Bilko Mobile Phase 0 Auth Bridge — Status 2026-06-05

Bilko Mobile Phase 0 Auth Bridge — Status 2026-06-05

Executive summary

Bilko mobile direction is native **iPhone + Samsung/Android**, with **React Native + Expo** as the implementation path. The PWA/mobile-web direction is superseded for the companion mobile app.

Phase 0 backend/auth work is implemented locally and targeted tests are green. The mobile app build should **not** be dispatched until the remaining gates below are closed.

What was changed

Documentation and architecture

Updated or created:

- `docs/mobile/MOBILE-ARCHITECTURE.md`
- `docs/mobile/MOBILE-IMPL-SPEC-PHASE1.md`
- `docs/mobile/MOBILE-PRD.md`
- `docs/mobile/README.md`
- `docs/INDEX.md`
- `/Users/makinja/system/specs/bilko-tech-stack.md`
- `docs/architecture/ADR-037-BILKO-MOBILE-NATIVE-ENTRA-AUTH.md`
- `docs/backend/MOBILE-ENTRA-AUTH-BRIDGE-SPEC.md`

Key doc decisions:

- Native iOS/Android app is the target, not PWA.

- React Native + Expo is the chosen native cross-platform path.
- Entra External ID + OIDC Authorization Code + PKCE is the target mobile/customer login model.
- Phase 1 uses existing `/api/v1/*` endpoints; a dedicated `/mobile/*` BFF is deferred.
- Mobile refresh must not depend on browser cookies.
- Email claims from Entra are not trusted for login mapping.

Backend/auth implementation

Added or changed:

- `apps/api/src/main/kotlin/no/alai/bilko/auth/EntraExternalIdService.kt`
  - Verifies Microsoft Entra External ID JWTs.
  - Fails closed if issuer/audience/JWKS config is missing.
  - Enforces RS256 and `kid`.
  - Verifies configured issuer and audience.
  - Extracts verified subject from `sub`, with `oid` fallback.
- `apps/api/src/main/resources/db/migration/V64__entra_external_identities.sql`
  - Adds `entra_external_identities` mapping table.
  - Maps verified `issuer + subject` to existing Bilko user.
  - Adds SECURITY DEFINER functions with fixed `SET search_path = public, pg_temp`:
    - `bilko_auth.find_user_by_entra_identity(text, text)`
    - `bilko_auth.mark_entra_login(text, text)`
- `apps/api/src/main/kotlin/no/alai/bilko/db/AuthUserRepository.kt`
  - Adds `findByEntraIdentity(issuer, subject)`.
  - Adds `markEntraLogin(issuer, subject)`.
- `apps/api/src/main/kotlin/no/alai/bilko/auth/AuthService.kt`
  - Adds `createSessionFromEntraIdToken(idToken)`.
  - Maps verified Entra identity to active Bilko user/org/role.
  - Issues existing Bilko access + refresh tokens.
- `apps/api/src/main/kotlin/no/alai/bilko/plugins/DI.kt`
  - Wires `EntraExternalIdService` into `AuthService`.
- `apps/api/src/main/kotlin/no/alai/bilko/routes/AuthRoutes.kt`
  - Adds `POST /api/v1/auth/entra/session`.
  - Adds `POST /api/v1/auth/mobile/refresh`.
  - Preserves existing web cookie refresh endpoint `POST /api/v1/auth/refresh`.
  - Hardened bad-body handling by removing `printStackTrace()` and detailed parser error echo from register bad-body response.

Tests added or extended

- `apps/api/src/test/kotlin/no/alai/bilko/auth/EntraExternalIdServiceTest.kt`
  - valid token

    - wrong audience
    - wrong issuer
    - expired token
    - HS256 rejection
    - missing `sub`/`oid`
    - missing config fail-closed
- `apps/api/src/test/kotlin/no/alai/bilko/db/AuthUserRepositoryTest.kt`
    - Flyway migration execution on disposable PostgreSQL/Testcontainers DB, including V64.
    - mapped Entra identity returns user
    - unmapped identity returns null
    - inactive mapped user returns null
    - soft-deleted mapped user returns null
    - org/role/status assertions
    - `markEntraLogin()` metadata update
- `apps/api/src/test/kotlin/no/alai/bilko/auth/AuthServiceTest.kt`
    - refresh-token rotation/reuse rejection test
- `apps/api/src/test/kotlin/no/alai/bilko/routes/AuthRoutesHttpIntegrationTest.kt`
    - `/auth/entra/session` missing `idToken` returns 400
    - `/auth/entra/session` missing Entra config returns 503 `CONFIGURATION_ERROR`
    - `/auth/mobile/refresh` missing `refreshToken` returns 400
    - `/auth/mobile/refresh` with structurally valid but stale/non-DB refresh JTI returns 401
    - web cookie refresh/logout stale-token regression remains covered

Validation evidence

Evidence files:

- `/Users/makinja/system/evidence/bilko-mobile-doc-review-20260604.md`
- `/Users/makinja/system/evidence/bilko-mobile-auth-local-security-audit-20260604.md`
- `/Users/makinja/system/evidence/securion-review-check-102962-20260605.md`

Commands recorded as green in evidence:

- `./gradlew compileKotlin --no-daemon` → BUILD SUCCESSFUL
- `./gradlew compileKotlin compileTestKotlin --no-daemon` → BUILD SUCCESSFUL
- `./gradlew test --tests no.alai.bilko.auth.EntraExternalIdServiceTest --no-daemon` → BUILD SUCCESSFUL
- `./gradlew integrationTest --tests no.alai.bilko.db.AuthUserRepositoryTest --no-daemon` → BUILD SUCCESSFUL
- `./gradlew integrationTest --tests no.alai.bilko.auth.AuthServiceTest --no-daemon` → BUILD SUCCESSFUL
- `./gradlew integrationTest --tests no.alai.bilko.routes.AuthRoutesHttpIntegrationTest --no-daemon` → BUILD SUCCESSFUL

- Combined targeted run:
  - `./gradlew compileKotlin compileTestKotlin test --tests no.alai.bilko.auth.EntraExternalIdServiceTest integrationTest --tests no.alai.bilko.db.AuthUserRepositoryTest --tests no.alai.bilko.auth.AuthServiceTest --tests no.alai.bilko.routes.AuthRoutesHttpIntegrationTest --no-daemon` → BUILD SUCCESSFUL

Where we stand

Done locally

- Mobile architecture direction cleaned up and made native-first.
- Entra External ID bridge implemented.
- Mobile-safe body refresh endpoint implemented.
- V64 migration implemented and executed via Testcontainers/Flyway integration test.
- Targeted local tests passed.
- Local security audit completed with no critical/high local findings; one route error-handling hygiene issue was fixed.

Still blocked

- No independent Securion/QA domain PASS has been received.
- MC `#102962` was checked and is still open in `/Users/makinja/system/evidence/securion-review-check-102962-20260605.md`.
- Real Entra staging trigger substitutions are provisioned/verified, but the current Azure tenant is `AAD` (`alemalai.onmicrosoft.com`), not a separate CIAM customer tenant. Customer-facing CIAM tenant policy/MFA/passwordless configuration remains a later production gate.
- No live environment/browser/mobile-device verification has been performed for this auth bridge.

Decision

Do **not** dispatch mobile app build yet.

Next concrete step is to stop waiting for passive task pickup and run/obtain a real independent security/QA review, then provision/test real Entra External ID config. After those pass, dispatch the native React Native + Expo mobile build.

Stage deploy — substitution wiring (MC #102996, 2026-06-05)

`infrastructure/gcp/cloudbuild-stage.yaml` is now substitution-ready for Entra External ID metadata:

- Three substitutions added to the `substitutions:` block: `_ENTRA_EXTERNAL_ID_ISSUER`, `_ENTRA_EXTERNAL_ID_AUDIENCE`, `_ENTRA_EXTERNAL_ID_JWKS_URL`, all defaulting to `__UNSET__`.
- A conditional block in the `deploy-api-no-traffic` step builds `ENTRA_ENV_VARS`. If all three substitutions are non-`__UNSET__` and non-empty, they are appended to `--set-env-vars` as `;ENTRA_EXTERNAL_ID_ISSUER=...;ENTRA_EXTERNAL_ID_AUDIENCE=...;ENTRA_EXTERNAL_ID_JWKS_URL=...`. Otherwise `ENTRA_ENV_VARS=""` — the env-vars string is unchanged and current stage behaviour is preserved exactly.
- Values are provisioned in the `bilko-stage-auto-deploy` trigger as of 2026-06-05:
  - `_ENTRA_EXTERNAL_ID_ISSUER=https://login.microsoftonline.com/3454a03f-20b4-4bda-a116-2293c459aecd/v2.0`
  - `_ENTRA_EXTERNAL_ID_AUDIENCE=95b2a55f-8f48-4c9c-b4f8-eb455e3bdfd7`
  - `_ENTRA_EXTERNAL_ID_JWKS_URL=https://login.microsoftonline.com/3454a03f-20b4-4bda-a116-2293c459aecd/discovery/v2.0/keys`
- No stage smoke has been run against Entra yet. Stage will only receive these env vars after the committed Cloud Build wiring is pushed/merged and the trigger deploys a new API revision.

Immediate next actions

1. Force active review path for MC `#102962` or run a direct independent Securion/QA validation with evidence.
2. Push/merge the clean Phase 0 branch through the gated path.
3. Trigger a stage build and confirm `MC#102996: Entra metadata present` log line appears and the three vars are visible in the Cloud Run revision env.
4. Run `/api/v1/auth/entra/session` against a real Entra test tenant token.
5. Run `/api/v1/auth/mobile/refresh` with real issued mobile refresh token.
6. Close Securion MC `#102989` with passing evidence.
7. Only after PASS evidence, dispatch native mobile implementation.

Revision #1
Created 2026-06-07 19:42:58 UTC by John
Updated 2026-06-07 19:42:58 UTC by John