

QA Review — MC #8745 for MC #8678 Intesa Bridge Leak

QA Review Final — MC #8745 reviewing MC #8678

Reviewer: John / Proveo QA mode

Date (UTC): 2026-07-28

Subject: MC #8678 — `FIX: /intesa-bridge leak on bilko-demo.alai.no – isolate to intesa Cloud`
`Run only`

Verdict

PASS for the leak fix. Current canonical Bilko source and live public demo domains do not expose a public `/intesa-bridge` route.

Evidence checked

Mission Control

- `mc.js show 8678`: task is `done`; original DoD text says `intesa-bridge 404 confirmed live on bilko-demo.alai.no (commit 66d2220)` and notes the CI fix was separate.
- `mc.js show 8745`: QA task existed for this review and was paused before this final evidence artifact.
- `mc.js show 8716`: follow-up task exists for the broader branch-purity/CI guard: `PI2: Client prefix registry + branch purity CI`, status `open`, priority `L`.

Repository inspected

Path: `/Users/makinja/business/ALAI-Holding-AS/products/Bilko`

- `BUILD-BLUEPRINT.md` read first. It identifies `azdo` as the canonical remote and warns that GitHub mirrors are stale.
- Worktree status at check time: `fix/chatbot-per-user-ratelimit-105463-v2...azdo/main` [ahead 1, behind 42] with unrelated modified files; therefore checks used both `azdo/main` and `HEAD` where relevant.
- Canonical ref observed: `azdo/main` = `c34f10e9`; local `HEAD` = `68578f35`.

Git/history checks

- Fix commit exists:
 - `66d222062543a59ac35d896c7f4953e67a262f64 fix(security): remove /intesa-bridge leak from public Bilko demo (MC #8678)`
 - Touched/removal files under `apps/web`: `apps/web/app/(dashboard)/intesa-bridge/page.tsx`, `apps/web/components/sidebar.tsx`, `apps/web/lib/auth-provider.tsx`, `apps/web/lib/intesa-bih-mock-data.ts`, and locale message files.
- Leak-introducing commit exists:
 - `13c2efb728e9eaab30aad9cc0b392940126a9ee feat(intesa-demo): BiH-localized bank bridge demo for Intesa Sanpaolo pitch`

Current source-tree leak checks

Commands run in the Bilko repo:

```
git ls-tree -r --name-only azdo/main apps/web/app | grep -Ei 'intesa|corpint' || true
git ls-tree -r --name-only HEAD apps/web/app | grep -Ei 'intesa|corpint' || true
find apps/web/app \( -iname '*intesa*' -o -iname '*corpint*' \) -print | sort
```

Result: all three checks returned no matching route paths.

The existing E2E spec `apps/e2e/tests/intesa-bridge.spec.ts` is fully skipped via `test.describe.skip(...)` and includes a comment stating `/intesa-bridge route is not implemented in apps/web/app/ yet`.

Live domain checks

Commands used `curl -k -sS -I -L --max-time 15`.

- `https://bilko-demo.alai.no/intesa-bridge` — `curl: Could not resolve host`, HTTP `000`. This is expected for the retired GCP-era demo host.
- `https://app.bilko.io/intesa-bridge` — redirects once to `/login?redirect=%2Fintesa-bridge`, final HTTP `200` login page.
- `https://app.bilko.cloud/intesa-bridge` — redirects once to `/login?redirect=%2Fintesa-bridge`, final HTTP `200` login page.

- `https://app.bilko.company/intesa-bridge` — redirects once to `/login?redirect=%2Fintesa-bridge`, final HTTP 200 login page.
- Control path `https://app.bilko.cloud/this-route-should-not-exist-xyz123` behaves the same: redirects once to `/login?redirect=%2Fthis-route-should-not-exist-xyz123`, final HTTP 200 login page.

Interpretation: current public app is auth-gated before route-specific 404s, so curl cannot distinguish nonexistent private routes from existing private routes unauthenticated. Source-tree absence is therefore the decisive leak check; live probes confirm no unauthenticated Intesa content is served.

Deployment-map/doc checks

`docs/DEPLOY-MAP.md` and related docs record that:

- Current public demo domains are `app.bilko.cloud`, `app.bilko.io`, and `app.bilko.company` on Azure ACA.
- `bilko-demo.alai.no` is legacy/dead DNS after the GCP → Azure migration (MC #103633 / OCD-11).
- GCP Cloud Run demo services are archived/decommissioned for current public demo use.

Evidence-file and CI-guard checks

- `docs/evidence/8678/verification.json` is **not present** in the current Bilko worktree.
- CI guard grep across `azure-pipelines.yml`, `.github/workflows/*`, and `scripts/ci/*` found no `intesa` or `corpint` guard in those checked files.
- This is not a regression in #8678 because MC #8678's own DoD said: `CI fix is separate task (WIF secrets)`. The separate open follow-up found is MC #8716.

Findings

1. **No current public leak found.** `apps/web/app` contains no `intesa`/`corpint` routes on `azdo/main`, local `HEAD`, or working tree.
2. **Original fix is real.** Commit `66d2220` exists and removes the leaked Intesa route and related web artifacts.
3. **Original proof file is stale/missing.** The DoD-cited `docs/evidence/8678/verification.json` does not exist in the current worktree, and the original host `bilko-demo.alai.no` no longer resolves.
4. **Preventive CI guard remains a follow-up.** No checked CI file currently contains the `intesa`/`corpint` branch-purity guard; MC #8716 tracks that broader follow-up.

Recommendation

Close MC #8745 as **QA PASS** for MC #8678. Keep MC #8716 open as the low-priority preventive CI/branch-purity follow-up.

Revision #2

Created 2026-07-28 07:47:13 UTC by John

Updated 2026-08-10 07:37:54 UTC by John