

KPO Export RBAC Fix — MC #105326

KPO Export RBAC Fix — MC #105326

Finding

Proveo adversarial verify on MC #105321 (2026-07-12) found that `GET /reports/kpo/export/pdf` and `GET /reports/kpo/export/xlsx` in `ReportRoutes.kt` were missing the `requirePermission(principal, "report:export")` guard that every other export route (KIR, KPR, VAT, P&L, balance-sheet, accountant CSV package) already has. Git diff confirmed the gap pre-dated the T1b diff — it was a pre-existing asymmetry, not a regression.

Fix

Added `if (requirePermission(principal, "report:export")) return@get` to both KPO export routes in `apps/api/src/main/kotlin/no/alai/bilko/routes/ReportRoutes.kt`, matching the exact pattern used at the other 11 export-route call sites in the same file (13 total after the fix).

Tests

Added 4 integration tests to

`apps/api/src/test/kotlin/no/alai/bilko/routes/ReportRoutesHttpIntegrationTest.kt`:

- `GET reports kpo export pdf rejects viewer role with 403`
- `GET reports kpo export xlsx rejects viewer role with 403`
- `GET reports kpo export pdf allows owner role` (passes RBAC, hits NotImplemented stub per MC #100038)
- `GET reports kpo export xlsx allows owner role`

Verified: `./gradlew integrationTest --tests "no.alai.bilko.routes.ReportRoutesHttpIntegrationTest"`
`--rerun` → BUILD SUCCESSFUL, 0 failures / 0 errors.

P2P Peer Verify

Proveo independent pre-verifier: PASS. `mesh-thr-d41602c0-65fa-4d4c-bca4-8fe770f11704` / `mesh-msg-e3c3869f-f160-4e65-a9d0-8ba27f000686`. Transcript: `/tmp/alai/p2p-pairing-evidence/mc105326-transcript.md`.

Revision #1

Created 2026-07-12 01:21:56 UTC by John

Updated 2026-07-12 01:21:57 UTC by John