

OPEN PROTOCOL STANDARDS • ARCHITECTURE SPECIFICATION • FEBRUARY 2026

Decentralized Model Context Protocol: Cryptographic Tool Transport & SSE Streaming for Enterprise CMS

Kites Protocol Working Group • protocol@kites.dev

Abstract: Autonomous agentic workflows (e.g., Claude Desktop, Cursor, LangChain) require standardized, bi-directional interfaces to inspect and modify structured content systems securely. This specification outlines an implementation of the Model Context Protocol (MCP) over JSON-RPC 2.0 with Server-Sent Events (SSE). We introduce a zero-trust capability model utilizing SHA-256 hashed API keys and per-endpoint capability whitelists, validated across thousands of live WordPress production environments through the official WP MCP connector.

1. Executive Summary & Protocol Rationale

The rapid proliferation of Large Language Model (LLM) agents has created an urgent need for secure, standardized communication between client agents and existing enterprise database architectures. WordPress, powering over 40% of the web, represents a critical surface for agentic content authoring, asset management, and analytics.

Traditional REST and GraphQL endpoints lack unified protocol-level handshakes for dynamic tool discovery, streaming execution feedback, and per-tool permission scopes. The WP MCP standard fills this gap by implementing the Model Context Protocol directly inside the WordPress core ecosystem.

2. Transport Layer: JSON-RPC 2.0 & SSE

WP MCP implements dual-mode transport: (a) Standard HTTP JSON-RPC 2.0 for single request-response invocations, and (b) Server-Sent Events (SSE) for streaming progress, long-running batch migrations, and real-time event subscriptions.

All endpoints implement nonces, rate-limiting tokens, and SHA-256 key verification, ensuring zero database vulnerabilities even on public multisite installations.

3. Tool & Resource Discovery

Clients querying the endpoint receive a self-documenting JSON Schema specification of available WordPress capabilities, including `wp.posts`, `wp.media`, and `wp.users`. This enables zero-configuration integration with tools like Claude Desktop and Cursor.

4. Open Source Availability

WP MCP is fully open-source and officially listed on the WordPress.org plugin directory and GitHub (github.com/jabedbd/wpmcp). Community contributions and RFC extensions are welcomed.