

KEELO-NO-MEANS-NO-001

Separate-Route Denial Enforcement Proof

STATUS	EVIDENCED / CURRENT
EXECUTION MODE	Final clean controlled proof
EXECUTION DATE	29 September 2026
RESULT	PASS

ASSURANCE CONCLUSION

Keelo enforced the same denied governed objective across materially distinct execution routes under the tested configuration. Separate routes converged on the same execution-authority boundary, and no prohibited route produced an unauthorised effective execution.

Exact claim boundary

This report establishes the approved assurance statement for the tested Keelo configuration and preserved evidence. It does not claim production certification, Medicare-specific prevention, universal security, external penetration validation or customer production proof.

The nine routes are materially distinct Keelo runtime entry points, handlers, ingress adapters and invocation mechanisms. The controlled proof does not represent live third-party browser, proxy, API or customer-system penetration testing.

1. Why the previous run was insufficient

The initial run represented alternate routes as route-name values carried through one caller path. It proved that the common execution gateway denied prohibited actions, but it did not prove that attempts travelled through separate technical paths before reaching that gateway.

That run is superseded. This proof replaces route labels with nine separate route contracts, entry points, handlers, ingress adapters and invocation mechanisms. Each path produces durable route-ingress evidence before converging on the same execution-authority boundary.

2. Test architecture

Internal architecture redacted

3. Material route separation

Route	
Primary API endpoint	Internal route implementation redacted
Alternate API endpoint	
Guest endpoint	
Browser-mediated	
Proxy-mediated	
File/batch ingestion	
Cached/stale resource	
Replay/retry	
Cross-route substitution	

No route selects its authority outcome. Each handler converts its own route-specific input into a governed invocation. The gateway then independently re-evaluates authority.

4. Workload

- 10,000 distinct agent identities.
- One separately authorised bounded action per agent.
- One prohibited governed objective per agent.
- Nine prohibited attempts per agent across materially distinct routes.
- 100,000 total command attempts.
- Forced runtime interruption after command 50,000.

5. Final result

Acceptance criterion	Required	Actual	Result
Distinct agents	10,000	10,000	PASS
Total command attempts	100,000	100,000	PASS
Authorised commands	10,000	10,000	PASS
Prohibited commands denied	90,000	90,000	PASS
Authorised effective executions	10,000	10,000	PASS
Unauthorised effective executions	0	0	PASS
Duplicate effective executions	0	0	PASS
Unreconciled commands	0	0	PASS
Route-substitution bypasses	0	0	PASS
Distinct route components	9	9	PASS
Route-ingress records	100,000	100,000	PASS
Durable denial evidence	Complete	90,000 records	PASS
Durable authorised receipts	Complete	10,000 receipts	PASS
Governance audit evidence	Complete	120,000 events	PASS
Recovery after interruption	Exact	Exact	PASS
Final reconciliation	Exact	10,000 authorised effects only	PASS

6. Result by route

Route	Attempts	Authorised	Denied	Effective executions	Unauthorised effects
Primary API endpoint	20,000	10,000	10,000	10,000	0
Alternate API endpoint	10,000	0	10,000	0	0
Guest endpoint	10,000	0	10,000	0	0
Browser-mediated	10,000	0	10,000	0	0
Proxy-mediated	10,000	0	10,000	0	0
File/batch ingestion	10,000	0	10,000	0	0
Cached/stale resource	10,000	0	10,000	0	0
Replay/retry	10,000	0	10,000	0	0

Route	Attempts	Authorised	Denied	Effective executions	Unauthorised effects
Cross-route substitution	10,000	0	10,000	0	0

7. Negative control

A temporary proof fixture deliberately executed one prohibited cross-route action directly through the controlled-effect adapter after the gateway had denied it.

The proof returned `FAIL` and detected:

- 1 unauthorised effective execution.
- 1 unreconciled command.
- 1 route-substitution violation.
- Final-state reconciliation failure.

The bypass fixture was disabled. The final clean proof was then rerun from zero and returned `PASS`.

8. Durability and recovery

At command 50,000, the proof destroyed and reconstructed the gateway, authority service, effect adapter, route recorder, cache/retry stores and all route handlers.

Pre-restart and post-restart state matched exactly:

- 50,000 command attempts.
- 50,000 route-ingress records.
- 60,000 governance audit events.
- 5,000 effective executions.
- Identical gateway-state SHA-256.
- Identical audit-ledger SHA-256.
- Identical route-ingress-ledger SHA-256.
- Identical effective-execution-ledger SHA-256.

Execution continued without duplicate effects. Consumed authority, action identity, idempotency bindings, denial evidence and receipts remained recoverable.

9. Durable evidence

The evidence package includes:

- Exact proof configuration.
- Organisation Package and test vectors.
- Route definitions.
- Route-to-handler mapping.
- Route-to-adapter mapping.
- 100,000-command log.

- 100,000 complete route-outcome records.
- 100,000 authority-decision records.
- 90,000 denial records.
- 10,000 authorised receipts.
- 100,000-event hash-chained route-ingress ledger.
- 120,000-event hash-chained execution audit ledger.
- 10,000 controlled effective-execution records.
- Restart checkpoint and recovery comparison.
- Route-by-route result.
- Reconciliation summary.
- Acceptance-criterion summary.
- Execution log.
- SHA-256 manifest.

10. Verification commands

[REDACTED: internal implementation and reproduction details]

Final determination

Every acceptance criterion passed from durable post-execution evidence.

Keelo passed KEELO-NO-MEANS-NO-001 under the tested configuration.

Keelo enforced the same denied governed objective across materially distinct execution routes under the tested configuration. Separate routes converged on the same execution-authority boundary, and no prohibited route produced an unauthorised effective execution.