MESSAGE-BASED SECURITY

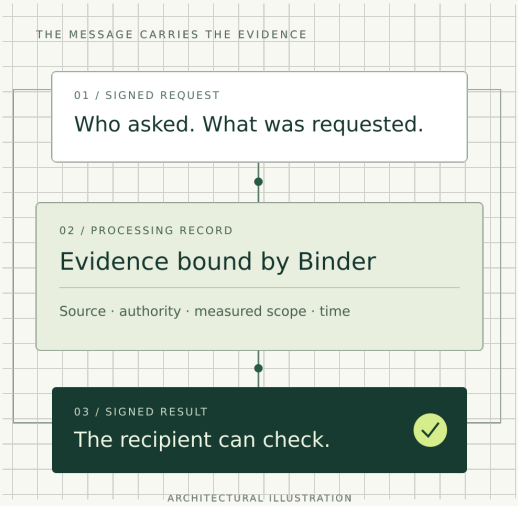
Evidence belongs in the exchange.

Signed requests, data with Origin, measured processing and signed results give a recipient evidence it can evaluate before acting.

Agree the evidence contract.

Name the principal, delegated scope, intended service, task, request binding, validity and replay controls. Specify which source, quality and process evidence must accompany the result.

Binder consumes available measurements and binds them to the request and output. The recipient applies its own acceptance policy.



Illustrative message record. Every deployment specifies actual fields, evidence and verification rules.

Governance becomes part of agentic state.

A verified exchange updates what the agent or conventional system is permitted to do next. Verification tools perform the deterministic checks; the workflow requires them at the decision point.

A signature, an authority assertion, a source commitment and a quality check answer different questions. Preserve those distinctions in the evidence profile.

THE COMPONENTS

Integrate the evidence your service needs.

These components connect to the customer application and infrastructure. Their configuration and acceptance rules are part of the delivery.

Authority and signed requests

Digital Name / CorpID patterns and signing tools connect instructions to a principal, delegated scope and validity. Organizations define their own authority.

Data with Origin

Preserve source references, versions and retrieval context. Add the defined quality tests with their methods, results and coverage. A hash alone does not establish semantic truth.

Binder

Bind request, result and available measurements. Declare the covered layers, measurement source, baseline and time. Boot evidence does not establish application or model integrity.

Signed message profiles

Define the covered content and context, request binding, recipient, validity windows and replay controls.

Data wallets and evidence records

Retain the evidence needed for later verification under the owner’s access, disclosure, retention and recovery policy.

Recipient verification

Check signature mathematics, issuer authority, request binding, freshness, status and evidence scope before the next action.

VERIFICATION POLICY

A valid signature is one required check.

Cryptographic correctness, authority, data quality and processing evidence have separate meanings and separate failure modes.

Content and authority

Verify covered bytes with the expected key material. Establish why that key may authorize this action, including delegation, scope and history.

Request binding and freshness

Match the result to the intended request. Enforce the profile’s time, replay and status rules using appropriate clocks and state.

Data quality and measured scope

Evaluate explicit quality tests and the evidence for the layers the decision depends on. Missing evidence is a policy outcome, not permission to infer a stronger claim.

Exceptions and preservation

Define rejection, retry and human review paths. Preserve historical verification material across key rotation and certificate expiry. Design encryption and access controls separately.

The April 2026 Five Eyes guidance recommends signed instructions and fresh proofs for privileged calls. The NSA’s May MCP guidance recommends message signatures, expiry and binding to time and context. These documents do not certify a vendor.

Five Eyes: Careful adoption of agentic AI services, pp. 23 and 28

NSA: MCP security design considerations, p. 12

LIVE EVIDENCE / 15 SEPTEMBER 2026

Inspect the service. Read the scope.

Rootz Node is a live Polygon service over MCP and JSON-RPC. A specific observation supports a specific claim.

What was checked

At 15:02 UTC, JSON-RPC returned block 93,853,009. Local checks verified the response-byte commitment, Ed25519 and P-256 signatures, keyset digest and certification signature under the supplied root key. Altered content failed integrity checking.

What that observation does not establish

The request was unsigned. The check did not independently anchor hardware identity or demonstrate signed-request authorization. The complete customer request-to-result path needs its own acceptance test.

Published measurement depth

Node publishes boot measurements for PCR 0, 4 and 7 using a software vTPM. Bor client measurement and runtime integrity are outside the declared scope. OCI instance evidence asserts identity.

Other working components

Origin exposes prepared data and source evidence. SEC references and leaf hashes are not SEC-issued signatures. Proof demonstrates message verification; CorpID addresses organizational authority.

Rootz Node and published claims

Machine-readable Node claims

Origin prepared-data service

Define your deployment evidence: datacenters.rootz.global/how