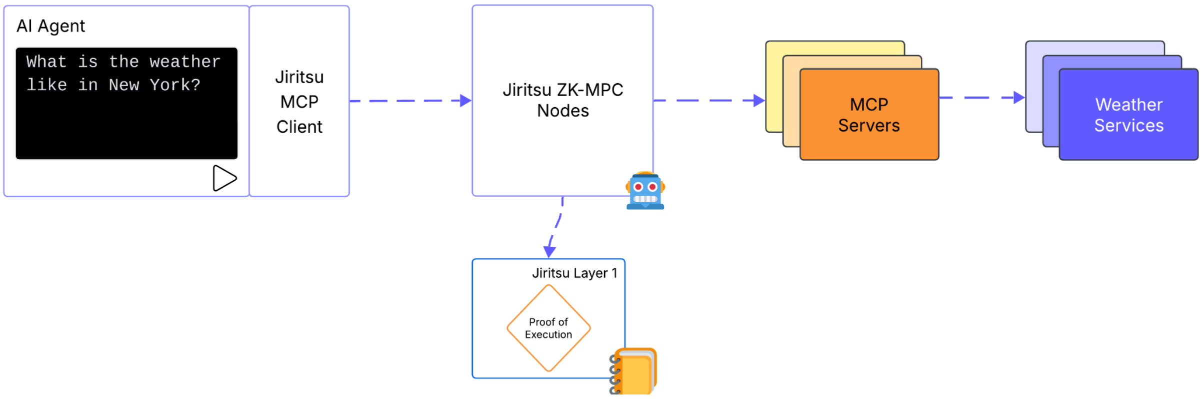
MCP Verifier - Product Overview

Overview

The **Jiritsu MCP Verifier** is a trustless job orchestration service that facilitates secure, verifiable calls to **Model Context Protocol** (MCP) services on behalf of a client or host. Built on top of the Jiritsu platform's zero-knowledge (ZK) infrastructure, it ensures that every MCP interaction is transparently executed, fully auditable, and cryptographically provable—without exposing sensitive data or relying on centralized trust.



Key Features

Deterministic Job Execution

The MCP Verifier operates as a pre-defined, declarative job on the Jiritsu platform. Each job is submitted with specific parameters for the intended MCP call and executes deterministically according to a validated flow. This guarantees consistent behavior and reproducibility across executions.

MCP Interface Integration

At its core, the verifier acts as a mediator between clients and MCP services. Clients submit parameters required for an MCP operation (e.g. key shares, session info), and the verifier dispatches the request to the designated MCP server or interface. Common use cases include secure signing, encrypted data aggregation, and threshold operations.

Result Collection and Delivery

Upon completion of the MCP process, the verifier receives the response and returns it to the originating client or host. Depending on configuration, this can include on-chain result anchoring or encrypted off-chain delivery.

Zero-Knowledge Proof of Execution

A ZK proof is generated for every MCP Verifier job, attesting to:

- The integrity of the job’s input parameters
- The authenticity of the MCP endpoint call
- The correctness and origin of the result
- The adherence to job constraints and system policies

This cryptographic proof is published on-chain and can be independently verified by any observer or counterparty, enabling tamper-proof audits without disclosing internal data or logic.

Use Cases

- **Secure Transaction Signing**: MPC-based signatures for wallets and custody workflows
- **Encrypted Data Collaboration**: Aggregation and processing of sensitive data across parties
- **Access Control & Escrow**: Threshold decryption or secret release protocols
- **Regulatory Process Verification**: Prove that cryptographic operations occurred under defined policy rules

Benefits

- ✅ End-to-end verifiability of MCP service usage
- ✅ Job determinism ensures consistency and traceability
- ✅ Privacy-preserving ZK architecture
- ✅ Seamless integration with off-chain MCP providers
- ✅ Immutable audit trail for compliance and governance