RESEARCH INSTITUTE OF SYSTEM SYNTHESIS, IS 3.0 VERIFICATION PASSPORT, EDITION OF 26 OCTOBER 2026

MITR, the open packages and the INDRA tester: what has been measured and how to repeat it

This document is written for an information security specialist. It gives every figure about MITR with the date and place of measurement, next to the commands that repeat it and the limits of applicability; what has not been measured is not in the document.

1. Subject

MITR checks an agent's call to a tool once the model has finished reasoning: the name of the action, its arguments, its addressee and the facts from sources assigned by the organization. The model's text and the agent's own words are left aside. Each rule, or contract, is kept as a separate data file. The solver Z3 (an open project of Microsoft Research), working in the QF_UFLIA logic, that is, quantifier-free logic with uninterpreted functions and linear integer arithmetic, proves that under these facts the action satisfies the safety condition. If there is no proof, the action is stopped in enforce mode.

Every decision produces a receipt. The receipts are linked into a chain with the SHA-256 hash function (SHA stands for Secure Hash Algorithm). Once a day the external time witness OpenTimestamps fixes the head of the chain, so any edit made after the fact is detected on recomputation.

The guarantee of MITR is soundness: an allowed action does not violate the rule. MITR does not guarantee that the rules are complete, because a person translates each norm into a rule. Every receipt names the specific rule under which the decision was made.

2. Measurements of MITR

- **Twenty contracts out of twenty** run in enforce mode; the mode was read from the environment of the live service process on 25 October 2026.
- **A decision under a rule in a warm process** takes 1.08 milliseconds at the median, 1.96 milliseconds at the 95th percentile and 3.61 milliseconds at the 99th percentile. The measurement of 24 October 2026 covered 1,000 decisions on 20 contracts, of which 500 were allowances and 500 refusals, with no false allowance or refusal.
- **A call together with the explanation of a refusal** takes 5.22 milliseconds at the median in the same measurement. The first decision in a freshly started process takes 30.7 milliseconds at the median over 300 launches.
- **The attack set on actions**, with 157 cases of which 114 are attacks and 43 are ordinary calls, ran on 24 October 2026 without a single missed attack and without false refusals.
- **Three known gaps in the rules** are named by the set itself: a restart of the checking service is allowed without approval, and for that time the hook lets actions pass unchecked; the owner's explicit objection is not asked on two of the three paths that delete an event; the approval marker is set by the agent's workstation in place of the owner's signature. Closing these gaps is in the work plan.
- **The receipt chain** has been kept since 16 September 2026 and held 5,094 records on 25 October; it is consistent from the first record.

- **The external time witness** fixed epoch 33 of 5,079 records with a timestamp in Bitcoin block 973,024, recorded on 25 October 2026.
- **The replay of decisions with the verifier for outsiders** matched in 5,079 cases of 5,079 with no discrepancy; the replay of 25 October 2026 was performed by the institute itself.
- **Each of the 92 refusals** in the thirty days to 25 October 2026 named the violated condition, and factual errors were refuted by 94 records in the same chain.
- **Six statements about MITR** were confirmed in full by the daily instrument for 23 October 2026; for 24 October five of six were confirmed and one was not measured. The target is six of six for fourteen consecutive days.
- **The automated code tests** in the run completed on 26 October 2026 all passed, 6,414 of them, with no failures.

MITR has run continuously since 24 April 2026 and holds the actions of the institute's agents. The measurements were taken on the institute's own server with four processor cores and eight gigabytes of memory. The spread under industrial load is determined on a joint bench with the customer.

3. Open packages

The packages are published under the Apache-2.0 license and check a call by pattern matching, without a solver: the solver and the chain with an external witness exist only in MITR. The institute's packages are not in the public PyPI index, where an unrelated project is published under the name `mcp-sentinel`, so the packages are installed only with the `--no-index` option from a downloaded directory.

The checksums are given in the format read by `sha256sum -c`: the lines below are saved to a file next to the downloaded packages and checked with one command.

```
681a4db59a1a44e89a2b1386ec4b4f2e1fc23c1025c295b9ebf00fd5d20901ea  mcp_sentinel-1.1.2-py3-none-any.whl
abb88978db7b34a2f1f56e0eff42bcd1365b9cc0eb17e4a4380f7815e4f1b79e  mcp_sentinel-1.1.2.tar.gz
8d4ffe60f41ebd377c476f369655aaef5e0ac91858a3d294be37fd1e3100bc87  iss_ledger_117-1.1.1-py3-none-any.whl
6eccef523e24fa60fed29c78866ff12afbab092bd17d51642e00d34dfcea9fa5  iss_ledger_117-1.1.1.tar.gz
7ed0ae9073f512a5cfd71b62904094ca36d0ae2fdb1b4bfff5900d3e368781c3  iss_agent_kit-0.1.1-py3-none-any.whl
0314047404888c29a231fc8710874f15bc2bd75e2b89ba7c4c882da3c792116a  iss_agent_kit-0.1.1.tar.gz
1ff894574407307d33ec99115652bcaec4e53d06189178696d0db1c767a8608f  iss_verifier.py
```

The files are at `https://isslab.ai/wp-content/uploads/iss-utils/`, and the source code is at `https://git.isslab.ru/isslab/`. The `iss-ledger-117` log is linked with the "Streebog-256" hash function of the Russian national standard GOST R 34.11-2012 (GOST stands for gosudarstvenny standart, the state standard) and passes the test examples of that algorithm's description (RFC 6986); the MITR chain is computed with SHA-256, and a second GOST digest for it remains a plan.

4. The INDRA tester

The INDRA tester is an internal bench of the institute's own design for checking web services and application programming interfaces (API). The acceptance protocol of 25 October 2026 met 12 criteria of 12 on a labeled set of 28 scenarios, 14 vulnerable and 14 clean: all 14 vulnerabilities were found, with no false positives.

The automated check covers seven classes: injection into database queries (SQL), injection of operating system commands, path traversal, access to other users' objects by direct reference (IDOR) and broken object-level authorization (BOLA), server-side request forgery (SSRF), leakage of secrets and missing security headers. Resource exhaustion is tested only in laboratory mode. A software filter in the request path intercepted all 26 destructive requests before they were sent, and probing is limited to the tenant's allowlist of addresses.

The acceptance protocol remains a developer's document and does not replace a certificate of the Federal Service for Technical and Export Control of Russia (FSTEC of Russia).

5. How to repeat

MITR's receipt chain

```
curl -O https://asi5.ru/console/verify/verify_chain_standalone.py.txt
mv verify_chain_standalone.py.txt verify_chain_standalone.py
curl -O https://asi5.ru/console/verify/gate_anchors-public.jsonl
python3 verify_chain_standalone.py gate_anchors-public.jsonl   # 0 means the anchors match
curl -O https://asi5.ru/console/verify/gate-anchor-epoch-33.json
curl -O https://asi5.ru/console/verify/gate-anchor-epoch-33.json.ots
ots --no-bitcoin verify gate-anchor-epoch-33.json.ots          # calendar attestation, no Bitcoin node needed
# check against block 973,024: ots verify with a Bitcoin node available
```

An open package without network access

```
mkdir wheels && cd wheels
curl -O https://isslab.ai/wp-content/uploads/iss-utils/mcp_sentinel-1.1.2-py3-none-any.whl
curl -O https://isslab.ai/wp-content/uploads/iss-utils/iss_ledger_117-1.1.1-py3-none-any.whl
sha256sum *.whl   # mcp-sentinel depends on the iss-ledger-117 log; checksums are in section 3
cd .. && python3 -m venv .venv && . .venv/bin/activate
pip install --no-index --find-links ./wheels mcp-sentinel
mcp-sentinel check --tool sql_query --args '{"query": "DROP TABLE users;"}'
# BLOCK, exit code 2
```

6. Limits of applicability

- MITR proves that an action is admissible under the facts passed to it, while the facts themselves are established by the customer's systems, so a wrong rule yields a provably wrong allowance.
- An agent that holds its own keys to the systems bypasses any control layer. The property "there is no way around MITR" belongs to the installation: MITR holds the keys, and the agent keeps only the right to request a check.
- The text of the model, the quality of its answer and implants in its weights lie outside the subject of MITR.
- MITR has no certificate of conformity. At significant critical information infrastructure facilities, the established procedure for confirming the conformity of software and certifying the system applies.
- There has been no third-party check yet: the attack set and the chain replay were run by the institute itself, and everything needed for an outside replay is published.



Autonomous Non-Profit Organization "Scientific Research Institute of System Synthesis", primary state registration number (OGRN) 1267700083617, taxpayer identification number (INN) 9731161602. 18 Davydkovskaya Street, premises VIII, Moscow 121352, Russia. E-mail: af@isslab.ai, page: isslab.ai/mitr/, edition of 26 October 2026.