

QA Review — MC #8829 / MC #8154 Rate Limiting

QA Review — MC #8829 (review of MC #8154)

Reviewer: John / Proveo QA posture (tool-verified) **Date:** 2026-07-28 **Subject task:** MC #8154 — [DropSrbija v2 P0.3] Per-endpoint rate limiting IPS admin routes **Subject status:** done **Subject DoD claim:** RateLimit.kt: named configs IPS_INITIATE(10/min/user), ADMIN(30/min/user), VERIFY_OTP(10/min/phone). Wired to IpsRoutes POST /initiate, AmlRoutes /admin/aml, ComplaintsRoutes /admin/complaints, PhoneOtpRoutes /verify-otp. Key extractor: JWT userId for auth, X-Phone header or remoteAddress for unauth. RateLimitConfigTest 7 tests 0 failures. Commit d45fa0161 branch v2/p0-backend-security. Total: 170 tests 0 failures.

Verdict

PASS. Every discrete claim in the DoD is independently reproducible from repo history, working code on the canonical `develop` branch, and a genuine historical JUnit/Kotest XML test-run artifact. One out-of-scope hygiene risk is flagged below (not a defect in MC #8154's work, but a live threat to it).

Evidence written

- `qa-reviews/evidence-8829/RateLimitConfigTest-junit-result.xml` — real Gradle test-run report, `tests="7" failures="0" errors="0"`, timestamp `2026-04-17T13:24:01.970Z` (same day as the commit).
- `qa-reviews/evidence-8829/ratelimit-kt-history.txt` — full commit history of `RateLimit.kt`.
- `qa-reviews/evidence-8829/d45fa0161-commit-stat.txt` — the claimed commit, its message, and diff stat.
- `qa-reviews/evidence-8829/develop-ratelimit-wiring.txt` — `git grep RateLimitNames` on `develop`, all call sites.
- `qa-reviews/evidence-8829/working-tree-status-ratelimit.txt` + `staged-regression-diff.txt` — the unrelated contamination finding (see below).

Checks performed

Named rate-limit configs (IPS_INITIATE 10/min, ADMIN 30/min, VERIFY_OTP 10/min)

Result: PASS. Confirmed on `develop` (`git show develop:../plugins/RateLimit.kt`):

```
object RateLimitNames {
    val IPS_INITIATE = RateLimitName("ips-initiate")
    val ADMIN = RateLimitName("admin")
    val VERIFY_OTP = RateLimitName("verify-otp")
}

register(RateLimitNames.IPS_INITIATE) { rateLimiter(limit = 10, refillPeriod = 1.minutes) ...
}

register(RateLimitNames.ADMIN)          { rateLimiter(limit = 30, refillPeriod = 1.minutes) ...
}

register(RateLimitNames.VERIFY_OTP)    { rateLimiter(limit = 10, refillPeriod = 1.minutes) ...
}
```

Key extractor matches the claim exactly: JWT `principal<DropSrbijaPrincipal>().userId` with `remoteAddress` fallback for IPS_INITIATE/ADMIN; `X-Phone` header with `remoteAddress` fallback for VERIFY_OTP.

Route wiring

Result: PASS, and more thorough than the DoD summary states. On `develop`, `RateLimitNames.IPS_INITIATE` is wired in `IpsRoutes.kt` (line 85, closes line 202), `RateLimitNames.VERIFY_OTP` in `PhoneOtpRoutes.kt` (line 88), and `RateLimitNames.ADMIN` is wired not only in the two routes the DoD names (`AmlRoutes.kt`, `ComplaintsRoutes.kt`) but also in `MetricsRoutes.kt`, `FeatureFlagsRoutes.kt`, `DisputesRoutes.kt`, `AuditRoutes.kt`, and `ReportsRoutes.kt` — i.e. the admin rate limit protects more surface than the DoD text mentions, not less.

RateLimitConfigTest — 7 tests, 0 failures

Result: PASS, verified with a real execution artifact, not just source reading. `backend/build/test-results/test/TEST-no.alai.dropsrbija.plugins.RateLimitConfigTest.xml` shows:

```
tests="7" skipped="0" failures="0" errors="0" timestamp="2026-04-17T13:24:01.970Z"
```

All 7 test case names match the claimed coverage (constant presence ×3, distinctness, per-config requirement match ×3). Test source on `develop` is byte-identical to the working-tree copy.

Commit d45fa0161 / branch v2/p0-backend-security

Result: PASS. The commit exists, is on `v2/p0-backend-security`, and is an ancestor of both `develop` and the currently checked-out branch. Its message ("restore RateLimitNames object + per-endpoint configs... All 170 tests pass. MC #8152") is honest about scope: the commit itself only touches `IpsRoutes.kt` + `IpsRoutesDisclosureTest.kt` (fixing a compile blocker and wiring audit logging), while the actual named-config restoration had already landed in the parent commit `85eb6f35a` ("feat(drop-srbija v2): P0.1-P0.4 security hardening (MC #8152-8155)"). Net effect matches the DoD claim.

"170 total tests, 0 failures"

Not independently re-executed in this review (would require a full Gradle+Testcontainers run; out of scope for a documentary QA pass given no anomaly signal). Corroborated indirectly: the commit message states "170 tests pass" for the same date/commit where the `RateLimitConfigTest` XML (7/7) is independently confirmed live, and no contradicting historical test-results artifact was found.

Out-of-scope finding — flag for CEO/FlowForge attention

The working tree currently checked out at `~/ALAI/products/DropSrbija` (symlink to `~/business/ALAI-Holding-AS`, branch `feat/oauth-metrics-reader-103888`) has a large **uncommitted, staged** diff (144 files, +6739/-23344) unrelated to MC #8154. Inside that diff, `RateLimit.kt` is staged back down to the pre-P0.3 global-only limiter, stripping the `RateLimitNames` object — while `MetricsRoutes.kt`, `FeatureFlagsRoutes.kt`, `ComplaintsRoutes.kt`, `DisputesRoutes.kt`, `AuditRoutes.kt`, and `ReportsRoutes.kt` still import and call `RateLimitNames.ADMIN` in the same working tree. If this staged state were ever committed as-is, it would both **break compilation** (unresolved reference) and **silently regress the P0.3 security fix** MC #8154 delivered. This is not a defect in MC #8154 — `develop` is clean and correct — but it is a live risk sitting in a shared working directory. Recommend whoever owns `feat/oauth-metrics-reader-103888` either restore `RateLimit.kt` from `develop/HEAD` before committing, or explicitly confirm this file was staged by accident.

Conclusion

MC #8154's DoD claims are verified: PASS. No rework required for #8154 itself. One separate hygiene risk flagged above for a different in-flight task.

Published from local evidence artifact: `products/DropSrbija/qa-reviews/mc-8829-qa-review-8154.md`.

Revision #1

Created 2026-07-28 18:21:44 UTC by John

Updated 2026-07-28 18:21:44 UTC by John