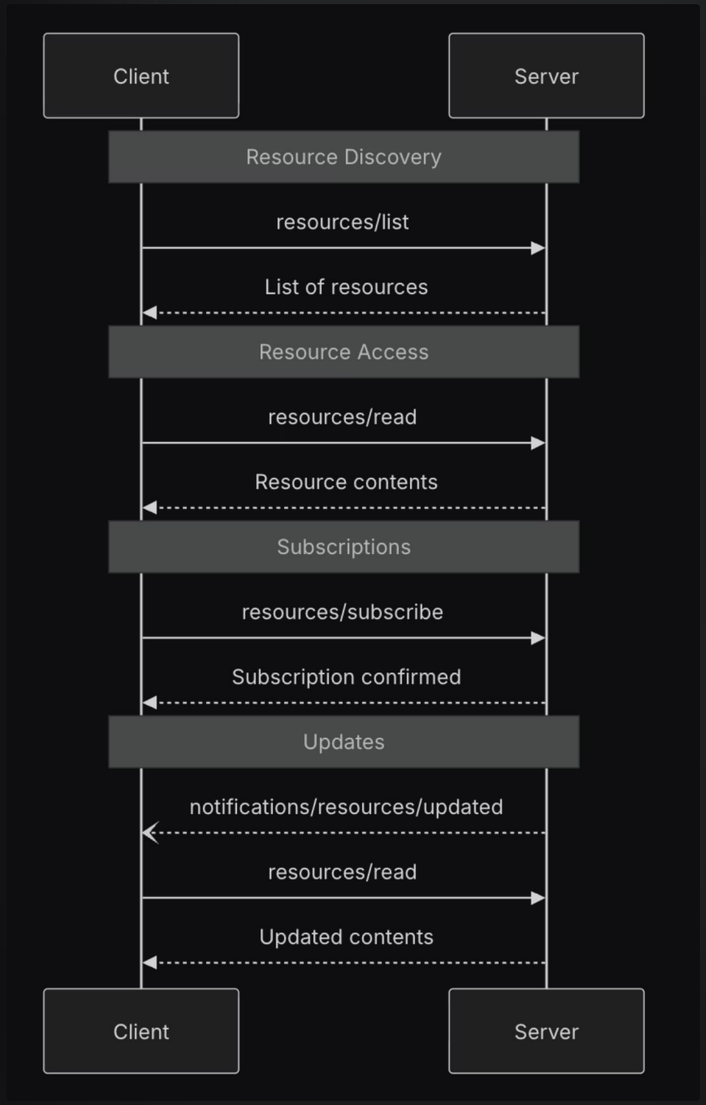


The Killer MCP Use Case: Closing The Agentic Loop



Pulse MCP blog

Tool Calling Demo



Resources & Notifications

Semantic Information Sources

Resources represent files, database records, live logs, screenshots, and other contextual data

URI-Based Identification

Unique identifiers like `file:///path/to/doc` or `db://table/record`

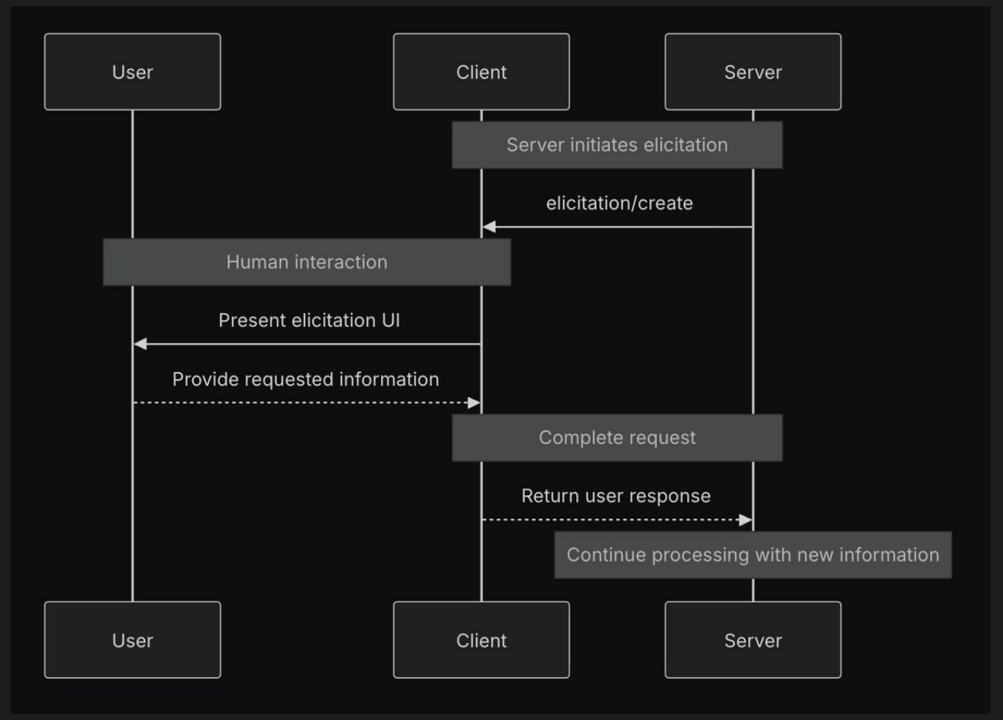
Dynamic Templates

Resource templates with parameters enable flexible access patterns

Elicitation

Servers request structured user input with JSON schema validation. Three possible outcomes: Accept, Decline, or Cancel.

Use cases: GitHub usernames, configuration preferences, sensitive parameters



Transport Mechanisms

STDIO

Standard Input/Output

- Local integrations, server runs as subprocess
- Messages over stdin/stdout, newline-delimited
- Use case: Claude Desktop, VS Code local servers
- Inherently local and secure

Streamable HTTP

Remote Connections

- Replaces HTTP+SSE approach
- POST for requests, GET with SSE for streaming
- Independent server process for remote access
- Requires authentication layer

Currently in transition period — support both transport methods for compatibility. HTTP implementations must implement proper authentication mechanisms. (Oath 2.1 being the spec)

Applications with MCP Support

Claude Desktop

First local MCP server support with native integration

Claude Code

Add MCP servers or use Claude Code itself as a server

ChatGPT Developer Mode

Remote MCP servers laying groundwork for apps

VS Code

June 2025: Full spec support including auth, prompts, resources, and sampling

Claude.ai Connectors

Remote MCP servers

Cursor

MCP integration for enhanced development workflows

APIs with MCP Support

Anthropic Messages API

Streaming MCP support with tool calling handled by Anthropic server side

Anthropic Agent SDK

Use the same harness as Claude Code while adding more capabilities

OpenAI APIs

Responses API:

Responses API handles first party tools as well

Realtime API: Same as above for real-time audio controlled interactions

Google Gemini SDK

Native capability to call MCP servers

ChatGPT Apps & New Use Cases

ChatGPT Apps SDK

Announced at OpenAI Dev Day — enables explicit brand invocation in prompts

AI's App Store moment? (Again?)

Brands prioritizing AI visibility over traditional web traffic?

Resources

Resources are finally being used in a core flow for building the UI components for the apps

Agentic Workflows

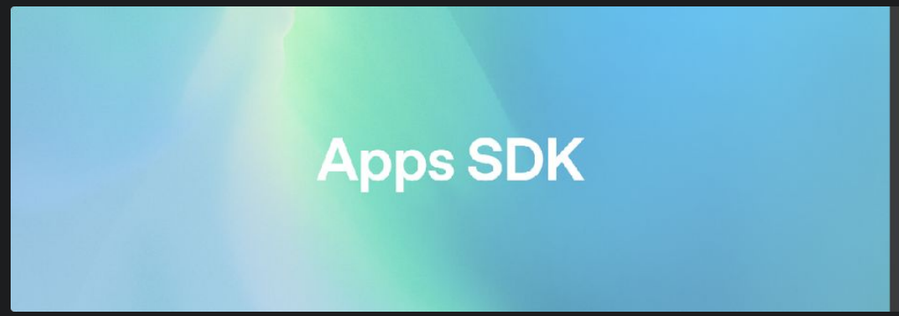
Persistent agents with session management and async tool calls

ChatGPT Apps

UI: React component runs in an iframe inside ChatGPT; it talks to the host via `window.openai` and renders inline/PiP/fullscreen.

Data flow: An MCP tool links to a UI template (`_meta["openai/outputTemplate"]` → `text/html+skybridge`). Its `structuredContent` is injected as `window.openai.toolOutput`; `content` is model-visible text; `_meta` is component-only.

Tandem loop: The component can `callTool`, `sendFollowUpMessage`, and `setWidgetState` (shown to the model) to iterate with the conversation.



developers.openai.com

Build a custom U

Build custom UI components & app page.

9:41

ChatGPT 5 >

can you send me a list of pizza restaurants in San Francisco?

Pizzazz

Little Nona's 9.2

1427 Via Campania

A tiny, brick-walled trattoria tucked down a side street near Washington Square P...

6:00pm 6:30pm

Dough-Re-M 512 Harmony A

A music-theme converted reco

6:00pm

Here are a few standout pizzerias to keep on your radar before you decide. Each one brings

Ask anything

9:41

ChatGPT 5 >

Show me more about Brick & Basil please

Pizzazz

Brick & Basil 9.2

1432 Shattuck Ave, Berkeley, CA

Opened in 2009 in San Francisco's North Beach neighborhood by world-champion pizzaiolo Tony...

If you're craving something comforting and classic, Brick & Basil is a great pick. It's the kind of place that balances warmth and tradition — handmade pastas, slow-simmered

Ask anything

9:41

ChatGPT 5 >

What's good there?

Pizzazz

Pepperoni

$21.50

Cupped pepperoni that curls and pools just the right amount of spicy oil. Finished with a sprinkle of oregano and a drizzle of extra-virgin olive oil.

Mushroom & Taleggio

$20.00

This one's quieter and more layered — earthy mushrooms roasted until golden, creamy taleggio that melts into the sauce, and a finish of thyme and olive oil. It's a more "thinky" pie.

Anchovy & Calabrian Chili

$21.50

If you want something you haven't had a hundred times, go for the punchy, umami-packed anchovy pie with Calabrian chilies and lemon zest. It's bright, salty, and surprising.

Each of these pies offers a distinct personality: the pepperoni leans classic and

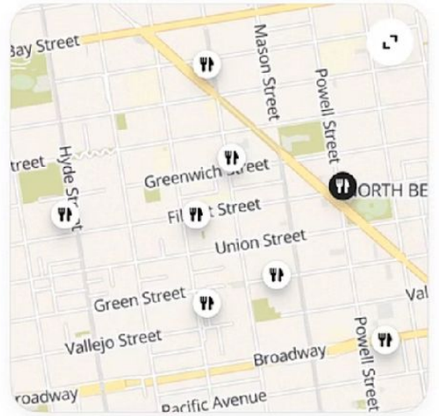
Ask anything

9:41

ChatGPT 5 >

What's good around here

Pizzazz



Here's a quick look at some of the best spots in the area — from beloved neighborhood institutions to a few newer, more creative kitchens. You could easily make a night of it by picking one here, or even plan a little pizza crawl and sample a few styles back-to-back.

Ask anything

Content Creation: Jade

MCP as creative infrastructure — Beyond coding into media production

AI-Powered Video Generation

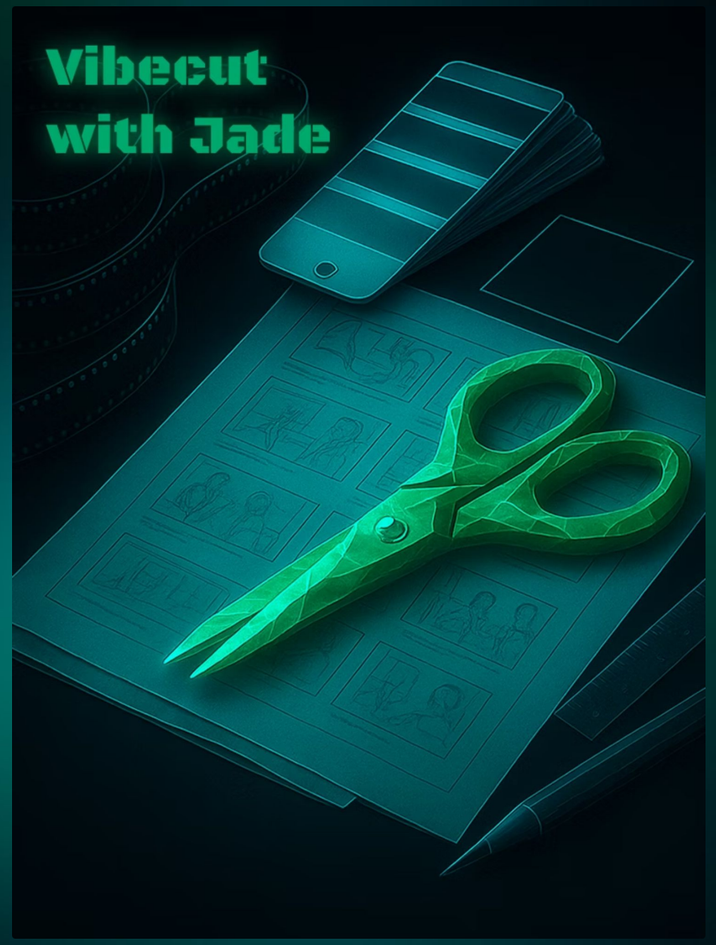
Tools for media generation using diffusion/flow matching models

Video editing and graphics

Programmatic video generation for use cases that require precision

Video understanding for closing the loop

Unit tests but for video



MCP Governance Model

SEPs

Specification Enhancement Proposals provide clear process for spec changes

Community-Driven

PulseMCP, Block, GitHub, Anthropic collaborating from inception

Working Groups

Push forward specific solutions with concrete deliverables

Interest Groups

Define problems MCP should solve and facilitate community discussions

Key principle: Open, collaborative project not controlled by any single vendor. The community shapes the protocol's evolution through transparent governance.

Get Involved

1 Build and publish MCP servers

Create tools, resources, and prompts for the ecosystem

2 Contribute to the registry

Pull requests welcome for server discovery and sharing

3 Join working and interest groups

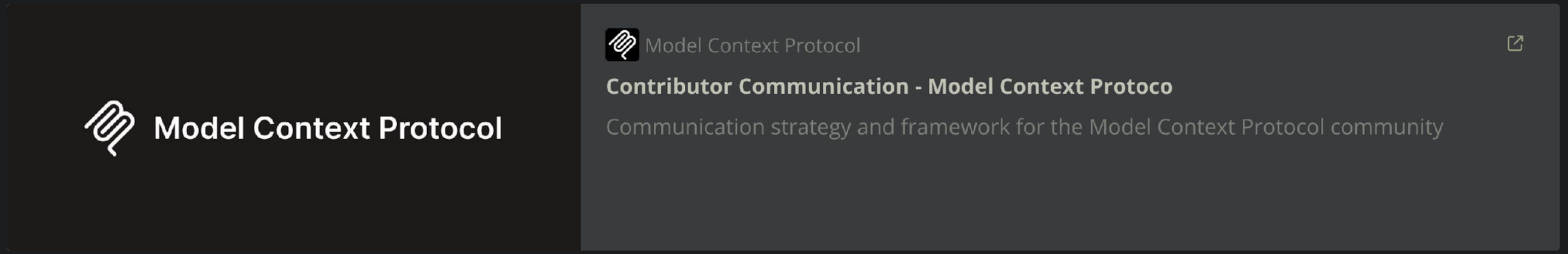
Shape the future direction of the protocol

4 Provide feedback via GitHub

Report issues, suggest enhancements, share use cases

MCP Registry

September 2025 launch — Open catalog and API for publicly available servers at `github.com/modelcontextprotocol/registry`



Questions?

Appendix

Connection Lifecycle

Initialization

Protocol version verification and capability negotiation establish the foundation

Identity Exchange

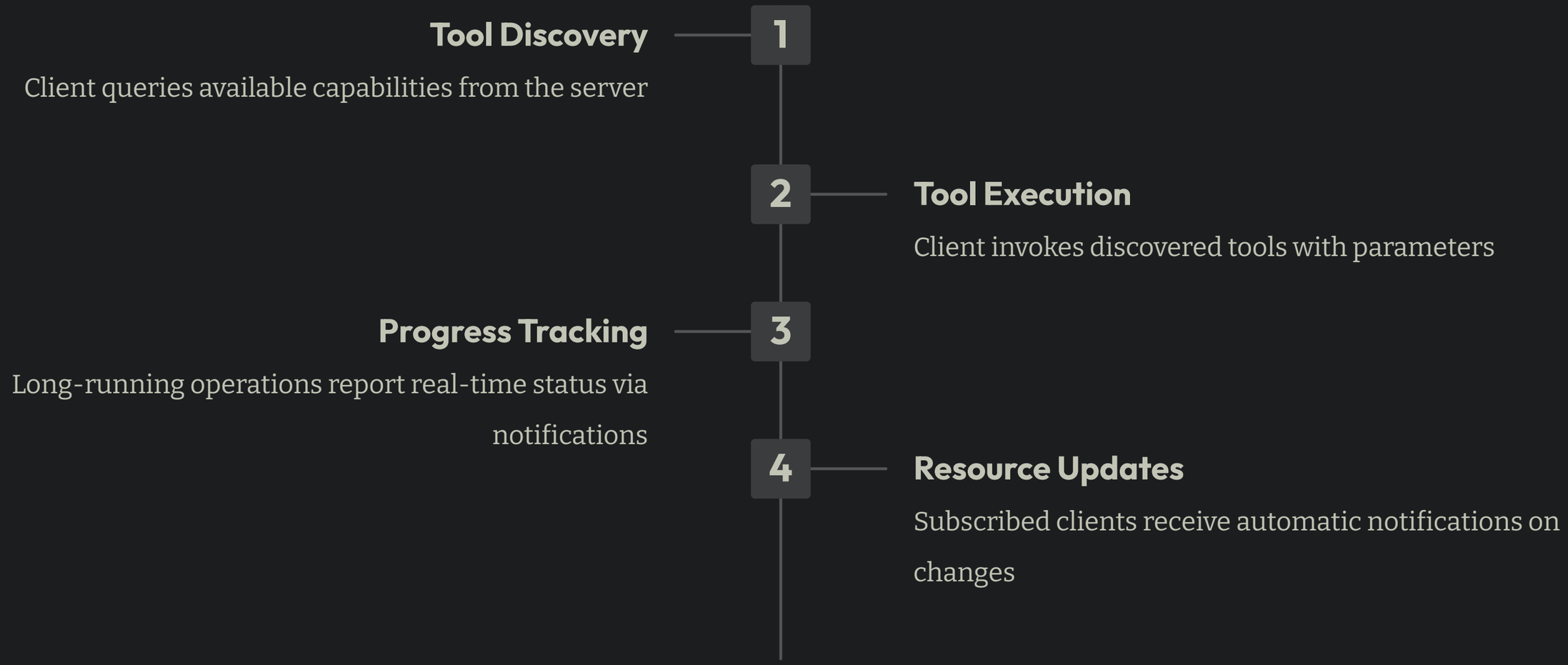
Client and server identify their capabilities: tools, resources, sampling support

Stateful Session

Maintains context throughout the entire session lifecycle

The lifecycle is transport layer agnostic — the same connection pattern works across STDIO, HTTP, and SSE implementations.

Request/Response Flow

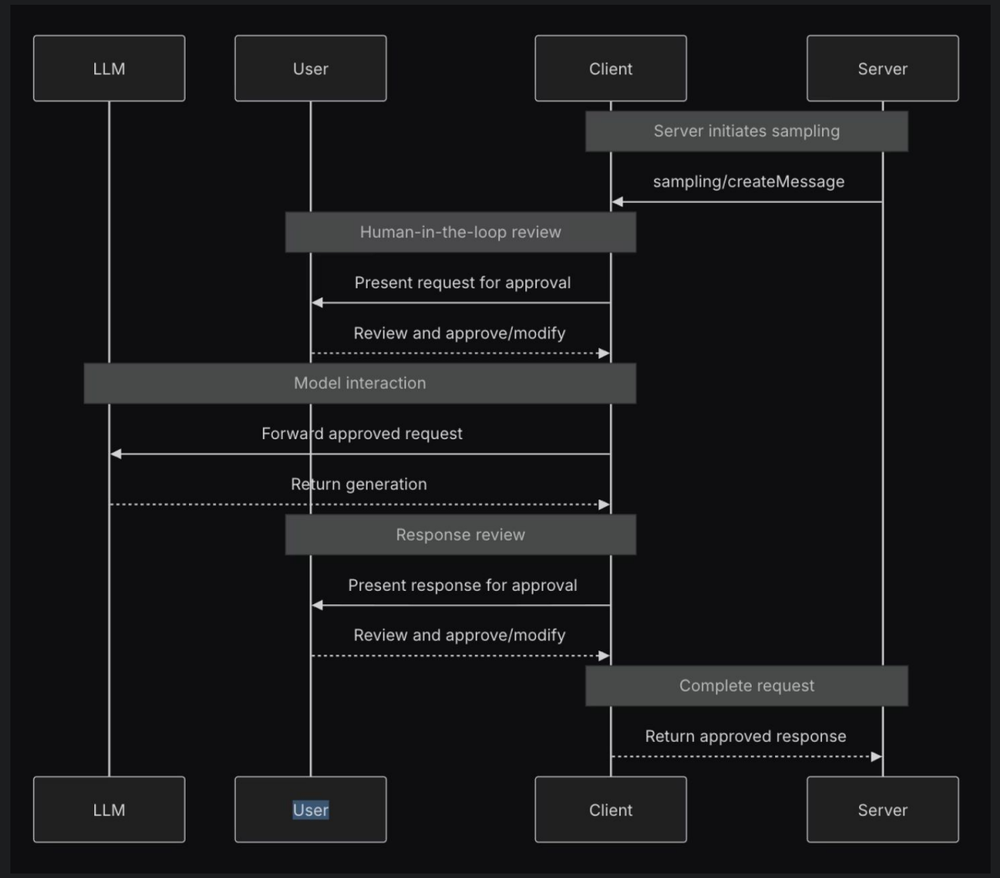


All communication follows **JSON-RPC 2.0 message patterns**: requests expect responses, while notifications flow without requiring acknowledgment. Bidirectional channels enable servers to request sampling or elicitation from clients.

Sampling

Servers request LLM completions from the client, enabling:

- Multi-agent coordination without exposing API keys
- Client control over costs, security, and model selection
- Sub-agents delegating complex reasoning to main LLM



OAuth 2.1 Authorization