ANNEX · AI MCP

Experiment: a verified measurement of the MCP Registry

An AI agent, working through the Truebit MCP server, captured the official MCP Registry, drew a seeded random sample of 50 servers and classified what each entry declares about authentication. Every fetch and every computation ran on Truebit and left a public, signed transcript. Data collected 8–9 October 2026.

40,873
current servers in the MCP Registry

50
sampled at random · seed 20260915

30
of the sample reachable over the network (60%)

93.3%
of those declare no credential · 95% CI 78.7–98.2%

PIPELINE · EVERY STEP ON TRUEBIT LEFT A PUBLIC, SIGNED TRANSCRIPT

STEP 1
Registry pages
409 verified API calls, one per page, in the enclave

→

STEP 2
Snapshot
assembled by the agent · 40,873 entries fixed by SHA-256

→

STEP 3
Sampling
seeded draw of 50 as a verified computation

→

STEP 4
Classify
four-class rules as a verified computation

→

STEP 5
Verification
4 checks on every transcript · all passed

RESULT · THE 50 SAMPLED ENTRIES



28 remote, no credential

2 remote, credential required

19 local package (stdio)

1 no usable endpoint

Same protocol on 26 Aug 2026 (24,940 servers): 87.1% → 93.3% now. The intervals overlap; no change shown.

Transcripts: sampling 03bf8313-f118-4ebb-b67a-20cb1a86c0e9 · classification 26dc0b7f-e4c4-4302-989e-1b0afe37b155 · https://run.truebit.network/task/{id}/transcript

ANNEX · AI MCP

Inside the experiment: method, verification and limits

METHOD · REGISTRY METADATA ONLY, NO SERVER CONTACTED

Population — Every current entry of registry.modelcontextprotocol.io/v0/servers, 409 pages of 100 → 40,873 servers in one canonical JSON snapshot, fixed by SHA-256 6684a861…75fc37.

Sampling — 50 drawn without replacement, seed 20260915 (Mersenne Twister), as a verified computation with a JavaScript port of the generator; its draw matched Python's random.sample index for index.

Classification — Four classes from the entry alone: remote with a required credential header (secret, or named authorization / api-key / x-api-key / token / bearer) · remote without one · local package (stdio) · no usable endpoint.

VERIFICATION · EVERY STEP CHECKED AGAINST TRUST ANCHORS v2026-10-07

Registry page = verified API call

the HTTPS request ran in an attested enclave; the transcript binds the response body to TLS evidence from the registry's server

Draw + classify = computation

independent nodes ran the same program and had to agree; the transcript records source, input and output

409 PAGE CALLS + 4 COMPUTATIONS · FOUR CHECKS EACH · ALL PASSED

existence · integrity · binding · signers

CHECK A FIGURE YOURSELF

1 run.truebit.network/task/{id}/transcript holds the response or output behind each figure.
2 sha256sum snapshot.json must give 6684a861…75fc37.
3 Re-run the draw (seed 20260915, n = 50) and apply the rules: Table 1 follows.

Declared, not enforced

OAuth via MCP discovery is not recorded in the registry

Sample size

n = 50: about ±14 points at 95%; wider on the 30 remote

Point in time

four-hour capture; the registry grew 64% in six weeks

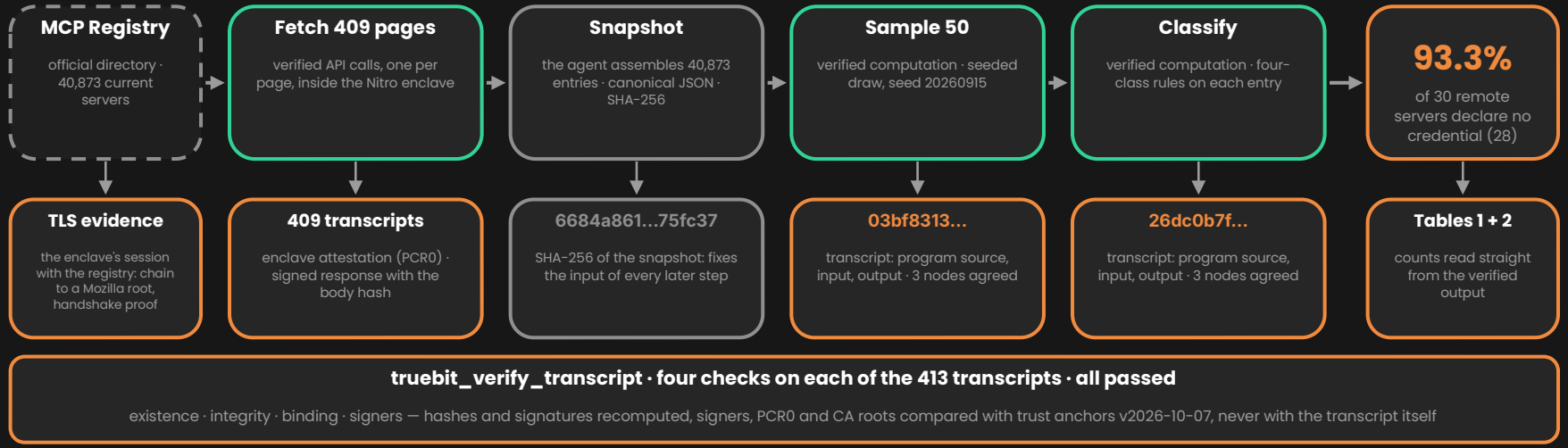
Coverage

only servers listed in the official MCP Registry

Trust anchors v2026-10-07 · SHA-256 2c53132818f575a61d1986ed6bbf8046568bf67e51ab26fd614d4cede79e0171 · all 409 page execution ids: report, Appendix B

ANNEX · AI MCP

The experiment as a pipeline — and the proof each stage leaves



Any step can be redone by a stranger from the execution ids alone: transcripts are public at https://run.truebit.network/task/{id}/transcript.