

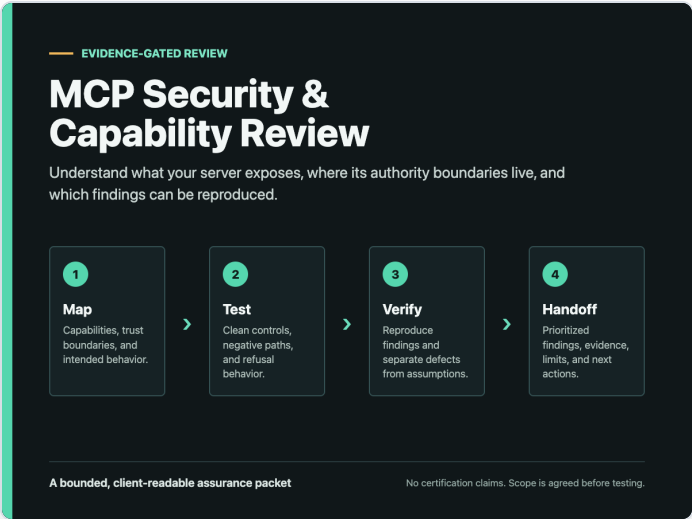
OPERATOR-OWNED SYNTHETIC DEMONSTRATION

MCP Security & Capability Review

A bounded example of how authority, refusal paths, and evidence can be mapped before higher-risk testing begins.

16 scenarios	14 expected denials
18 passing tests	0 external actions

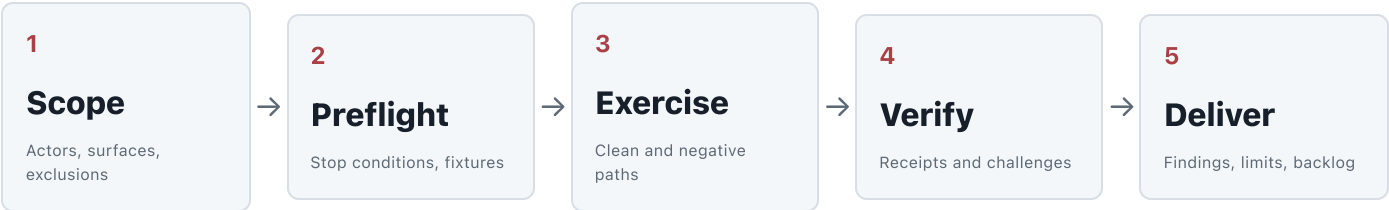
No client or production system. This sample uses two versioned local fixtures, synthetic data, and loopback-only execution. It is not a vulnerability report, audit, penetration test, compliance assessment, or certification.



What the review is designed to answer

The review turns an MCP-shaped system into a decision map: who can act, what resource is addressed, which operation is allowed, how refusal behaves, and what evidence can be handed to another reviewer.

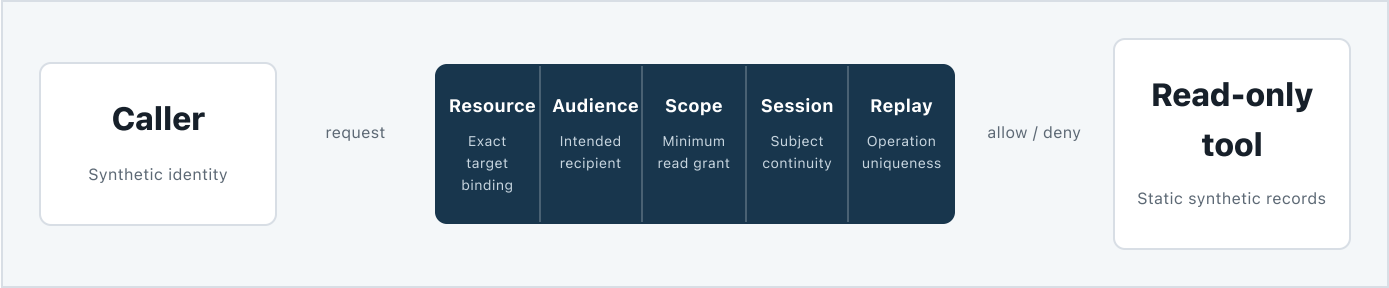
A Authority Which identity, audience, resource, scope, and session bindings govern a call?	B Boundary Where do local policy, MCP transport, application behavior, and external effects separate?	E Evidence Which clean control and negative paths are reproducible from pinned inputs?	H Handoff What can be stated now, what remains untested, and what needs new authorization?
---	--	---	---



Decision rule A result advances only when its authority, evidence, and limitation are visible together. A plausible explanation is not treated as a verified result.

The surface before testing

The sample starts with a narrow read-only operation and makes each policy decision explicit. The diagram describes the fixture, not MCP as a whole.



BOUNDARY	FIXTURE RULE	EXERCISED EVIDENCE	LIMIT
Resource	Exact target required	Mismatch denied	No production protected-resource deployment
Audience	Intended recipient required	Wrong audience denied	No external issuer validation
Scope	Minimal read grant	Insufficient scope denied	No complete authorization matrix
Session / replay	Bound subject and unique operation	Mismatch and replay denied	No production session service
Network	Loopback target only	External host refused before request	No external-host assessment

Two fixtures, one bounded result pattern

Both runs were regenerated from current source. Each retains one clean control, seven expected refusal paths, and zero external actions.

CORE EXAMPLE

Authorization boundary fixture

Node.js loopback policy surface

1 accepted

7 denied

• Missing authority

• Resource and audience mismatch

• Insufficient scope

• Session-subject mismatch

• Token forwarding attempt

• External host attempt

9/9 tests passed · receipt verifier passed

ADVANCED APPENDIX

FastMCP signed-agent fixture

FastMCP 3.4.4 · stateless JSON Streamable HTTP

1 accepted

7 denied

• Missing signed envelope

• Invalid signature

• Resource and scope mismatch

• Operation replay

• Revoked key

• External host attempt

9/9 tests passed · receipt verifier passed

Observed Current fixture behavior and retained receipts	Not tested Client systems, production identities, external hosts	Needs authority Any live integration, credentialed call, or write action
---	--	--

The signed-agent envelope is application-layer fixture policy and **not an MCP conformance result**. Receipt verification is local and **not an independent certification**.

What a real engagement would produce

The synthetic sample demonstrates the format. A client engagement starts from written scope and substitutes client-approved staging evidence only where authorization permits.

01 Authority map Actors, resources, scopes, side effects, and decision owners.	02 Capability inventory Tools, transports, trust boundaries, and declared exclusions.	03 Evidence table Clean controls, negative paths, receipts, and confidence labels.
04 Findings backlog Prioritized questions with the smallest useful next proof.	05 Reproduction handoff Client-safe commands, expected outcomes, and stop conditions.	06 Closeout receipt Inputs, environment, delivered artifacts, verification, and limits.

BOUNDARY Map the surface Best for teams that need a credible authority and capability inventory before testing.	ASSURANCE Exercise the controls Add clean and negative-path checks against an approved fixture or staging surface.	ADVANCED Leave a reusable fixture Add a bounded regression fixture and a reviewer-ready evidence handoff.
--	---	--

START WITH THE BOUNDARY

Bring a repository, architecture, or staging question.

The first decision is whether the work can be scoped and checked safely.

View on Upwork

Review the public method

Download the PDF

Pinned local artifacts and limits

Machine-readable evidence is included alongside this report in `evidence.json`. It records the source hashes, scenario counts, external-action totals, and claim boundaries used for this synthetic sample.

Current receipts

`proof-labs/mock-mcp-authz/artifacts/latest-scenarios.json`

`proof-labs/fastmcp-signed-agent-integration/artifacts/latest-scenarios.json`

Public artifacts

[evidence.json](#)

[six-page PDF](#)

[public method and fixtures](#)

This sample does not establish

- MCP, OAuth, or framework-wide conformance.
- Security, availability, or compliance of an external system.
- A complete test plan, vulnerability inventory, or production result.
- Independent validation, certification, testimonial, or client outcome.
- Permission to reuse client data, names, metrics, logos, or reports publicly.