Bilko CIAM abuse-gate fix — checkBefore moved outside SERIALIZABLE tx (MC #104069, root-cause of #103245)

Bilko CIAM abuse-gate fix — checkBefore moved outside SERIALIZABLE tx

MC #104069 | Root-cause of **MC #103245** | Fixed 2026-06-20

1. THE BUG (root cause)

MC #103245 [H1-PRE-PUBLIC-LAUNCH] CIAM abuse gate was marked done 2026-06-09 16:35, but the actual fix was committed 17:27 and **NEVER merged**. In `origin/main`, `CiamAbuseGate.checkBefore()` ran ONLY inside `UserProvisioningService.kt` (called from inside the SERIALIZABLE `transaction{}` block in `AuthService.createSessionFromEntraIdToken`, line 334).

Exposed's SERIALIZABLE transaction retry handler caught/swallowed `DisposableEmailException` and `TooManyRequestsException` → disposable-email accounts (e.g. guerrillamailblock.com) and over-rate-limit requests got provisioned with HTTP 200 despite the gate. **The disposable-email + rate-limit abuse gate was effectively defeated on the JIT/Entra provisioning path.**

2. THE FIX

Commit: `a862355a` → rebased `deb1621d`
Branch: `fix/abuse-gate-tx-swallow-103245`
PR: #3

Changes:

- **FIX1:** `AuthService.kt` (~line 329) — `CiamAbuseGate.checkBefore(email)` now called **BEFORE** the SERIALIZABLE `transaction{}` opens; exceptions propagate directly to StatusPages with no retry/swallow.
- **FIX2:** `routes/AuthRoutes.kt` (lines 379-388) — explicit re-throw catches for `DisposableEmailException` and `TooManyRequestsException` before the broad `catch(Exception)`.
- `StatusPages.kt` (111-129): `DisposableEmailException` → HTTP 422 (VAL_002); `TooManyRequestsException` → HTTP 429 (INFRA_002).
- **New test:** `CiamAbuseGateTransactionPathTest.kt` (+223 lines) — TX1/TX2/TX3 exercising the full `createSessionFromEntraIdToken` path through the SERIALIZABLE tx wrapper (the gap prior unit tests missed).

3. VERIFICATION

- **Manual branch build #44** (Azure DevOps Bilko-CI-CD): `CI_Gates 8/8 PASS` + `Build` + `Flyway` + `Deploy_Stage` SUCCEEDED on commit `deb1621d`.

  URL: https://dev.azure.com/alai-holding/Bilko/_build/results?buildId=44
- **Proveo integration tests** (real PostgreSQL/Testcontainers): `CiamAbuseGateTransactionPathTest 3/3 PASS`, `CiamAbuseGateTest 4/4 PASS`.
- **Live stage** confirmed serving the fix; gate sits behind Entra JWT signature verification (security boundary — a fully external HTTP 422 probe is not reachable without a tenant-signed Entra token, which is itself a positive security property).
- **Evidence bundle:** `/tmp/evidence-104069/` (proveo-abuse-probe/VERDICT.md, test XMLs, probe captures; build-43/44 logs).

4. PROCESS LESSON

A parent MC was closed before its fix was merged → the fix sat unmerged in a worktree for ~11 days.

Lesson: Do not mark a security MC done until the fix is verified merged on main. Link this to the broader "no fake DONE" rule.

References

- MC #104069 (parent security fix task)
- MC #103245 (original abuse gate task)
- Evidence bundle: `/tmp/evidence-104069/`
- PR #3: `fix/abuse-gate-tx-swallow-103245`

Revision #1
Created 2026-06-21 06:02:52 UTC by John
Updated 2026-06-21 06:02:52 UTC by John